



Documentación del software StorageGRID 11.9

StorageGRID software

NetApp
December 03, 2025

This PDF was generated from <https://docs.netapp.com/es-es/storagegrid-119/index.html> on December 03, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Documentación del software StorageGRID 11.9	1
Dispositivos StorageGRID	2
Notas de la versión	3
Comience a utilizar un sistema StorageGRID	4
Obtenga más información sobre StorageGRID	4
¿Qué es StorageGRID?	4
Nubes híbridas con StorageGRID	6
Arquitectura y topología de red de StorageGRID	7
Nodos y servicios de la red	11
Cómo gestiona StorageGRID los datos	23
Explorar StorageGRID	35
Pautas para establecer redes	43
Pautas para establecer redes	43
Tipos de red StorageGRID	45
Ejemplos de topología de red	49
Requisitos de red	55
Requisitos específicos de la red	57
Consideraciones de red específicas de la implementación	59
Instalación y aprovisionamiento de redes	62
Pautas posteriores a la instalación	63
Referencia del puerto de red	63
Inicio rápido para StorageGRID	74
Instalar, actualizar y reparar StorageGRID	77
Dispositivos StorageGRID	77
Instalar StorageGRID en Red Hat Enterprise Linux	77
Inicio rápido para la instalación de StorageGRID en Red Hat Enterprise Linux	77
Planifique y prepare la instalación en Red Hat	78
Automatizar la instalación de StorageGRID en Red Hat Enterprise Linux	105
Implementar nodos de red virtuales (Red Hat)	108
Configurar la red y completar la instalación (Red Hat)	132
Instalación API REST	145
¿A dónde ir después?	146
Solucionar problemas de instalación	147
Ejemplo /etc/sysconfig/network-scripts	148
Instalar StorageGRID en Ubuntu o Debian	150
Inicio rápido para instalar StorageGRID en Ubuntu o Debian	150
Planifique y prepare la instalación en Ubuntu o Debian	151
Automatizar la instalación (Ubuntu o Debian)	179
Implementar nodos de red virtuales (Ubuntu o Debian)	181
Configurar la red y completar la instalación (Ubuntu o Debian)	205
Instalación API REST	218
¿A dónde ir después?	219
Solucionar problemas de instalación	220

Ejemplo /etc/network/interfaces	221
Instalar StorageGRID en VMware	222
Inicio rápido para la instalación de StorageGRID en VMware	222
Planificar y prepararse para la instalación en VMware	223
Automatizar la instalación (VMware)	233
Implementar nodos de red de máquinas virtuales (VMware)	247
Configurar la red y completar la instalación (VMware)	256
Instalación API REST	269
¿A dónde ir después?	270
Solucionar problemas de instalación	271
Actualizar el software StorageGRID	273
Actualizar el software StorageGRID	273
Novedades de StorageGRID 11.9	273
Funciones y capacidades eliminadas o en desuso	276
Cambios en la API de administración de la red	278
Cambios en la API de administración de inquilinos	279
Planifique y prepárese para la actualización	279
Actualizar software	287
Solucionar problemas de actualización	303
Aplicar la revisión de StorageGRID	306
Procedimiento de revisión de StorageGRID	306
Cómo se ve afectado su sistema cuando aplica una revisión	307
Obtener los materiales necesarios para la revisión	308
Descargar archivo de revisión	309
Verifique el estado del sistema antes de aplicar la revisión	309
Aplicar revisión	310
Configurar y administrar un sistema StorageGRID	315
Administrar StorageGRID	315
Administrar StorageGRID	315
Comience a usar Grid Manager	315
Controlar el acceso a StorageGRID	346
Utilizar la federación de red	398
Gestionar la seguridad	435
Administrar inquilinos	504
Configurar conexiones de cliente	525
Administrar redes y conexiones	567
Utilice AutoSupport	586
Administrar nodos de almacenamiento	601
Administrar nodos de administración	615
Administrar objetos con ILM	618
Administrar objetos con ILM	618
ILM y ciclo de vida de los objetos	619
Crear y asignar grados de almacenamiento	641
Utilice grupos de almacenamiento	644
Utilice grupos de almacenamiento en la nube	652

Administrar perfiles de codificación de borrado	673
Configurar regiones (opcional y solo S3)	676
Crear regla ILM	678
Administrar políticas de ILM	694
Trabajar con políticas y reglas de ILM	711
Usar bloqueo de objetos S3	715
Ejemplo de reglas y políticas de ILM	724
Endurecimiento del sistema	744
Consideraciones generales para el fortalecimiento del sistema	744
Pautas de refuerzo para las actualizaciones de software	745
Pautas de fortalecimiento para redes StorageGRID	746
Pautas de refuerzo para nodos StorageGRID	747
Pautas de refuerzo para TLS y SSH	750
Otras pautas de endurecimiento	751
Configurar StorageGRID para FabricPool	753
Configurar StorageGRID para FabricPool	753
Información necesaria para adjuntar StorageGRID como un nivel de nube	755
Utilice el asistente de configuración de FabricPool	756
Configurar StorageGRID manualmente	770
Configurar el Administrador del sistema ONTAP	780
Configurar el servidor DNS	782
Prácticas recomendadas de StorageGRID para FabricPool	783
Eliminar datos de FabricPool de StorageGRID	787
Utilice inquilinos y clientes de StorageGRID	789
Utilice una cuenta de inquilino	789
Utilice una cuenta de inquilino	789
Cómo iniciar y cerrar sesión	790
Comprender el panel de control de Tenant Manager	795
API de gestión de inquilinos	798
Utilizar conexiones de federación de red	803
Administrar grupos y usuarios	816
Administrar claves de acceso S3	835
Administrar depósitos S3	841
Administrar los servicios de la plataforma S3	865
Utilice la API REST de S3	898
Versiones y actualizaciones compatibles con la API REST de S3	898
Referencia rápida: solicitudes de API de S3 compatibles	901
Probar la configuración de la API REST de S3	920
Cómo StorageGRID implementa la API REST de S3	921
Compatibilidad con la API REST de Amazon S3	936
Operaciones personalizadas de StorageGRID	986
Políticas de acceso a grupos y buckets	1008
Operaciones de S3 rastreadas en los registros de auditoría	1034
Utilice la API REST de Swift (fin de vida útil)	1035
Utilice la API REST de Swift	1035

Supervisar y solucionar problemas de un sistema StorageGRID	1036
Supervisar el sistema StorageGRID	1036
Supervisar un sistema StorageGRID	1036
Ver y administrar el panel de control	1036
Ver la página de Nodos	1039
Información a monitorear regularmente	1073
Administrar alertas	1104
Referencia de archivos de registro	1143
Configurar destinos de mensajes y registros de auditoría	1163
Utilice la monitorización SNMP	1177
Recopilar datos adicionales de StorageGRID	1189
Solucionar problemas del sistema StorageGRID	1224
Solucionar problemas de un sistema StorageGRID	1224
Solucionar problemas de objetos y almacenamiento	1232
Solucionar problemas de metadatos	1261
Solucionar errores de certificado	1263
Solucionar problemas del nodo de administración y de la interfaz de usuario	1264
Solucionar problemas de red, hardware y plataforma	1268
Solucionar problemas de un servidor syslog externo	1275
Revisar los registros de auditoría	1278
Mensajes y registros de auditoría	1278
Auditoría del flujo y retención de mensajes	1279
Archivo de registro de auditoría de acceso	1282
Rotación de archivos de registro de auditoría	1283
Formato de archivo de registro de auditoría	1283
Formato del mensaje de auditoría	1296
Mensajes de auditoría y el ciclo de vida de los objetos	1301
Mensajes de auditoría	1308
Expandir una cuadrícula	1360
Tipos de expansión	1360
Plan de expansión de StorageGRID	1361
Añadir capacidad de almacenamiento	1361
Añadir capacidad de metadatos	1369
Agregue nodos de red para agregar capacidades a su sistema	1371
Agregar un nuevo sitio	1371
Reúna los materiales necesarios	1372
Descargue y extraiga los archivos de instalación de StorageGRID	1373
Verificar hardware y redes	1379
Agregar volúmenes de almacenamiento	1379
Agregar volúmenes de almacenamiento a los nodos de almacenamiento	1380
VMware: Agregar volúmenes de almacenamiento al nodo de almacenamiento	1382
Linux: Agregar volúmenes SAN o de conexión directa al nodo de almacenamiento	1384
Agregar nodos de cuadrícula o sitio	1387
Agregar nodos de cuadrícula a un sitio existente o agregar un sitio nuevo	1387
Actualizar subredes para la red Grid	1388

Implementar nuevos nodos de red	1389
Realizar expansión.	1395
Configurar el sistema expandido	1402
Pasos de configuración después de la expansión.	1402
Verificar que el nodo de almacenamiento esté activo	1404
Copiar la base de datos del nodo de administración	1405
Copiar métricas de Prometheus	1406
Copiar registros de auditoría	1407
Reequilibrar los datos codificados por borrado después de agregar nodos de almacenamiento	1409
Solucionar problemas de expansión	1412
Mantener un sistema StorageGRID	1414
Mantenimiento de la red.	1414
Antes de empezar	1414
Procedimientos de mantenimiento de electrodomésticos	1414
Descargar paquete de recuperación	1414
Desmantelar nodos o sitios	1415
Nodo o sitio de desmantelamiento.	1415
Nodos de desmantelamiento	1415
Sitio de desmantelamiento.	1435
Cambiar el nombre de la cuadrícula, el sitio o el nodo	1458
Utilice el procedimiento de cambio de nombre	1458
Agregar o actualizar nombres para mostrar	1463
Procedimientos de nodo	1469
Procedimientos de mantenimiento de nodos.	1469
Procedimientos del Administrador de servidores.	1470
Procedimientos de reinicio, apagado y encendido	1479
Procedimientos de reasignación de puertos	1492
Procedimientos de red	1496
Actualizar subredes para la red Grid	1496
Configurar direcciones IP.	1498
Agregar interfaces a un nodo existente	1516
Configurar servidores DNS	1520
Modificar la configuración de DNS para un solo nodo de red	1521
Administrar servidores NTP	1523
Restaurar la conectividad de red para nodos aislados	1524
Procedimientos de host y middleware	1526
Linux: Migrar el nodo de la red a un nuevo host	1526
VMware: Configurar la máquina virtual para el reinicio automático.	1528
Recuperar o reemplazar nodos	1529
Advertencias y consideraciones para la recuperación del nodo de la red	1529
Condiciones previas para la recuperación de nodos de la red	1529
Orden de recuperación de nodos si falla un servidor que aloja más de un nodo de red.	1530
Direcciones IP de los nodos recuperados	1530
Reúna los materiales necesarios para la recuperación del nodo de la red	1530
Descargue y extraiga los archivos de instalación de StorageGRID	1531

Seleccionar el procedimiento de recuperación del nodo	1537
Recuperarse de fallos del nodo de almacenamiento	1538
Recuperarse de fallos del nodo de almacenamiento	1538
Recuperar el nodo de almacenamiento del dispositivo	1539
Recuperarse de una falla del volumen de almacenamiento donde la unidad del sistema está intacta	1562
Recuperarse de una falla de la unidad del sistema	1577
Restaurar datos de objetos mediante Grid Manager	1595
Supervisar trabajos de reparación de datos	1598
Recuperarse de fallos del nodo de administración	1600
Recuperación del nodo de administración primario o no primario	1600
Recuperarse de fallas del nodo de administración principal	1600
Recuperarse de fallas del nodo de administración no principal	1609
Recuperarse de fallos del nodo de enlace	1617
Reemplazar el nodo de puerta de enlace	1617
Seleccione Iniciar recuperación para configurar el nodo de puerta de enlace	1618
Recuperarse de fallos del nodo de archivo	1620
Recuperarse de fallos del nodo de archivo	1620
Reemplazar el nodo Linux	1620
Reemplazar el nodo Linux	1620
Implementar nuevos hosts Linux	1620
Restaurar los nodos de la red en el host	1621
¿Qué sigue?: Realice pasos de recuperación adicionales, si es necesario	1626
Reemplazar el nodo VMware	1627
Reemplazar el nodo fallido con un dispositivo de servicios	1628
Reemplazar el nodo fallido con un dispositivo de servicios	1628
Instalar dispositivo de servicios (solo cambio de plataforma)	1629
Preparar el dispositivo para la reinstalación (solo reemplazo de plataforma)	1629
Iniciar la instalación del software en el dispositivo de servicios	1630
Instalación de dispositivos de servicios de monitorización	1633
Cómo el soporte técnico recupera un sitio	1636
Cómo habilitar StorageGRID en su entorno	1638
Cómo administrar StorageGRID mediante la consola de NetApp	1639
Avisos legales	1640
Copyright	1640
Marcas comerciales	1640
Patentes	1640
Política de privacidad	1640
Código abierto	1640

Documentación del software StorageGRID 11.9

Dispositivos StorageGRID

Ir a "[Documentación del dispositivo StorageGRID](#)" para aprender a instalar, configurar y mantener dispositivos de almacenamiento y servicios StorageGRID .

Notas de la versión

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

Inicie sesión en el sitio de soporte de NetApp para ["ver o descargar un archivo PDF"](#) Contiene las notas de la versión de StorageGRID 11.9.

Comience a utilizar un sistema StorageGRID

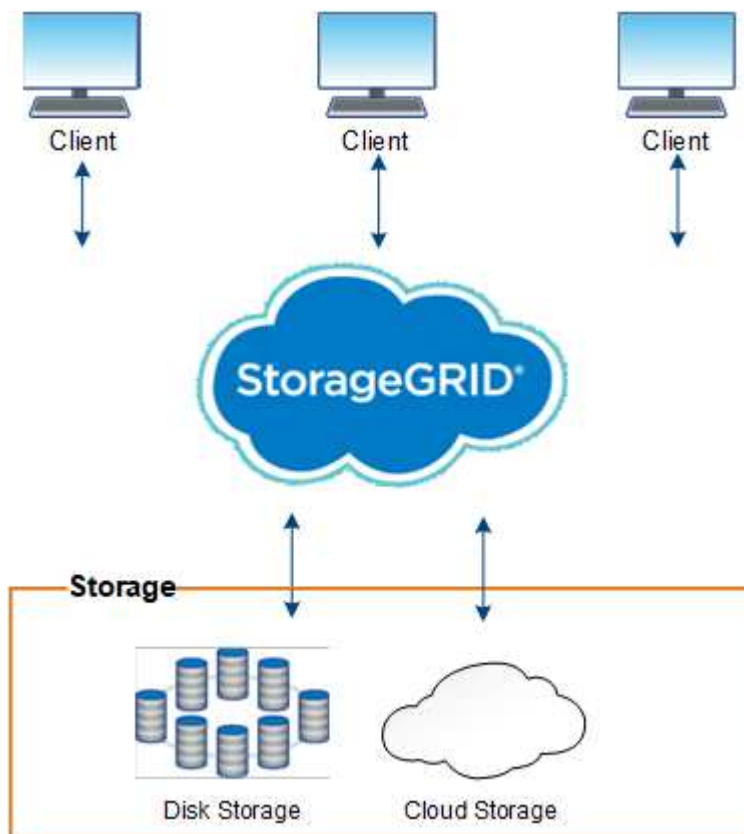
Obtenga más información sobre StorageGRID

¿Qué es StorageGRID?

NetApp® StorageGRID® es una suite de almacenamiento de objetos definido por software que admite una amplia gama de casos de uso en entornos multicloud públicos, privados e híbridos. StorageGRID ofrece soporte nativo para la API de Amazon S3 y brinda innovaciones líderes en la industria, como administración automatizada del ciclo de vida para almacenar, proteger, asegurar y preservar datos no estructurados de manera rentable durante períodos prolongados.

StorageGRID proporciona almacenamiento seguro y duradero para datos no estructurados a escala. Las políticas de gestión del ciclo de vida integradas y basadas en metadatos optimizan dónde residen sus datos a lo largo de su vida. El contenido se coloca en el lugar correcto, en el momento correcto y en el nivel de almacenamiento correcto para reducir costos.

StorageGRID está compuesto de nodos redundantes, heterogéneos y distribuidos geográficamente, que pueden integrarse con aplicaciones cliente existentes y de próxima generación.



Se ha eliminado el soporte para nodos de archivo. El traslado de objetos desde un nodo de archivo a un sistema de almacenamiento de archivo externo a través de la API S3 ha sido reemplazado por "[Grupos de almacenamiento en la nube de ILM](#)", que ofrecen más funcionalidad.

Beneficios de StorageGRID

Las ventajas del sistema StorageGRID incluyen las siguientes:

- Repositorio de datos distribuido geográficamente, masivo, escalable y fácil de usar para datos no estructurados.
- Protocolos estándar de almacenamiento de objetos:
 - Servicio de almacenamiento simple de Amazon Web Services (S3)
 - OpenStack Swift



La compatibilidad con aplicaciones cliente Swift ha quedado obsoleta y se eliminará en una versión futura.

- Nube híbrida habilitada. La gestión del ciclo de vida de la información (ILM) basada en políticas almacena objetos en nubes públicas, 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 nubes públicas.
- Protección de datos flexible para garantizar durabilidad y disponibilidad. Los datos se pueden proteger mediante replicación y codificación de borrado en capas. La verificación de datos en reposo y en vuelo garantiza la integridad para la retención a largo plazo.
- Gestión dinámica del ciclo de vida de los datos para ayudar a gestionar los costes de almacenamiento. Puede crear reglas ILM que administren el ciclo de vida de los datos a nivel de objeto, personalizando la localidad de los datos, la durabilidad, el rendimiento, el costo y el tiempo de retención.
- Alta disponibilidad de almacenamiento de datos y algunas funciones de gestión, con equilibrio de carga integrado para optimizar la carga de datos en los recursos de StorageGRID .
- Compatibilidad con múltiples cuentas de inquilinos de almacenamiento para segregar los objetos almacenados en su sistema por diferentes entidades.
- Numerosas herramientas para supervisar el estado de su sistema StorageGRID , incluido un sistema de alerta integral, un panel gráfico y estados detallados de todos los nodos y sitios.
- Soporte para implementación basada en software o hardware. Puede implementar StorageGRID en cualquiera de los siguientes:
 - Máquinas virtuales ejecutándose en VMware.
 - Motores de contenedores en hosts Linux.
 - Dispositivos diseñados por StorageGRID .
 - Los dispositivos de almacenamiento proporcionan almacenamiento de objetos.
 - Los dispositivos de servicios proporcionan servicios de administración de red y equilibrio de carga.
- Cumplimiento de los requisitos de almacenamiento pertinentes de esta normativa:
 - Comisión de Bolsa y Valores (SEC) en 17 CFR § 240.17a-4(f), que regula a los miembros de la bolsa, corredores o distribuidores.
 - Regla 4511(c) de la Autoridad Reguladora de la Industria Financiera (FINRA), que se remite a los requisitos de formato y medios de la Regla 17a-4(f) de la SEC.
 - Comisión de Comercio de Futuros de Productos Básicos (CFTC) en la regulación 17 CFR § 1.31(c)-(d), que regula el comercio de futuros de productos básicos.
- Operaciones de actualización y mantenimiento sin interrupciones. Mantener el acceso al contenido durante los procedimientos de actualización, expansión, desmantelamiento y mantenimiento.

- Gestión de identidad federada. Se integra con Active Directory, OpenLDAP o Oracle Directory Service para la autenticación de usuarios. Admite el inicio de sesión único (SSO) mediante 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).

Nubes híbridas con StorageGRID

Utilice StorageGRID en una configuración de nube híbrida implementando una gestión de datos basada en políticas para almacenar objetos en grupos de almacenamiento en la nube, aprovechando los servicios de la plataforma StorageGRID y clasificando los datos de ONTAP a StorageGRID con NetApp FabricPool.

Grupos de almacenamiento en la nube

Los grupos de almacenamiento en la nube le permiten almacenar objetos fuera del sistema StorageGRID . Por ejemplo, es posible que desee mover objetos a los que se accede con poca frecuencia a un almacenamiento en la nube de menor costo, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o el nivel de acceso de archivo en el almacenamiento de blobs de Microsoft Azure. O bien, es posible que desee mantener una copia de seguridad en la nube de los objetos StorageGRID , que se puede utilizar para recuperar datos perdidos debido a una falla del volumen de almacenamiento o del nodo de almacenamiento.

También se admite el almacenamiento de socios de terceros, incluido el almacenamiento en disco y en cinta.



No se admite el uso de grupos de almacenamiento en la nube con FabricPool debido a la latencia adicional para recuperar un objeto del destino del grupo de almacenamiento en la nube.

Servicios de la plataforma S3

Los servicios de la plataforma S3 le brindan la posibilidad de utilizar servicios remotos como puntos finales para la replicación de objetos, notificaciones de eventos o integración de búsqueda. Los servicios de plataforma funcionan independientemente de las reglas ILM de la red y están habilitados para depósitos S3 individuales. Se admiten los siguientes servicios:

- El servicio de replicación CloudMirror refleja automáticamente objetos específicos en un bucket S3 de destino, que puede estar en Amazon S3 o en un segundo sistema StorageGRID .
- El servicio de notificación de eventos envía mensajes sobre acciones específicas a un punto final externo que admite la recepción de eventos del Servicio de notificación simple (Amazon SNS).
- El servicio de integración de búsqueda envía metadatos de objetos a un servicio Elasticsearch externo, lo que permite buscar, visualizar y analizar metadatos utilizando herramientas de terceros.

Por ejemplo, puede utilizar la replicación de CloudMirror para reflejar registros de clientes específicos en Amazon S3 y luego aprovechar los servicios de AWS para realizar análisis de sus datos.

Clasificación de datos de ONTAP mediante FabricPool

Puede reducir el costo del almacenamiento de ONTAP al organizar los datos en StorageGRID mediante FabricPool. FabricPool permite la clasificación automatizada de datos en niveles de almacenamiento de objetos de bajo costo, ya sea dentro o fuera de las instalaciones.

A diferencia de las soluciones de niveles manuales, FabricPool reduce el costo total de propiedad al

automatizar la clasificación de datos para reducir el costo de almacenamiento. Ofrece los beneficios de la economía de la nube mediante la clasificación en nubes públicas y privadas, incluido StorageGRID.

Información relacionada

- ["¿Qué es Cloud Storage Pool?"](#)
- ["Administrar los servicios de la plataforma"](#)
- ["Configurar StorageGRID para FabricPool"](#)

Arquitectura y topología de red de StorageGRID

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

Ver el ["descripciones de los tipos de nodos de la cuadrícula"](#) .

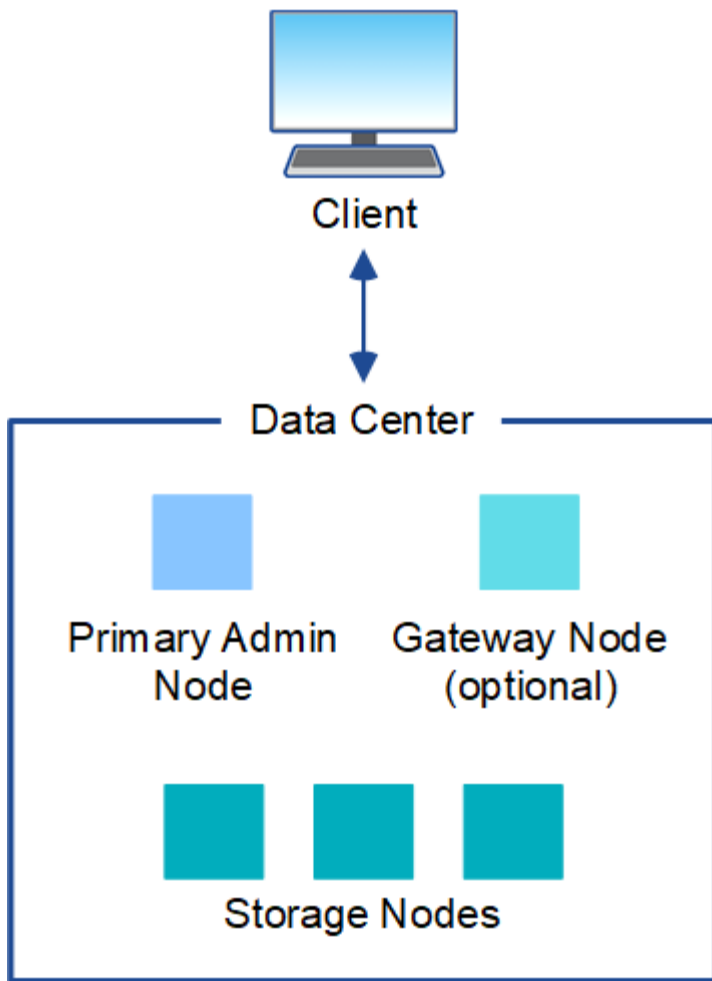
Para obtener información adicional sobre la topología de red, los requisitos y las comunicaciones de red de StorageGRID , consulte ["Pautas para establecer redes"](#) .

Topologías de implementación

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

Sitio único

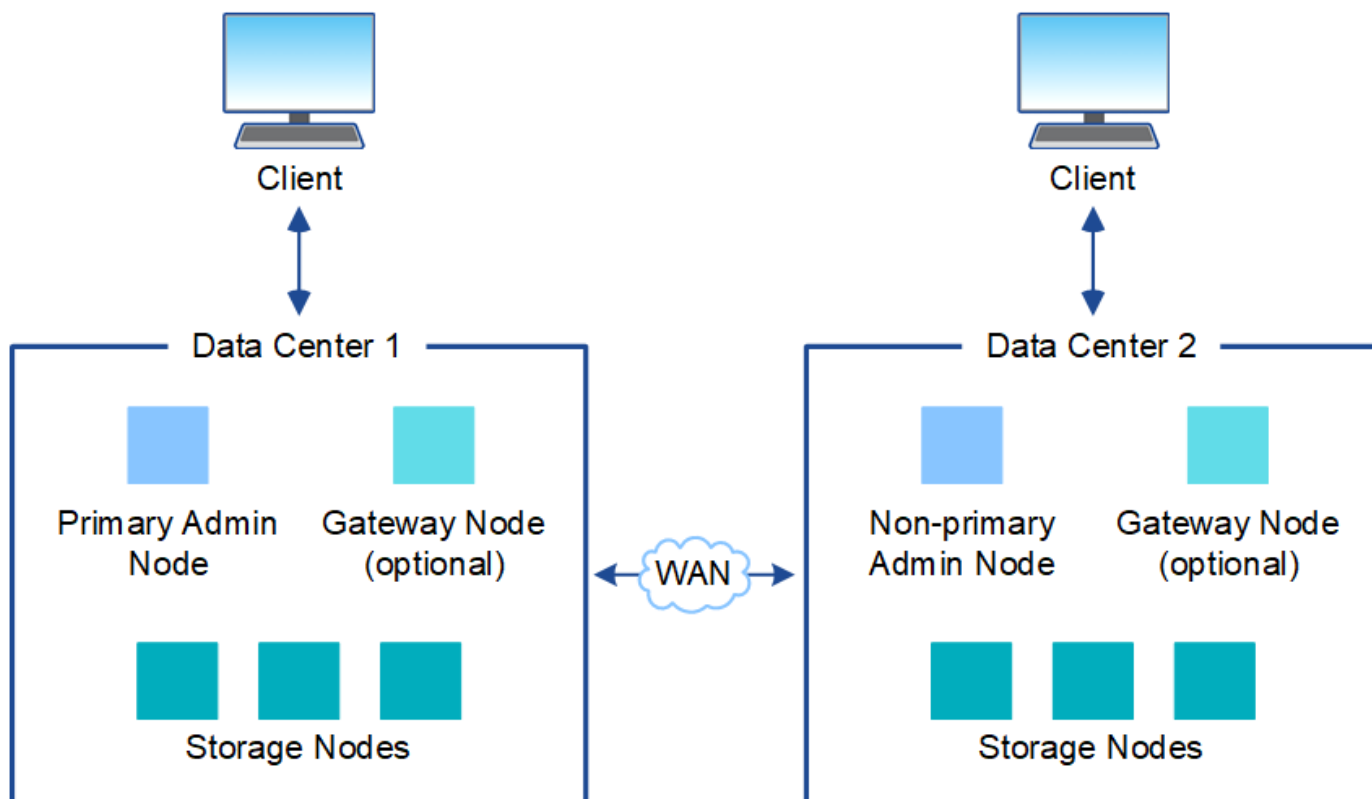
En una implementación con un solo sitio, la infraestructura y las operaciones del sistema StorageGRID están centralizadas.



Múltiples sitios

En una implementación con varios sitios, se pueden instalar distintos tipos y cantidades de recursos StorageGRID en cada sitio. Por ejemplo, podría requerirse más almacenamiento en un centro de datos que en otro.

A menudo, los distintos sitios se ubican en lugares geográficamente diferentes a lo largo de distintos dominios de falla, como una falla sísmica o una llanura aluvial. El intercambio de datos y la recuperación ante desastres se logran mediante la distribución automatizada de datos a otros sitios.



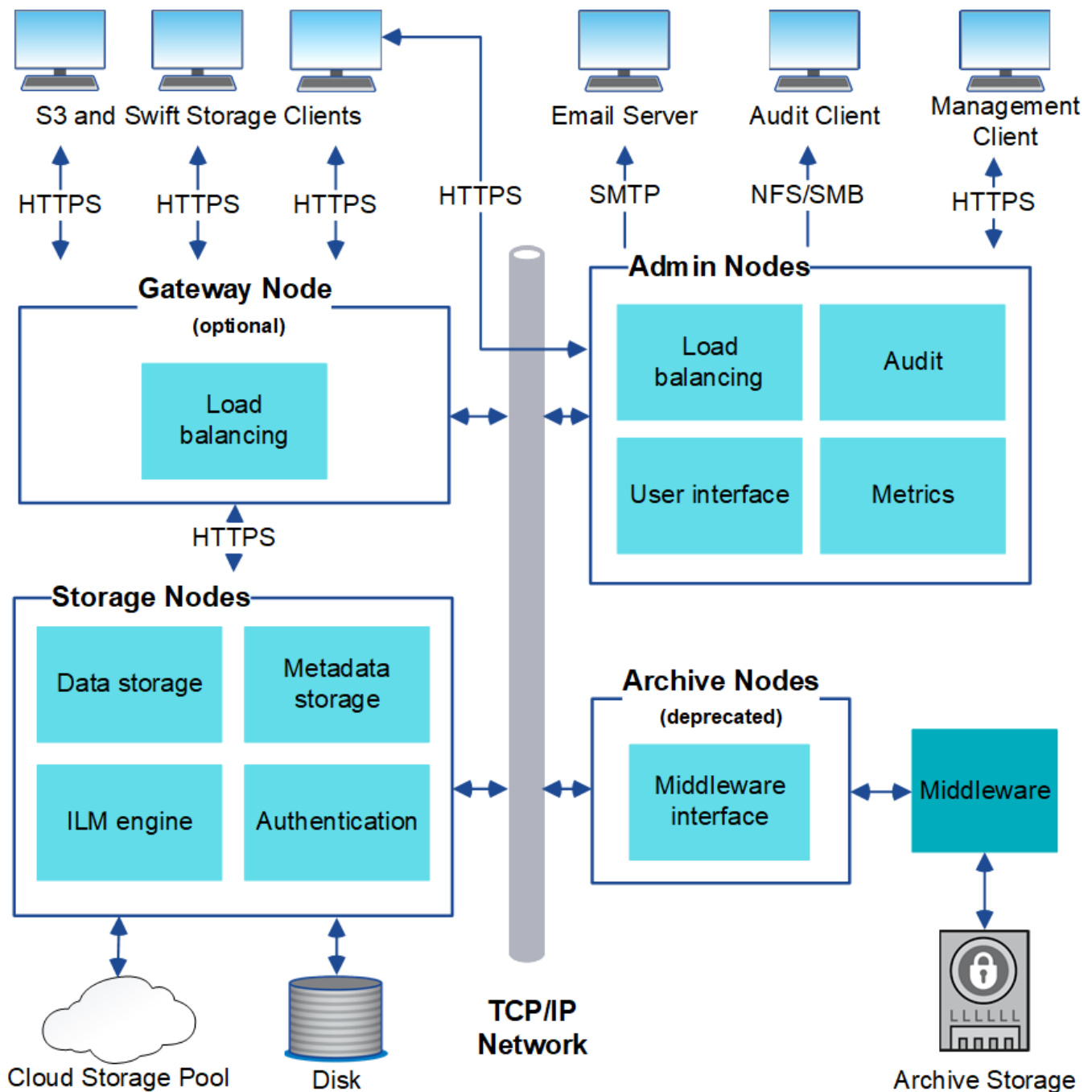
También pueden existir múltiples sitios lógicos dentro de un solo centro de datos para permitir el uso de replicación distribuida y codificación de borrado para aumentar la disponibilidad y la resiliencia.

Redundancia de nodos de red

En una implementación de un solo sitio o de varios sitios, puede incluir opcionalmente más de un nodo de administración o nodo de puerta de enlace para 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 administración principal.

Arquitectura del sistema

Este diagrama muestra cómo se organizan los nodos de la red dentro de un sistema StorageGRID .



Los clientes S3 almacenan y recuperan objetos en StorageGRID. Se utilizan otros clientes para enviar notificaciones por correo electrónico, acceder a la interfaz de administración de StorageGRID y, opcionalmente, acceder al recurso compartido de auditoría.

Los clientes S3 pueden conectarse a un nodo de puerta de enlace o a un nodo de administración para utilizar la interfaz de equilibrio de carga para los nodos de almacenamiento. Alternativamente, los clientes S3 pueden conectarse directamente a los nodos de almacenamiento mediante HTTPS.

Los objetos se pueden almacenar dentro de StorageGRID en nodos de almacenamiento basados en software o hardware, o en grupos de almacenamiento en la nube, que consisten en depósitos S3 externos o contenedores de almacenamiento de blobs de Azure.

Nodos y servicios de la red

Nodos y servicios de la red

El componente básico de un sistema StorageGRID es el nodo de la red. Los nodos contienen servicios, que son módulos de software que proporcionan un conjunto de capacidades a un nodo de la red.

Tipos de nodos de la red

El sistema StorageGRID utiliza cuatro tipos de nodos de red:

Nodos de administración

Proporcionar servicios de gestión como configuración del sistema, supervisión y registro. Cuando inicia sesión en Grid Manager, se conecta a un nodo de administración. Cada red debe tener un nodo de administración principal y puede tener nodos de administración no principales adicionales para redundancia. Puede conectarse a cualquier nodo de administración y cada nodo de administración muestra una vista similar del sistema StorageGRID. Sin embargo, los procedimientos de mantenimiento deben realizarse utilizando el nodo de administración principal.

Los nodos de administración también se pueden utilizar para equilibrar la carga del tráfico del cliente S3.

Ver "[¿Qué es un nodo de administración?](#)"

Nodos de almacenamiento

Administrar y almacenar datos de objetos y metadatos. Cada sitio de su sistema StorageGRID debe tener al menos tres nodos de almacenamiento.

Ver "[¿Qué es un nodo de almacenamiento?](#)"

Nodos de puerta de enlace (opcionales)

Proporciona una interfaz de equilibrio de carga que las aplicaciones cliente puedan usar para conectarse a StorageGRID. Un balanceador de carga dirige sin problemas a los clientes a un nodo de almacenamiento óptimo, de modo que la falla de los nodos o incluso de un sitio completo sea transparente.

Ver "[¿Qué es un nodo de enlace?](#)"

Nodos de hardware y software

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

Nodos de dispositivos StorageGRID

Los dispositivos de hardware StorageGRID están diseñados especialmente para su uso en un sistema StorageGRID. Algunos dispositivos pueden utilizarse como nodos de almacenamiento. Se pueden utilizar otros dispositivos como nodos de administración o nodos de puerta de enlace. Puede combinar nodos de dispositivos con nodos basados en software o implementar redes de dispositivos completamente diseñadas que no dependan de hipervisores externos, almacenamiento o hardware de cómputo.

Consulte lo siguiente para obtener información sobre los electrodomésticos disponibles:

- "[Documentación del dispositivo StorageGRID](#)"

- ["NetApp Hardware Universe"](#)

Nodos basados en software

Los nodos de red basados en software se pueden implementar como máquinas virtuales VMware o dentro de motores de contenedores en un host Linux.

- Máquina virtual (VM) en VMware vSphere: consulte ["Instalar StorageGRID en VMware"](#) .
- Dentro de un motor de contenedores en Red Hat Enterprise Linux: Ver ["Instalar StorageGRID en Red Hat Enterprise Linux"](#) .
- Dentro de un motor de contenedores en Ubuntu o Debian: Ver ["Instalar StorageGRID en Ubuntu o Debian"](#) .

Utilice el ["Herramienta de matriz de interoperabilidad de NetApp \(IMT\)"](#) para determinar las versiones compatibles.

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

Servicios de StorageGRID

La siguiente es una lista completa de los servicios de StorageGRID .

Servicio	Descripción	Ubicación
Reenvío de servicios de cuenta	Proporciona una interfaz para que el servicio Load Balancer consulte al servicio de cuenta en hosts remotos y proporciona notificaciones de cambios de configuración del punto final de Load Balancer al servicio Load Balancer.	Servicio de balanceador de carga en nodos de administración y nodos de puerta de enlace
ADC (Controlador de dominio administrativo)	Mantiene la información de topología, proporciona servicios de autenticación y responde a las consultas de los servicios LDR y CMN.	Al menos tres nodos de almacenamiento que contienen el servicio ADC en cada sitio
AMS (Sistema de Gestión de Auditoría)	Supervisa y registra todos los eventos y transacciones del sistema auditados en un archivo de registro de texto.	Nodos de administración
Cassandra Reaper	Realiza reparaciones automáticas de metadatos de objetos.	Nodos de almacenamiento
Servicio de fragmentos	Gestiona datos codificados por borrado y fragmentos de paridad.	Nodos de almacenamiento
CMN (Nodo de gestión de configuración)	Gestiona configuraciones de todo el sistema y tareas de la red. Cada red tiene un servicio CMN.	Nodo de administración principal

Servicio	Descripción	Ubicación
DDS (Almacén de datos distribuidos)	Interfaces con la base de datos Cassandra para administrar metadatos de objetos.	Nodos de almacenamiento
DMV (Transportador de datos)	Mueve datos a puntos finales en la nube.	Nodos de almacenamiento
IP dinámica (dynip)	Supervisa la red para detectar cambios dinámicos de IP y actualiza las configuraciones locales.	Todos los nodos
Grafana	Se utiliza para la visualización de métricas en el Administrador de cuadrícula.	Nodos de administración
Alta disponibilidad	Administra direcciones IP virtuales de alta disponibilidad en los nodos configurados en la página Grupos de alta disponibilidad. Este servicio también se conoce como servicio keepalived.	Nodos de administración y de puerta de enlace
Identidad (idnt)	Federa identidades de usuarios de LDAP y Active Directory.	Nodos de almacenamiento que utilizan el servicio ADC
Árbitro Lambda	Administra solicitudes SelectObjectContent de S3 Select.	Todos los nodos
Balanceador de carga (nginx-gw)	Proporciona equilibrio de carga del tráfico S3 desde los clientes a los nodos de almacenamiento. El servicio Load Balancer se puede configurar a través de la página de configuración de puntos finales de Load Balancer. Este servicio también se conoce como servicio nginx-gw.	Nodos de administración y de puerta de enlace
LDR (Enrutador de distribución local)	Gestiona el almacenamiento y la transferencia de contenido dentro de la red.	Nodos de almacenamiento
Demonio de control del servicio de información MISCd	Proporciona una interfaz para consultar y administrar servicios en otros nodos y para administrar configuraciones ambientales en el nodo, como consultar el estado de los servicios que se ejecutan en otros nodos.	Todos los nodos
nginx	Actúa como un mecanismo de autenticación y comunicación segura para varios servicios de red (como Prometheus y Dynamic IP) para poder comunicarse con servicios en otros nodos a través de API HTTPS.	Todos los nodos

Servicio	Descripción	Ubicación
nginx-gw	Alimenta el servicio Load Balancer.	Nodos de administración y de puerta de enlace
NMS (Sistema de gestión de red)	Potencia las opciones de monitoreo, informes y configuración que se muestran a través del Administrador de cuadrícula.	Nodos de administración
Persistencia	Administra archivos en el disco raíz que deben persistir luego de un reinicio.	Todos los nodos
Prometeo	Recopila métricas de series temporales de los servicios en todos los nodos.	Nodos de administración
RSM (Máquina de estados replicada)	Garantiza que las solicitudes de servicio de la plataforma se envíen a sus respectivos puntos finales.	Nodos de almacenamiento que utilizan el servicio ADC
SSM (Monitor de estado del servidor)	Supervisa las condiciones del hardware y las informa al servicio NMS.	Hay una instancia presente en cada nodo de la red
Recolector de trazas	Realiza la recopilación de seguimiento para reunir información para uso del soporte técnico. El servicio de recopilación de rastros utiliza software Jaeger de código abierto.	Nodos de administración

¿Qué es un nodo de administración?

Los nodos de administración brindan servicios de gestión como configuración del sistema, monitoreo y registro. Los nodos de administración también se pueden utilizar para equilibrar la carga del tráfico del cliente S3. Cada red debe tener un nodo de administración principal y puede tener cualquier cantidad de nodos de administración no principales para redundancia.

Diferencias entre nodos de administración primarios y no primarios

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

La tabla resume las capacidades de los nodos de administración primarios y no primarios.

Capacidades	Nodo de administración principal	Nodo de administración no principal
Incluye el AMS servicio	Sí	Sí

Capacidades	Nodo de administración principal	Nodo de administración no principal
Incluye elCMN servicio	Sí	No
Incluye elNuevos Estados Miembros servicio	Sí	Sí
Incluye elPrometeo servicio	Sí	Sí
Incluye elSSM servicio	Sí	Sí
Incluye elBalanceador de carga yAlta disponibilidad servicios	Sí	Sí
Apoya elInterfaz del programa de aplicación de gestión (API de gestión)	Sí	Sí
Se puede utilizar para todas las tareas de mantenimiento relacionadas con la red, por ejemplo, cambio de dirección IP y actualización de servidores NTP.	Sí	No
Puede realizar el reequilibrio de EC después de la expansión del nodo de almacenamiento	Sí	No
Se puede utilizar para el procedimiento de restauración de volumen.	Sí	Sí
Puede recopilar archivos de registro y datos del sistema de uno o más nodos	Sí	No
Envía notificaciones de alerta, paquetes de AutoSupport y trampas SNMP e informa	Sí. Actúa como elremite nte preferido .	Sí. Actúa como un remitente en espera.

Nodo de administración del remitente preferido

Si su implementación de StorageGRID incluye varios nodos de administración, el nodo de administración principal es el remitente preferido para notificaciones de alerta, paquetes de AutoSupport y trampas e informes SNMP.

En condiciones normales de funcionamiento del sistema, sólo el remitente preferido envía notificaciones. Sin embargo, todos los demás nodos de administración monitorean al remitente preferido. Si se detecta un problema, otros nodos de administración actúan como *remitentes en espera*.

Es posible que se envíen múltiples notificaciones en estos casos:

- Si los nodos de administración quedan "aislados" unos de otros, tanto el remitente preferido como los remitentes en espera intentarán enviar notificaciones y se podrían recibir múltiples copias de las notificaciones.

- Si el remitente en espera detecta problemas con el remitente preferido y comienza a enviar notificaciones, el remitente preferido podría recuperar 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 los paquetes de AutoSupport, todos los nodos de administración envían la prueba. Al probar las notificaciones de alerta, debe iniciar sesión en cada nodo de administración para verificar la conectividad.

Servicios principales para nodos de administración

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

Servicio	Función de tecla
Sistema de Gestión de Auditorías (AMS)	Realiza un seguimiento de la actividad y los eventos del sistema.
Nodo de gestión de configuración (CMN)	Gestiona la configuración de todo el sistema.
[[alta disponibilidad]]Alta disponibilidad	Administra direcciones IP virtuales de alta disponibilidad para grupos de nodos de administración y nodos de puerta de enlace. Nota: Este servicio también se encuentra en los nodos Gateway.
Balanceador de carga	Proporciona equilibrio de carga del tráfico S3 desde los clientes a los nodos de almacenamiento. Nota: Este servicio también se encuentra en los nodos Gateway.
Interfaz de programación de aplicaciones de gestión (mgmt-api)	Procesa solicitudes de la API de administración de red y de la API de administración de inquilinos.
Sistema de gestión de red (NMS)	Proporciona funcionalidad para el administrador de cuadrícula.
Prometeo	Recopila y almacena métricas de series temporales de los servicios en todos los nodos.
Monitor de estado del servidor (SSM)	Supervisa el sistema operativo y el hardware subyacente.

¿Qué es un nodo de almacenamiento?

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

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

Tipos de nodos de almacenamiento

Durante la instalación, puede seleccionar el tipo de nodo de almacenamiento que desea instalar. Estos tipos están disponibles para nodos de almacenamiento basados en software y para nodos de almacenamiento basados en dispositivos que admiten la función:

- Nodo de almacenamiento de datos y metadatos combinados
- Nodo de almacenamiento solo de metadatos
- Nodo de almacenamiento de solo datos

Puede seleccionar el tipo de nodo de almacenamiento en estas situaciones:

- Al instalar inicialmente un nodo de almacenamiento
- Cuando agrega un nodo de almacenamiento durante la expansión del sistema StorageGRID



No es posible cambiar el tipo una vez finalizada la instalación del nodo de almacenamiento.

Nodo de almacenamiento de datos y metadatos (combinado)

De forma predeterminada, todos los nodos de almacenamiento nuevos almacenarán datos de objetos y metadatos. Este tipo de nodo de almacenamiento se denomina nodo de almacenamiento *combinado*.

Nodo de almacenamiento solo de metadatos

Usar un nodo de almacenamiento exclusivamente para metadatos puede tener sentido si su red almacena una gran cantidad de objetos pequeños. La instalación de capacidad de metadatos dedicada proporciona un mejor equilibrio entre el espacio necesario para una gran cantidad de objetos pequeños y el espacio necesario para los metadatos de esos objetos. Además, los nodos de almacenamiento de solo metadatos alojados en dispositivos de alto rendimiento pueden aumentar el rendimiento.

Los nodos de almacenamiento de solo metadatos tienen requisitos de hardware específicos:

- Al utilizar dispositivos StorageGRID, los nodos de solo metadatos se pueden configurar únicamente en dispositivos SGF6112 con doce unidades de 1,9 TB o doce unidades de 3,8 TB.
- Al utilizar nodos basados en software, los recursos de nodo de solo metadatos deben coincidir con los recursos de los nodos de almacenamiento existentes. Por ejemplo:
 - Si el sitio StorageGRID existente utiliza dispositivos SG6000 o SG6100, los nodos de solo metadatos basados en software deben cumplir los siguientes requisitos mínimos:
 - 128 GB de RAM
 - CPU de 8 núcleos
 - SSD de 8 TB o almacenamiento equivalente para la base de datos Cassandra (rangedb/0)
 - Si el sitio StorageGRID existente usa nodos de almacenamiento virtuales con 24 GB de RAM, CPU de 8 núcleos y 3 TB o 4 TB de almacenamiento de metadatos, los nodos solo de metadatos basados en software deben usar recursos similares (24 GB de RAM, CPU de 8 núcleos y 4 TB de almacenamiento de metadatos (rangedb/0)).
- Al agregar un nuevo sitio StorageGRID, la capacidad total de metadatos del nuevo sitio debe coincidir, como mínimo, con los sitios StorageGRID existentes y los recursos del nuevo sitio deben coincidir con los nodos de almacenamiento de los sitios StorageGRID existentes.

Al instalar nodos de solo metadatos, la cuadrícula también debe contener una cantidad mínima de nodos para

el almacenamiento de datos:

- Para una cuadrícula de un solo sitio, configure al menos dos nodos de almacenamiento combinados o de solo datos.
- Para una cuadrícula de varios sitios, configure al menos un nodo de almacenamiento combinado o de solo datos *por sitio*.



Aunque los nodos de almacenamiento de solo metadatos contienen [Servicio LDR](#) y puede procesar solicitudes de clientes S3, es posible que el rendimiento de StorageGRID no aumente.

Nodo de almacenamiento de solo datos

Usar un nodo de almacenamiento exclusivamente para datos puede tener sentido si sus nodos de almacenamiento tienen diferentes características de rendimiento. Por ejemplo, para aumentar potencialmente el rendimiento, podría tener nodos de almacenamiento de disco giratorio de alta capacidad y solo datos acompañados de nodos de almacenamiento de alto rendimiento y solo metadatos.

Al instalar nodos de solo datos, la cuadrícula debe contener lo siguiente:

- Un mínimo de dos nodos de almacenamiento combinados o de solo datos *por red*
- Al menos un nodo de almacenamiento combinado o de solo datos *por sitio*
- Un mínimo de tres nodos de almacenamiento combinados o de solo metadatos *por sitio*

Servicios principales para nodos de almacenamiento

La siguiente tabla muestra los servicios principales para 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 existen solo en tres nodos de almacenamiento en cada sitio.

Servicio	Función de tecla
Cuenta (acct)	Administra las cuentas de los inquilinos.

Servicio	Función de tecla
Controlador de dominio administrativo (ADC)	Mantiene la topología y la configuración de toda la red. Nota: Los nodos de almacenamiento de solo datos no alojan el servicio ADC. Detalles El servicio del controlador de dominio administrativo (ADC) autentica los nodos de la red y sus conexiones entre sí. El servicio ADC está alojado en un mínimo de tres nodos de almacenamiento en un sitio. El servicio ADC mantiene información de topología, incluida la ubicación y la disponibilidad de los servicios. Cuando un nodo de la red requiere información de otro nodo de la red o que otro nodo de la red realice una acción, se comunica con un servicio ADC para encontrar el mejor nodo de la red para procesar su solicitud. Además, el servicio ADC conserva una copia de los paquetes de configuración de la implementación de StorageGRID , lo que permite que cualquier nodo de la red recupere la información de configuración actual. Para facilitar las operaciones distribuidas e aisladas, cada servicio ADC sincroniza certificados, paquetes de configuración e información sobre servicios y topología con los demás servicios ADC en el sistema StorageGRID . En general, todos los nodos de la red mantienen una conexión a al menos un servicio ADC. Esto garantiza que los nodos de la red siempre tengan acceso a la información más reciente. Cuando los nodos de la red se conectan, almacenan en caché los certificados de otros nodos de la red, lo que permite que los sistemas sigan funcionando con los nodos de la red conocidos incluso cuando un servicio ADC no está disponible. Los nuevos nodos de la red solo pueden establecer conexiones mediante un servicio ADC. La conexión de cada nodo de la red permite que el servicio ADC recopile información de topología. Esta información del nodo de la red incluye la carga de la CPU, el espacio en disco disponible (si tiene almacenamiento), los servicios admitidos y el ID del sitio del nodo de la red. Otros servicios solicitan al servicio ADC información de topología a través de consultas de topología. El servicio ADC responde a cada consulta con la última información recibida del sistema StorageGRID .
Cassandra	Almacena y protege los metadatos de los objetos. Nota: Los nodos de almacenamiento de solo datos no alojan el servicio Cassandra.
Cassandra Reaper	Realiza reparaciones automáticas de metadatos de objetos. Nota: Los nodos de almacenamiento de solo datos no alojan el servicio Cassandra Reaper.

Servicio	Función de tecla
Pedazo	Gestiona datos codificados por borrado y fragmentos de paridad.
Transportador de datos (dmv)	Mueve datos a grupos de almacenamiento en la nube.
Almacén de datos distribuidos (DDS)	Supervisa el almacenamiento de metadatos de objetos. Detalles Cada nodo de almacenamiento incluye el servicio de almacén de datos distribuidos (DDS). Este servicio interactúa con la base de datos Cassandra para realizar tareas en segundo plano en los metadatos de objetos almacenados en el sistema StorageGRID . El servicio DDS rastrea la cantidad total de objetos ingeridos en el sistema StorageGRID , así como la cantidad total de objetos ingeridos a través de cada una de las interfaces compatibles del sistema (S3).
Identidad (idnt)	Federa identidades de usuarios de LDAP y Active Directory.

Servicio	Función de tecla
Enrutador de distribución local (LDR)	Procesa solicitudes de protocolo de almacenamiento de objetos y administra datos de objetos en el disco.

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

El servicio LDR realiza la mayor parte del trabajo pesado del sistema StorageGRID al manejar las cargas de transferencia de datos y las funciones de tráfico de datos.

¿Qué es un nodo de enlace?

Los nodos de puerta de enlace proporcionan una interfaz de equilibrio de carga dedicada que las aplicaciones cliente S3 pueden usar para conectarse a StorageGRID. El equilibrio de carga maximiza la velocidad y la capacidad de conexión al distribuir la carga de trabajo entre múltiples nodos de almacenamiento. Los nodos de puerta de enlace son opcionales.

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

Configura uno o más puntos finales del balanceador de carga para definir el puerto y el protocolo de red (HTTPS o HTTP) que las solicitudes de cliente entrantes y salientes utilizarán para acceder a los servicios del balanceador de carga en los nodos de puerta de enlace y de administración. El punto final del balanceador de carga también define el tipo de solicitudes de cliente permitidas o bloqueadas. Ver "Consideraciones para el equilibrio de carga".

Según sea necesario, puede agrupar las interfaces de red de varios nodos de puerta de enlace y nodos de administración en un grupo de alta disponibilidad (HA). Si la interfaz activa en el grupo HA falla, una interfaz de respaldo puede administrar la carga de trabajo de la aplicación cliente. Ver "Administrar grupos de alta disponibilidad (HA)".

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 los nodos.

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

Protección de metadatos

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

Para garantizar la redundancia y, por tanto, la protección contra pérdidas, se mantienen tres copias de los metadatos de los objetos en cada sitio. Esta replicación no es configurable y se realiza automáticamente. Para obtener más información, consulte "Administrar el almacenamiento de

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

¿Qué es un nodo de archivo?

Se ha eliminado el soporte para nodos de archivo.

Para obtener información sobre los nodos de archivo, consulte "[¿Qué es un nodo de archivo \(sitio de documentación de StorageGRID 11.8\)?](#)".

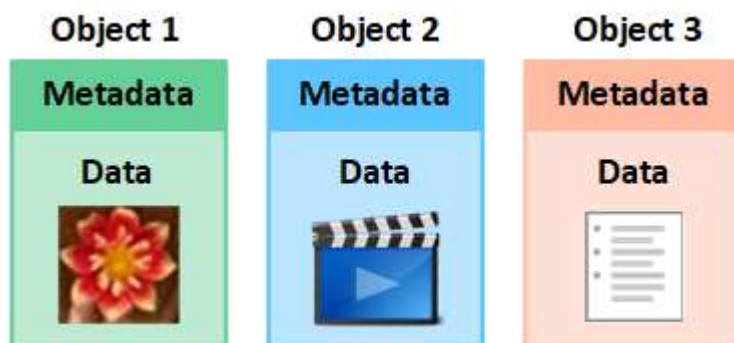
Cómo gestiona StorageGRID los datos

¿Qué es un objeto?

Con el almacenamiento de objetos, la unidad de almacenamiento es un objeto, en lugar de un archivo o un bloque. A diferencia de la jerarquía en forma de árbol de un sistema de archivos o de almacenamiento en bloques, el almacenamiento de objetos organiza los datos en un diseño plano y no estructurado.

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

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



¿Qué son los datos de objeto?

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

¿Qué son los metadatos de un objeto?

Los metadatos de un objeto son cualquier información que describe un objeto. StorageGRID utiliza metadatos de objetos para rastrear las ubicaciones de todos los objetos en la red y administrar el ciclo de vida de cada objeto a lo largo del tiempo.

Los metadatos de un objeto incluyen información como la siguiente:

- Metadatos del sistema, incluido un ID único para cada objeto (UUID), el nombre del objeto, el nombre del bucket S3 o del contenedor Swift, el nombre o ID de la cuenta del inquilino, el tamaño lógico del objeto, la fecha y hora en que se creó el objeto por primera vez y la fecha y hora en que se modificó el objeto por última vez.
- La ubicación de almacenamiento actual de cada copia de objeto o fragmento codificado de borrado.
- Cualquier metadato de usuario asociado con el objeto.

Los metadatos de los objetos son personalizables y ampliables, lo que hace que sean flexibles para que las aplicaciones los utilicen.

Para obtener información detallada sobre cómo y dónde StorageGRID almacena los metadatos de los objetos, vaya a ["Administrar el almacenamiento de metadatos de objetos"](#).

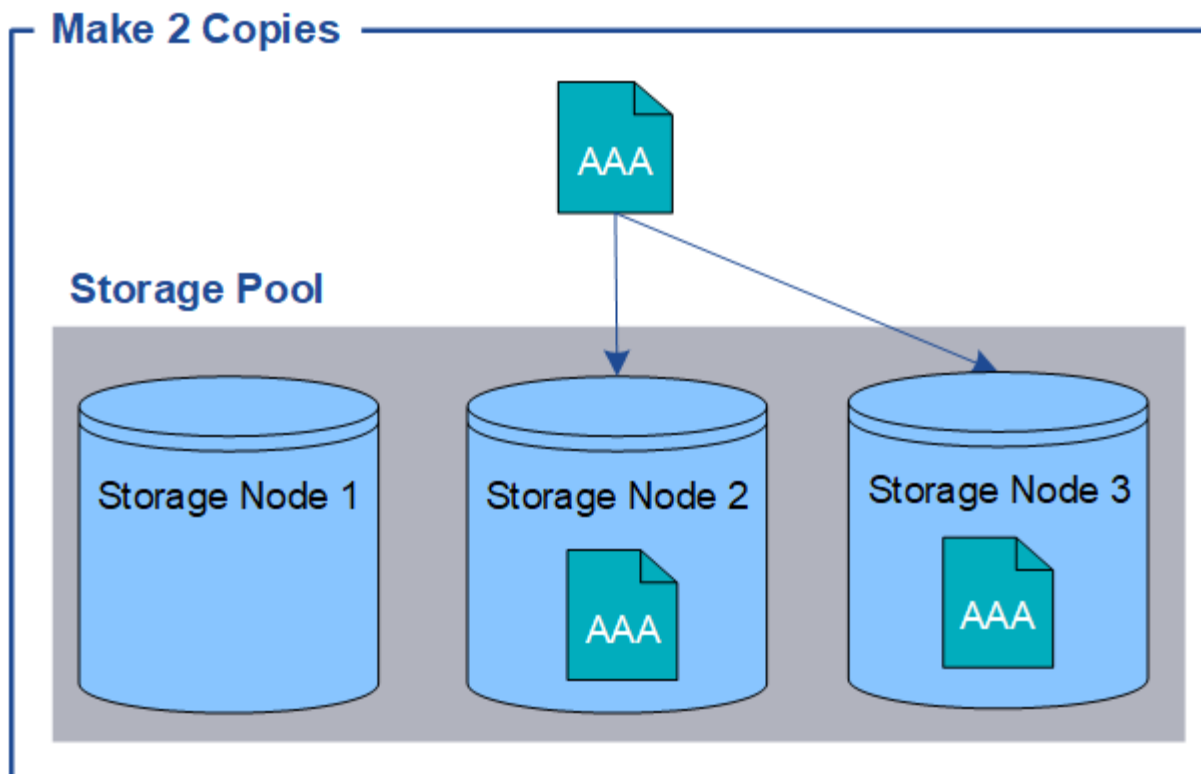
¿Cómo se protegen los datos de los objetos?

El sistema StorageGRID le proporciona dos mecanismos para proteger los datos de los objetos contra pérdidas: replicación y codificación de borrado.

Replicación

Cuando StorageGRID hace coincidir objetos con una regla de administración del ciclo de vida de la información (ILM) configurada para crear copias replicadas, el sistema crea copias exactas de los datos de los objetos y las almacena en nodos de almacenamiento o grupos de almacenamiento en la nube. Las reglas de ILM determinan la cantidad de copias que se realizan, dónde se almacenan dichas copias y durante cuánto tiempo las conserva el sistema. Si se pierde una copia, por ejemplo, como resultado de la pérdida de un nodo de almacenamiento, el objeto aún estará disponible si existe una copia del mismo en otra parte del sistema StorageGRID.

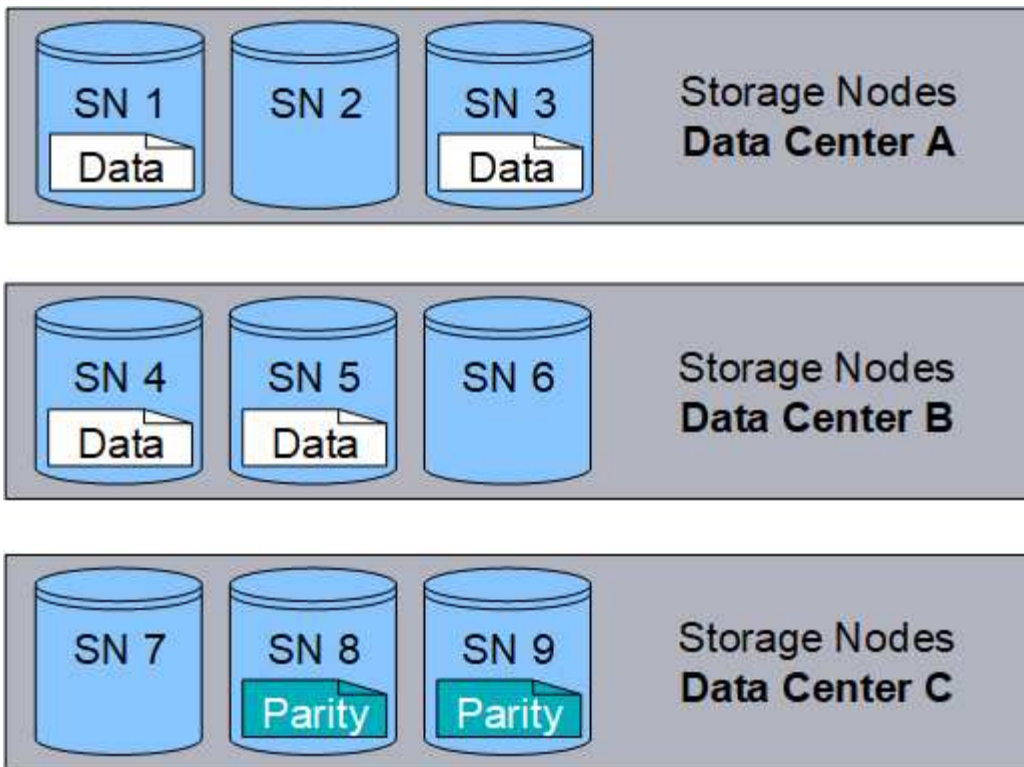
En el siguiente ejemplo, la regla Hacer 2 copias especifica que se coloquen dos copias replicadas de cada objeto en un grupo de almacenamiento que contiene tres nodos de almacenamiento.



Codificación de borrado

Cuando StorageGRID hace coincidir objetos con una regla ILM configurada para crear copias con código de borrado, divide los datos de los 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 fragmento de datos o de paridad se corrompe o se pierde, el algoritmo de codificación de borrado puede recrear ese fragmento utilizando un subconjunto de los fragmentos de datos y de paridad restantes. Las reglas ILM y los perfiles de codificación de borrado determinan el esquema de codificación de borrado utilizado.

El siguiente ejemplo ilustra el uso 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 se calculan dos fragmentos de paridad 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 brindar protección de datos ante fallas de nodos o pérdidas de sitios.



Información relacionada

- ["Administrar objetos con ILM"](#)
- ["Utilice la gestión del ciclo de vida de la información"](#)

La vida de un objeto

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

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

- **Ingesta:** El proceso por el cual una aplicación cliente S3 guarda un objeto a través de HTTP en el sistema StorageGRID. En esta etapa, el sistema StorageGRID comienza a administrar el objeto.
- **Administración de copias:** el proceso de administrar copias replicadas y codificadas por borrado en StorageGRID, como se describe en las reglas de ILM en las políticas de ILM activas. Durante la etapa de gestión de copias, StorageGRID protege los datos de los objetos contra pérdidas mediante la creación y el mantenimiento de la cantidad y el tipo especificados de copias de objetos en nodos de almacenamiento o en un grupo de almacenamiento en la nube.
- **Recuperar:** El proceso por el cual una aplicación cliente accede a un objeto almacenado por el sistema StorageGRID. El cliente lee el objeto, que se recupera de un nodo de almacenamiento o de un grupo de almacenamiento en la nube.
- **Eliminar:** El proceso de eliminar todas las copias de objetos de la cuadrícula. Los objetos se pueden eliminar como resultado de una solicitud de eliminación por parte de la aplicación cliente al sistema StorageGRID o como resultado de un proceso automático que StorageGRID realiza cuando expira la vida útil del objeto.



Información relacionada

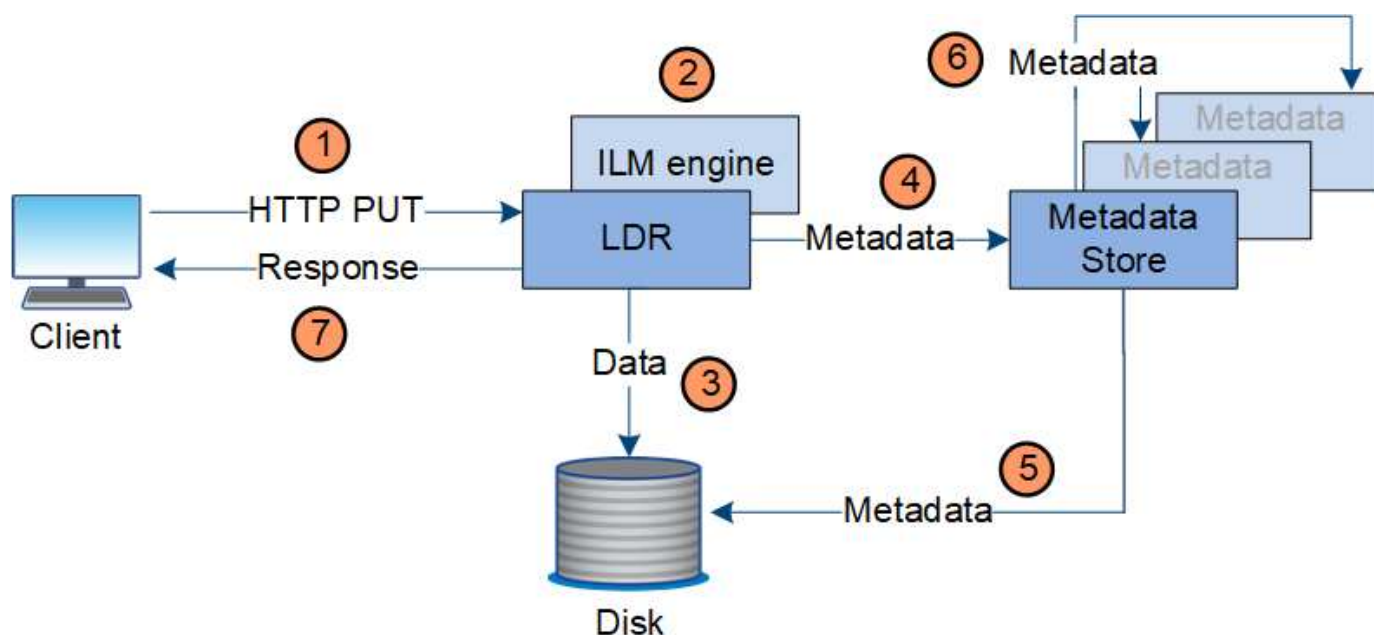
- ["Administrar objetos con ILM"](#)
- ["Utilice la gestión del ciclo de vida de la información"](#)

Flujo de ingesta de datos

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

Flujo de datos

Cuando un cliente ingiere un objeto en el 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 a través de una solicitud HTTP PUT.
2. El objeto se evalúa según la política ILM del sistema.
3. El servicio LDR guarda los datos del objeto como una copia replicada o como una copia con código de borrado. (El diagrama muestra una versión simplificada de cómo almacenar 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 se ha ingerido el objeto.

Gestión de copias

Los datos de los objetos se administran mediante las políticas ILM activas y las reglas ILM asociadas. Las reglas ILM realizan copias replicadas o con código de borrado para proteger los datos de los objetos contra pérdidas.

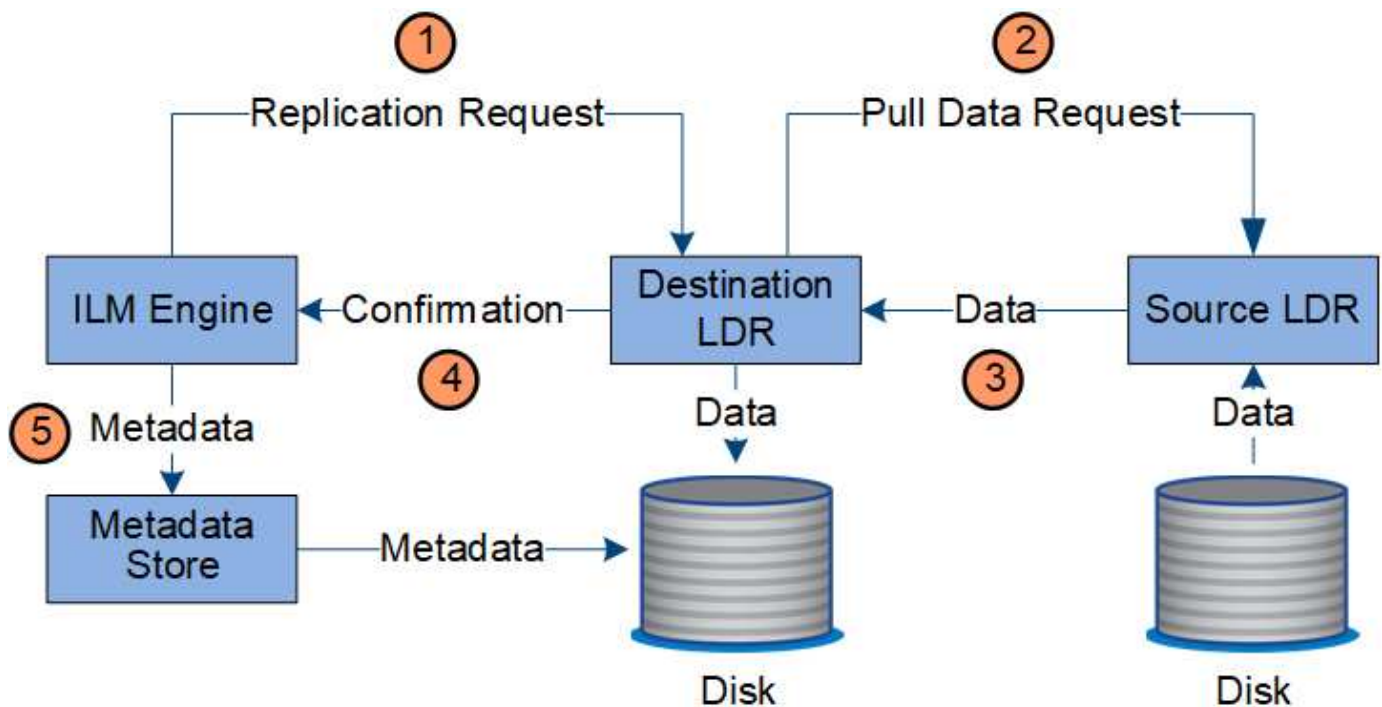
Es posible que se requieran distintos tipos o ubicaciones de copias de objetos en distintos momentos de la vida del objeto. Las reglas de ILM se evalúan periódicamente para garantizar que los objetos se coloquen según lo requerido.

Los datos de los objetos son administrados por el servicio LDR.

Protección de contenido: replicación

Si las instrucciones de ubicación de contenido de una regla ILM requieren copias replicadas de datos de objetos, los nodos de almacenamiento que conforman el grupo de almacenamiento configurado realizan copias y las almacenan en el disco.

El motor ILM del servicio LDR controla la replicación y garantiza que se almacene la cantidad correcta de copias en las ubicaciones correctas y durante el tiempo correcto.



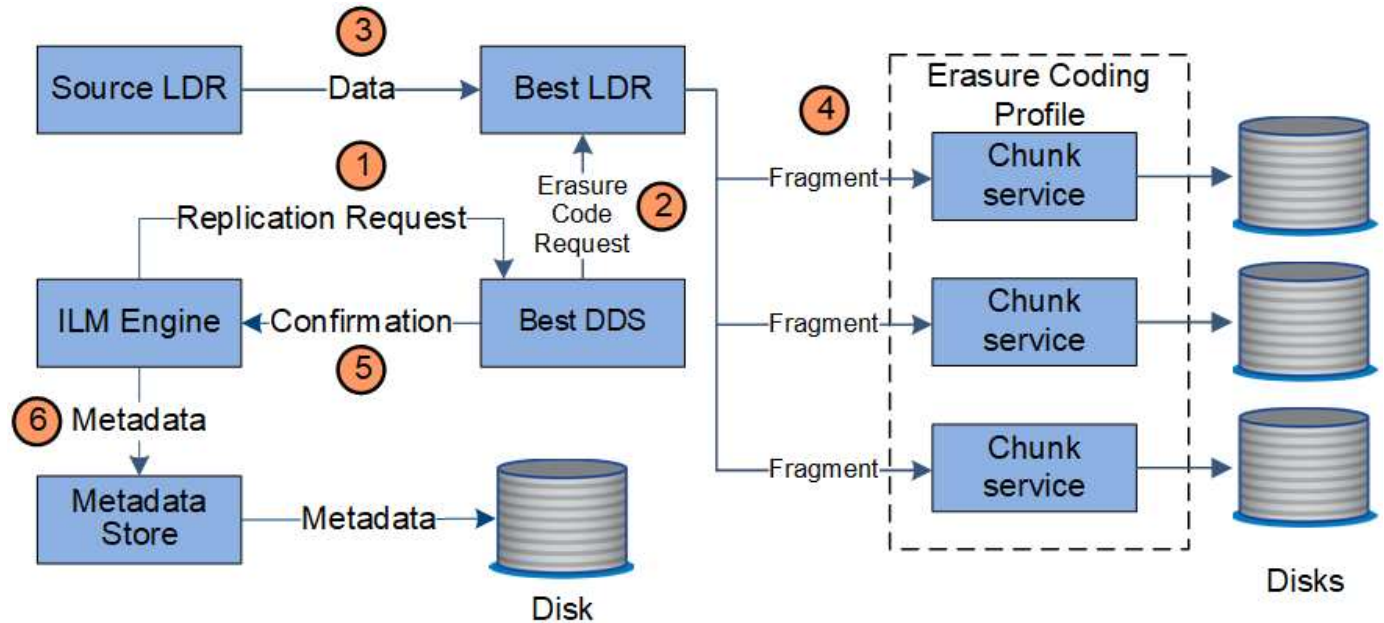
1. El motor ILM consulta al servicio ADC para determinar el mejor servicio LDR de destino dentro del grupo de almacenamiento especificado por la regla ILM. Luego envía a ese servicio LDR un comando para iniciar la replicación.
2. El servicio LDR de destino consulta al servicio ADC para obtener la mejor ubicación de origen. Luego 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 ILM que se han almacenado los datos del objeto.
5. El motor ILM actualiza el almacén de metadatos con metadatos de ubicación de objetos.

Protección de contenido: codificación de borrado

Si una regla ILM incluye instrucciones para realizar copias codificadas de borrado de datos de objetos, el esquema de codificación de borrado aplicable divide los datos de objetos en fragmentos de datos y paridad y distribuye estos fragmentos entre los nodos de almacenamiento configurados en el perfil de codificación de borrado.

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



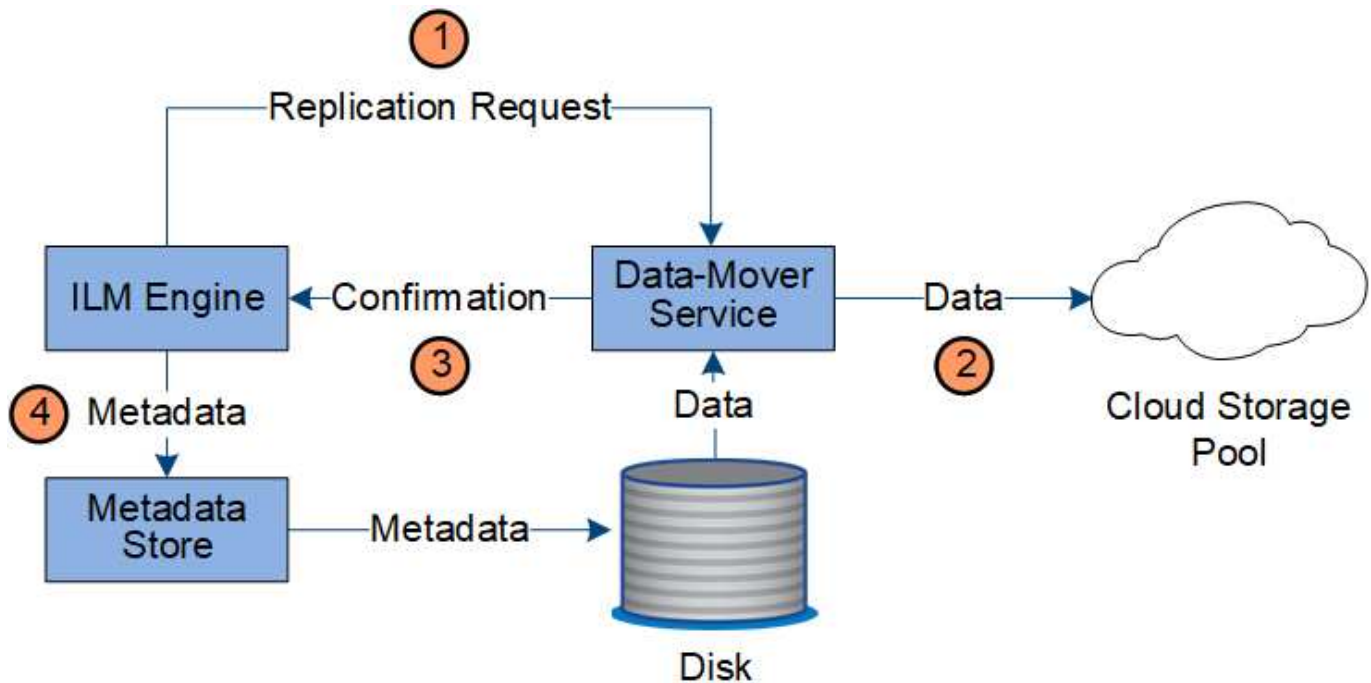
1. El motor ILM consulta al servicio ADC para determinar qué servicio DDS puede realizar mejor la operación de codificación de borrado. Cuando se determina, el motor ILM envía una solicitud de "inicio" a ese servicio.
2. El servicio DDS instruye a un LDR a codificar el borrado de los datos del objeto.
3. El servicio LDR de origen envía una copia al servicio LDR seleccionado para la codificación de borrado.
4. Después de crear la cantidad adecuada de fragmentos de paridad y datos, el servicio LDR distribuye estos fragmentos entre los nodos de almacenamiento (servicios de fragmentos) que conforman el grupo de almacenamiento del perfil de codificación de borrado.
5. El servicio LDR notifica al motor ILM, confirmando que los datos del objeto se distribuyeron correctamente.
6. El motor ILM actualiza el almacén de metadatos con metadatos de ubicación de objetos.

Protección de contenido: Cloud Storage Pool

Si las instrucciones de ubicación de contenido de una regla ILM requieren que se almacene una copia replicada de los datos del objeto en un grupo de almacenamiento en la nube, los datos del objeto se duplican en el bucket S3 externo o en el contenedor de almacenamiento de blobs de Azure que se especificó para el grupo de almacenamiento en la nube.

El motor ILM, que es un componente del servicio LDR, y el servicio Data Mover controlan el movimiento de

objetos al grupo de almacenamiento en la nube.



1. El motor ILM selecciona un servicio Data Mover para replicar en el grupo de almacenamiento en la nube.
2. El servicio Data Mover envía los datos del objeto al grupo 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 ILM actualiza el almacén de metadatos con metadatos de ubicación de objetos.

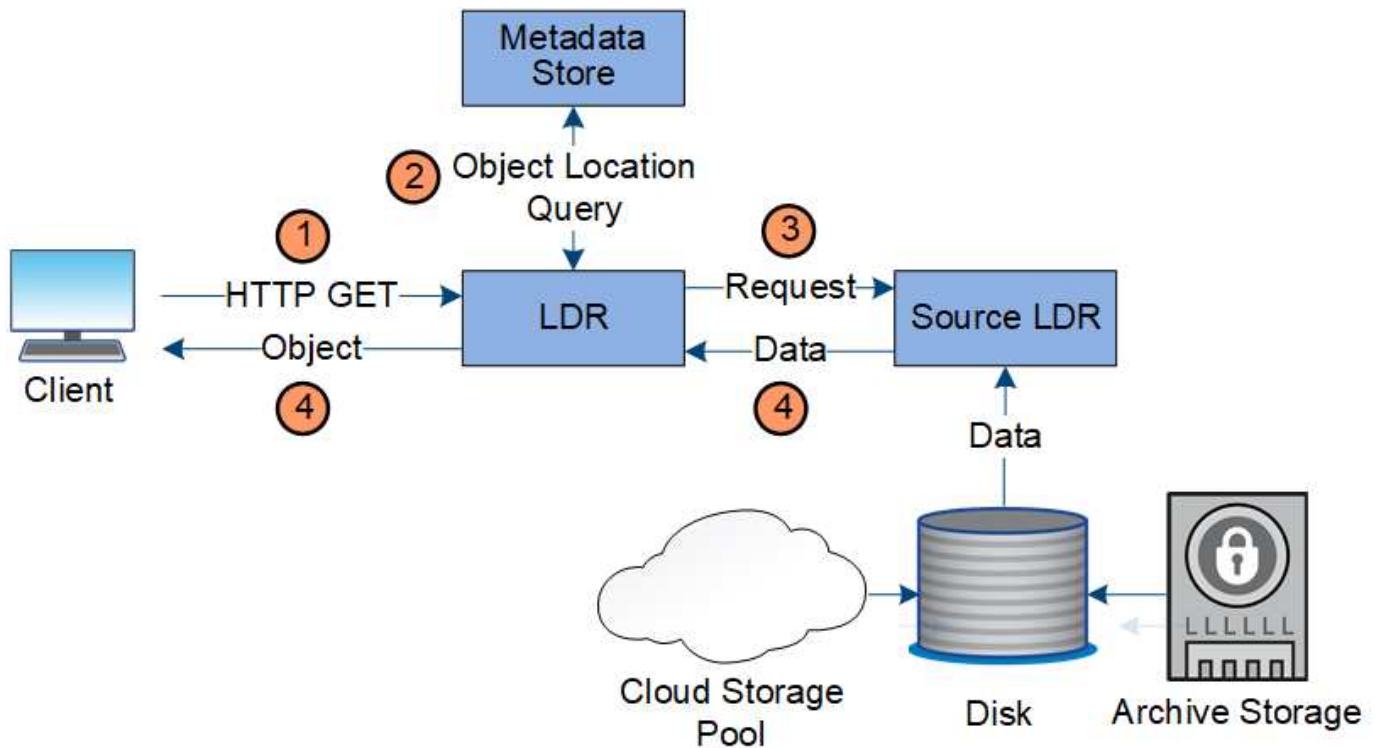
Recuperar flujo de datos

Una operación de recuperación consiste en un flujo de datos definido entre el sistema StorageGRID y el cliente. El sistema utiliza atributos para rastrear la recuperación del objeto desde un nodo de almacenamiento o, si es necesario, un grupo de almacenamiento en la nube.

El servicio LDR del nodo de almacenamiento consulta el almacén de metadatos para conocer la ubicación de 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 grupo de almacenamiento en la nube.



Si la única copia del objeto está en el almacenamiento de AWS Glacier o en el nivel de Azure Archive, la aplicación cliente debe emitir una solicitud S3 RestoreObject para restaurar una copia recuperable en el grupo de almacenamiento en la nube.



1. El servicio LDR recibe una solicitud de recuperación de la aplicación cliente.
2. El servicio LDR consulta el almacén de metadatos para conocer la ubicación de los datos del objeto y los metadatos.
3. El servicio LDR reenvía la solicitud de recuperación al servicio LDR de origen.
4. El servicio LDR de origen devuelve los datos del 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 expira la vida útil del objeto, lo que activa su eliminación automática. Hay un flujo de datos definido para la eliminación de objetos.

Jerarquía de eliminación

StorageGRID proporciona varios métodos para controlar cuándo se conservan o eliminan los objetos. Los objetos se pueden eliminar a petición del cliente o de forma automática. StorageGRID siempre prioriza cualquier configuración de bloqueo de objetos S3 sobre las solicitudes de eliminación del cliente, que tienen prioridad sobre el ciclo de vida del bucket S3 y las instrucciones de ubicación de ILM.

- **Bloqueo de objetos S3:** si la configuración global de Bloqueo de objetos S3 está habilitada para la cuadrícula, los clientes S3 pueden crear depósitos con el Bloqueo de objetos S3 habilitado y luego usar la API REST de S3 para especificar las configuraciones de retención hasta la fecha y retención legal para cada versión de objeto agregada a ese depósito.
 - Una versión de un objeto que se encuentra bajo retención legal no se puede eliminar mediante ningún método.
 - Antes de que se alcance la fecha de conservación de una versión de un objeto, esa versión no se puede eliminar mediante ningún método.

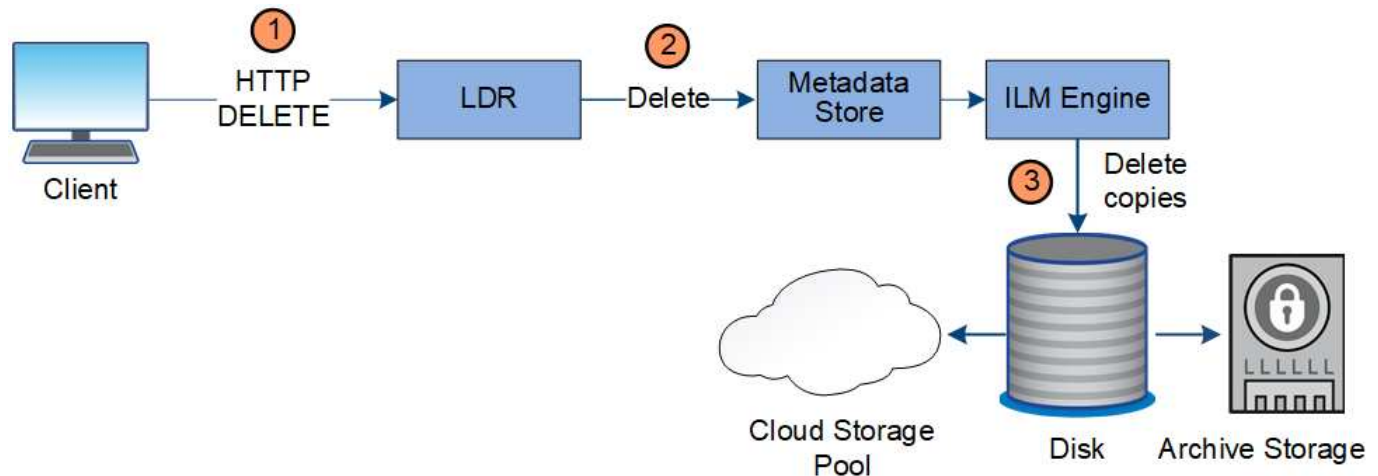
- Los objetos en depósitos con el bloqueo de objetos S3 habilitado son retenidos por ILM "para siempre". Sin embargo, una vez alcanzada su fecha de retención, una versión de un objeto puede eliminarse mediante una solicitud del cliente o mediante la expiración del ciclo de vida del depósito.
- Si los clientes S3 aplican una fecha de retención hasta predeterminada al depósito, no necesitan especificar una fecha de retención hasta para cada objeto.
- **Solicitud de eliminación de cliente:** Un cliente S3 puede emitir una solicitud de eliminación de objeto. Cuando un cliente elimina un objeto, se eliminan todas las copias del objeto del sistema StorageGRID .
- **Eliminar objetos en el depósito:** los usuarios de Tenant Manager pueden usar esta opción para eliminar de forma permanente todas las copias de los objetos y las versiones de objetos en los depósitos seleccionados del sistema StorageGRID .
- **Ciclo de vida del bucket S3:** los clientes S3 pueden agregar una configuración de ciclo de vida a sus buckets que especifique una acción de vencimiento. Si existe un ciclo de vida de depósito, StorageGRID elimina automáticamente todas las copias de un objeto cuando se cumple la fecha o la cantidad de días especificada en la acción Vencimiento, a menos que el cliente elimine el objeto primero.
- **Instrucciones de ubicación de ILM:** Suponiendo que el bucket no tiene habilitado el bloqueo de objetos S3 y que no hay un ciclo de vida del bucket, StorageGRID elimina automáticamente un objeto cuando finaliza el último período de tiempo en la regla de ILM y no hay más ubicaciones especificadas para el objeto.



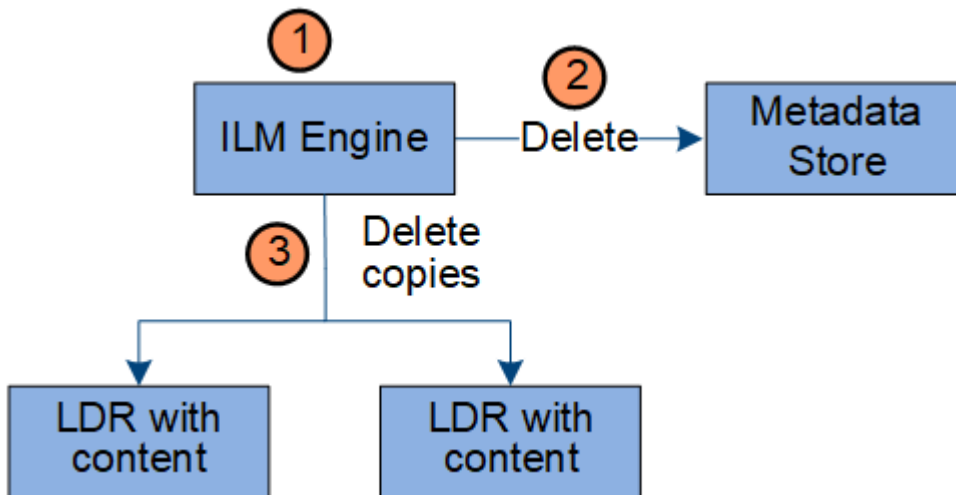
Cuando se configura un ciclo de vida de un bucket S3, las acciones de vencimiento del ciclo de vida anulan la política ILM para los objetos que coinciden con el filtro del ciclo de vida. Como resultado, un objeto podría permanecer en la cuadrícula incluso después de que hayan transcurrido las instrucciones ILM para colocar el objeto.

Ver "[Cómo se eliminan los objetos](#)" Para más información.

Flujo de datos para eliminaciones de clientes



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



1. El motor ILM determina que es necesario eliminar el objeto.
2. El motor ILM notifica al almacén de metadatos. El almacén de metadatos actualiza los metadatos del objeto para que el objeto parezca eliminado ante las solicitudes del cliente.
3. El motor ILM elimina todas las copias del objeto. El almacén de metadatos se actualiza para eliminar los metadatos del objeto.

Gestión del ciclo de vida de la información

Utilice la gestión del ciclo de vida de la información (ILM) para controlar la ubicación, la duración y el comportamiento de ingesta de todos los objetos en su sistema StorageGRID . Las reglas ILM determinan cómo StorageGRID almacena objetos a lo largo del tiempo. Configura una o más reglas ILM y luego las agrega a una política ILM. Una red puede tener más de una política activa a la vez.

Las reglas de ILM definen:

- ¿Qué objetos deben almacenarse? Una regla puede aplicarse 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 objetos asociados con determinadas cuentas de inquilino, depósitos S3 o contenedores Swift específicos, o valores de metadatos específicos.
- El tipo y la ubicación de almacenamiento. Los objetos se pueden almacenar en nodos de almacenamiento o en grupos de almacenamiento en la nube.
- El tipo de copias de objetos realizadas. Las copias pueden replicarse o codificarse para borrarlas.
- Para copias replicadas, el número de copias realizadas.
- Para copias con código 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 los objetos a medida que se incorporan a la red (ubicación sincrónica o confirmación dual).

Tenga en cuenta que los metadatos de los objetos no son administrados por las reglas ILM. En cambio, los metadatos de los objetos se almacenan en una base de datos de Cassandra en lo que se conoce como un almacén de metadatos. Se mantienen automáticamente tres copias de los metadatos de los objetos en cada sitio para proteger los datos contra pérdidas.

Ejemplo de regla ILM

A modo de ejemplo, una regla ILM podría especificar lo siguiente:

- Aplicar únicamente a los objetos pertenecientes al Inquilino A.
- Haga dos copias replicadas de esos objetos y almacene cada copia en un sitio diferente.
- Conserve las dos copias "para siempre", lo que significa que StorageGRID no las eliminará automáticamente. En su lugar, StorageGRID conservará estos objetos hasta que sean eliminados por una solicitud de eliminación del cliente o hasta que expire el ciclo de vida de un depósito.
- Utilice la opción Equilibrado para el comportamiento de ingesta: la instrucción de ubicación de dos sitios se aplica tan pronto como el Inquilino A guarda un objeto en StorageGRID, a menos que no sea posible realizar inmediatamente ambas copias requeridas.

Por ejemplo, si no se puede acceder al Sitio 2 cuando el Inquilino A guarda un objeto, StorageGRID hará dos copias provisionales en los Nodos de almacenamiento del Sitio 1. Tan pronto como el Sitio 2 esté disponible, StorageGRID hará la copia requerida en ese sitio.

Cómo una política ILM evalúa los objetos

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

Cuando los clientes guardan objetos en StorageGRID, los objetos se evalúan en función del conjunto ordenado de reglas 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 ingiere de acuerdo con el comportamiento de ingesta de esa regla y se almacena de acuerdo con las instrucciones de ubicación de esa regla.
2. Si los filtros de la primera regla no coinciden con el objeto, este se evalúa en relación con cada regla posterior de la política hasta que se encuentre una coincidencia.
3. Si ninguna regla coincide con un objeto, se aplican el comportamiento de ingesta y las instrucciones de ubicación de la regla predeterminada en la política. La regla predeterminada es la última regla de una política y no puede utilizar ningún filtro. Debe aplicarse a todos los inquilinos, todos los depósitos y todas las versiones de objetos.

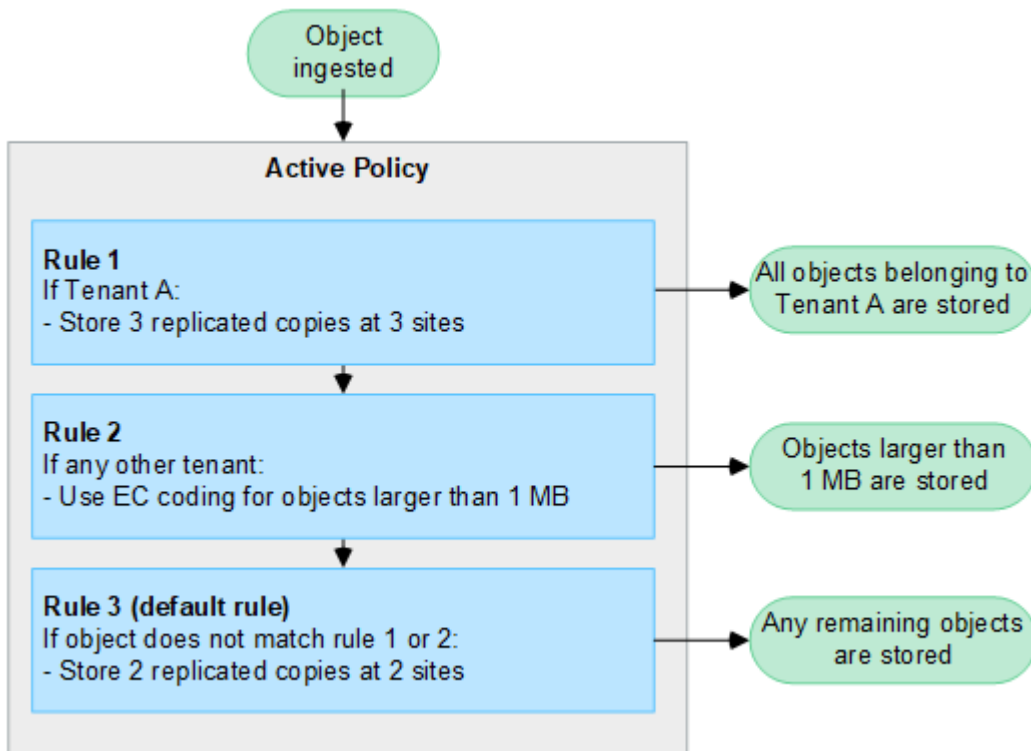
Ejemplo de política ILM

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

- **Regla 1: Copias replicadas para el inquilino A**
 - Empareja todos los objetos que pertenecen al inquilino A.
 - Almacene estos objetos como tres copias replicadas en tres sitios.
 - Los objetos que pertenecen a otros inquilinos no coinciden con la Regla 1, por lo que se evalúan según la Regla 2.
- **Regla 2: Codificación de borrado para objetos mayores a 1 MB**
 - Coincide con todos los objetos de otros inquilinos, pero solo si son mayores a 1 MB. Estos objetos más grandes se almacenan utilizando codificación de borrado 6+3 en tres sitios.
 - No coincide con objetos de 1 MB o más pequeños, por lo que estos objetos se evalúan según la Regla 3.

- **Regla 3: 2 copias, 2 centros de datos** (predeterminado)

- Es la última regla predeterminada de la política. No utiliza filtros.
- Realice dos copias replicadas de todos los objetos que no coincidan con la Regla 1 o la Regla 2 (objetos que no pertenecen al Inquilino A y que tienen 1 MB o menos).



Información relacionada

- ["Administrar objetos con ILM"](#)

Explorar StorageGRID

Explorar el Administrador de cuadrícula

Grid Manager es la interfaz gráfica basada en navegador que le permite configurar, administrar y monitorear su sistema StorageGRID .



El Grid Manager se actualiza con cada versión y es posible que no coincida con las capturas de pantalla de ejemplo en esta página.

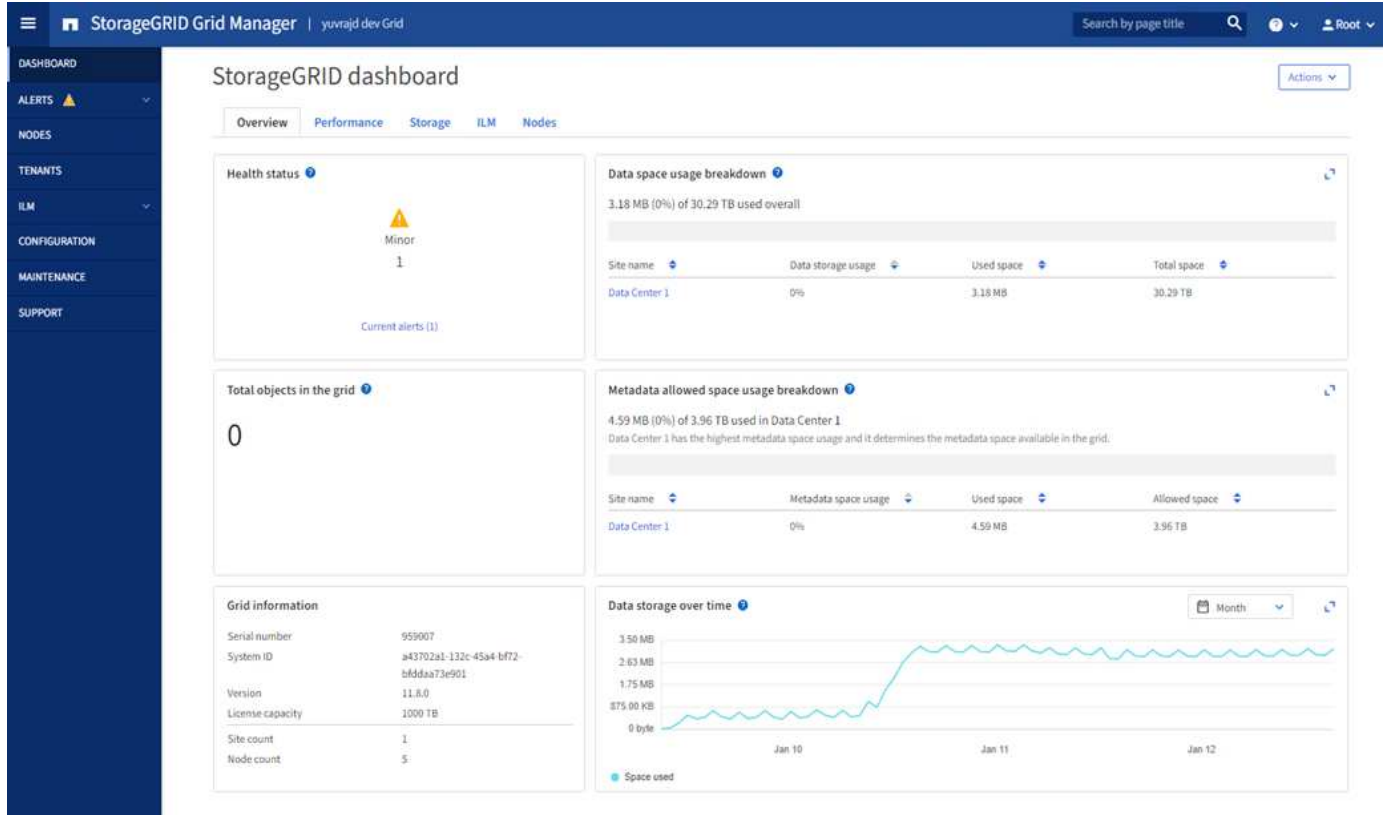
Cuando inicia sesión en Grid Manager, se conecta a un nodo de administración. Cada sistema StorageGRID incluye un nodo de administración principal y cualquier cantidad de nodos de administración no principales. Puede conectarse a cualquier nodo de administración y cada nodo de administración muestra una vista similar del sistema StorageGRID .

Puede acceder al Administrador de cuadrícula mediante un ["navegador web compatible"](#) .

Panel de control de Grid Manager

Cuando inicie sesión por primera vez en Grid Manager, podrá usar el panel de control para ["supervisar las actividades del sistema"](#) De un vistazo.

El panel contiene información sobre la salud y el rendimiento del sistema, el uso del almacenamiento, los procesos ILM, las operaciones S3 y los nodos de la red. Puede [configurar el panel de control](#) seleccionando de una colección de tarjetas que contienen la información que necesita para monitorear eficazmente su sistema.



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

Campo de búsqueda

El campo **Buscar** en la barra de encabezado le permite navegar rápidamente a una página específica dentro de Grid Manager. Por ejemplo, puede ingresar **km** para acceder a la página del servidor de administración de claves (KMS).

Puede utilizar **Buscar** para encontrar entradas en la barra lateral del Administrador de Grid y en los menús Configuración, Mantenimiento y Soporte. También puede buscar por nombre elementos como nodos de la red y cuentas de inquilinos.

Menú de ayuda

El menú de ayuda  proporciona acceso a:

- El ["FabricPool"](#) y ["Configuración de S3"](#) mago
- El centro de documentación de StorageGRID para la versión actual
- ["Documentación de API"](#)
- Información sobre qué versión de StorageGRID está instalada actualmente

Menú de alertas

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

Desde el menú Alertas, puede hacer lo siguiente para ["gestionar alertas"](#) :

- Revisar las alertas actuales
- Revisar alertas resueltas
- Configurar silencios para suprimir las notificaciones de alerta
- Definir reglas de alerta para las condiciones que activan alertas
- Configurar el servidor de correo electrónico para notificaciones de alerta

Página de nodos

El ["Página de nodos"](#) muestra información sobre toda la cuadrícula, cada sitio de la cuadrícula y cada nodo de un sitio.

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

Nodes

View the list and status of sites and grid nodes.

Total node count: 14

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

Página de inquilinos

El ["Página de inquilinos"](#) te permite ["Crear y supervisar las cuentas de inquilinos de almacenamiento"](#) para su sistema StorageGRID . Debe crear al menos una cuenta de inquilino para especificar quién puede almacenar y recuperar objetos y qué funcionalidad está disponible para ellos.

La página Inquilinos también proporciona detalles de uso para cada inquilino, incluida la cantidad de

almacenamiento utilizado y la cantidad de objetos. Si establece una cuota cuando creó el inquilino, podrá ver cuánto de esa cuota se ha utilizado.

Tenants

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

CreateExport to CSVActions

Search tenants by name or ID

Displaying 2 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	S3 Tenant	0 bytes	0%	100.00 GB	0	→ 📄
☐	Swift Tenant	0 bytes	0%	100.00 GB	0	→ 📄

← Previous1Next →

Menú de ILM

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

Desde el menú ILM puedes ver y administrar ILM:

- Normas
- Políticas
- Etiquetas de política
- Pools de almacenamiento
- Grados de almacenamiento
- Regiones
- Búsqueda de metadatos de objetos

Menú de configuración

El menú Configuración le permite especificar configuraciones de red, configuraciones de seguridad, configuraciones del sistema, opciones de monitoreo y opciones de control de acceso.

Tareas de red

Las tareas de red incluyen:

- "Gestión de grupos de alta disponibilidad"
- "Administración de puntos finales del balanceador de carga"
- "Configuración de nombres de dominio de puntos finales S3"
- "Gestión de políticas de clasificación de tráfico"
- "Configuración de interfaces VLAN"

Tareas de seguridad

Las tareas de seguridad incluyen:

- "Gestión de certificados de seguridad"
- "Administrar los controles internos del firewall"
- "Configuración de servidores de administración de claves"
- Configurar ajustes de seguridad, incluyendo la "Política de TLS y SSH", "Opciones de seguridad de red y objetos", y "configuración de seguridad de la interfaz".
- Configurar los ajustes para un "proxy de almacenamiento" o un "proxy de administración"

Tareas del sistema

Las tareas del sistema incluyen:

- Usando "federación de red" para clonar la información de la cuenta del inquilino y replicar datos de objetos entre dos sistemas StorageGRID.
- Opcionalmente, habilitar la "Comprimir objetos almacenados" opción.
- "Administración del bloqueo de objetos S3"
- Comprender las opciones de almacenamiento como "segmentación de objetos" y "marcas de agua de volumen de almacenamiento".
- "Administrar perfiles de codificación de borrado".

Tareas de seguimiento

Las tareas de monitoreo incluyen:

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

Tareas de control de acceso

Las tareas de control de acceso incluyen:

- "Administrar grupos de administradores"
- "Administrar usuarios administradores"
- Cambiando el "frase de contraseña de aprovisionamiento" o "contraseñas de la consola del nodo"
- "Uso de la federación de identidades"
- "Configuración de SSO"

Menú de mantenimiento

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

Tareas

Las tareas de mantenimiento incluyen:

- ["Operaciones de desmantelamiento"](#) para eliminar nodos y sitios de la red no utilizados
- ["Operaciones de expansión"](#) para agregar nuevos nodos y sitios de la red
- ["Procedimientos de recuperación de nodos de red"](#) Para reemplazar un nodo fallido y restaurar datos
- ["Cambiar el nombre de los procedimientos"](#) para cambiar los nombres para mostrar de su cuadrícula, sitios y nodos
- ["Operaciones de comprobación de existencia de objetos"](#) para verificar la existencia (aunque no la exactitud) de los datos del objeto
- Realizando una ["reinicio continuo"](#) para reiniciar varios nodos de la red
- ["Operaciones de restauración de volumen"](#)

Sistema

Las tareas de mantenimiento del sistema que puede realizar incluyen:

- ["Visualización de la información de la licencia de StorageGRID"](#) o ["actualización de la información de la licencia"](#)
- Generando y descargando el ["Paquete de recuperación"](#)
- Realizar actualizaciones de software de StorageGRID , incluidas actualizaciones de software, revisiones y actualizaciones del software SANtricity OS en dispositivos seleccionados
 - ["Procedimiento de actualización"](#)
 - ["Procedimiento de revisión urgente"](#)
 - ["Actualice el sistema operativo SANtricity en los controladores de almacenamiento SG6000 mediante Grid Manager"](#)
 - ["Actualice el sistema operativo SANtricity en los controladores de almacenamiento SG5700 mediante Grid Manager"](#)

Red

Las tareas de mantenimiento de red que puede realizar incluyen:

- ["Configuración de servidores DNS"](#)
- ["Actualización de subredes de la red Grid"](#)
- ["Administración de servidores NTP"](#)

Menú de soporte

El menú Soporte proporciona opciones que ayudan al soporte técnico a analizar y solucionar problemas de su sistema.

Herramientas

Desde la sección Herramientas del menú Soporte, puedes:

- ["Configurar AutoSupport"](#)
- ["Ejecutar diagnósticos"](#) sobre el estado actual de la red
- ["Acceder al árbol de topología de la cuadrícula"](#) para ver información detallada sobre los nodos de la red, los servicios y los atributos

- ["Recopilar archivos de registro y datos del sistema"](#)
- ["Revisar las métricas de soporte"](#)



Las herramientas disponibles en la opción **Métricas** están destinadas a ser utilizadas por el soporte técnico. Algunas funciones y elementos del menú de estas herramientas no son funcionales intencionalmente.

Alarmas (heredadas)

La información sobre las alarmas heredadas se ha eliminado de esta versión de la documentación. Referirse a ["Administrar alertas y alarmas \(documentación de StorageGRID 11.8\)"](#).

Otro

Desde la sección Otros del menú Soporte, puedes:

- Administrar ["costo del enlace"](#)
- Vista ["Sistema de gestión de red \(NMS\)"](#) entradas
- Administrar ["marcas de agua de almacenamiento"](#)

Explorar el Administrador de inquilinos

El ["Administrador de inquilinos"](#) es la interfaz gráfica basada en navegador a la que los usuarios inquilinos acceden para configurar, administrar y monitorear sus cuentas de almacenamiento.



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

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

Panel de control del administrador de inquilinos

Después de que un administrador de red crea una cuenta de inquilino mediante el Administrador de red o la API de administración de red, los usuarios inquilinos pueden iniciar sesión en el Administrador de inquilinos.

El panel de control de Tenant Manager permite a los usuarios inquilinos monitorear el uso del almacenamiento de un vistazo. El panel de uso de almacenamiento contiene una lista de los depósitos (S3) o contenedores (Swift) más grandes para el inquilino. El valor de Espacio utilizado es la cantidad total de datos del objeto en el depósito o contenedor. El gráfico de barras representa los tamaños relativos de estos cubos o contenedores.

El valor que se muestra sobre el gráfico de barras es una suma del espacio utilizado para todos los contenedores o depósitos del inquilino. 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.

Dashboard

16**Buckets**[View buckets](#)**2****Platform services****endpoints**[View endpoints](#)**0****Groups**[View groups](#)**1****User**[View users](#)

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Top buckets by capacity limit usage [?](#)

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details [?](#)

Name: Tenant02

ID: 3341 1240 0546 8283 2208

- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

Menú de almacenamiento (S3)

El menú Almacenamiento está disponible únicamente para cuentas de inquilinos de S3. Este menú permite a los usuarios de S3 administrar claves de acceso; crear, administrar y eliminar depósitos; administrar puntos finales de servicios de la plataforma y ver cualquier conexión de federación de red que tengan permitido usar.

Mis teclas de acceso

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

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



La gestión de las claves de acceso de otros usuarios se realiza desde el menú Gestión de acceso.

Cubos

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

- Crear depósitos
- Habilitar el bloqueo de objetos S3 para un nuevo depósito (se supone que el bloqueo de objetos S3 está habilitado para el sistema StorageGRID)
- Actualizar valores de consistencia
- Habilitar y deshabilitar las actualizaciones de la última hora de acceso
- Habilitar o suspender el control de versiones de objetos
- Actualizar la retención predeterminada de bloqueo de objetos S3
- Configurar el uso compartido de recursos entre orígenes (CORS)
- Eliminar todos los objetos en un depósito
- Eliminar depósitos vacíos
- Utilice el ["Consola S3"](#) Para gestionar objetos de depósito

Si un administrador de red ha habilitado el uso de servicios de plataforma para la cuenta de inquilino, un usuario de inquilino S3 con los permisos adecuados también puede realizar estas tareas:

- Configure las notificaciones de eventos S3, que se pueden enviar a un servicio de destino que admita Amazon Simple Notification Service.
- Configure la replicación de CloudMirror, que permite al inquilino replicar automáticamente objetos en un depósito S3 externo.
- Configure la integración de búsqueda, que envía metadatos de objetos a un índice de búsqueda de destino cada vez que se crea o elimina un objeto, o se actualizan sus metadatos o etiquetas.

Puntos finales de servicios de plataforma

Si un administrador de red ha habilitado el uso de servicios de plataforma para la cuenta de inquilino, un usuario de inquilino S3 con el permiso Administrar puntos finales puede configurar un punto final de destino para cada servicio de plataforma.

Conexiones de federación de red

Si un administrador de red ha habilitado el uso de una conexión de federación de red para la cuenta de inquilino, un usuario de inquilino S3 que tenga permiso de acceso raíz puede ver el nombre de la conexión, acceder a la página de detalles del depósito para cada depósito que tenga habilitada la replicación entre redes y ver el error más reciente que ocurrió cuando los datos del depósito se estaban replicando a la otra red en la conexión. Ver ["Ver las conexiones de la federación de red"](#) .

Menú de gestión de acceso

El menú Administración de acceso permite a los inquilinos de StorageGRID importar grupos de usuarios desde una fuente de identidad federada y asignar permisos de administración. Los inquilinos también pueden administrar grupos de inquilinos y usuarios locales, a menos que el inicio de sesión único (SSO) esté vigente para todo el sistema StorageGRID .

Pautas para establecer redes

Pautas para establecer redes

Utilice estas pautas para obtener información sobre la arquitectura y las topologías de

red de StorageGRID , y para conocer los requisitos para la configuración y el aprovisionamiento de la red.

Acerca de estas instrucciones

Estas pautas proporcionan información que puede utilizar para crear la infraestructura de red de StorageGRID antes de implementar y configurar los nodos de StorageGRID . Utilice estas pautas para ayudar a garantizar que la comunicación pueda ocurrir entre todos los nodos de la red y entre la red y los clientes y servicios externos.

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

- Almacenar y recuperar datos de objetos
- Recibir notificaciones por correo electrónico
- Acceda a la interfaz de administración de StorageGRID (Grid Manager y Tenant Manager)
- Acceder al recurso compartido de auditoría (opcional)
- Proporcionar servicios como:
 - Protocolo de tiempo de red (NTP)
 - Sistema de nombres de dominio (DNS)
 - Servidor de administración de claves (KMS)

La red StorageGRID debe configurarse adecuadamente para manejar el tráfico para estas funciones y más.

Antes de empezar

La configuración de la red para un sistema StorageGRID requiere un alto nivel de experiencia con conmutación Ethernet, redes TCP/IP, subredes, enrutamiento de red y firewalls.

Antes de configurar la red, familiarícese con la arquitectura de StorageGRID como se describe en "[Obtenga más información sobre StorageGRID](#)".

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

Instalar nodos de dispositivos

- "[Instalar el hardware del dispositivo](#)"

Instalar nodos basados en software

- "[Instalar StorageGRID en Red Hat Enterprise Linux](#)"
- "[Instalar StorageGRID en Ubuntu o Debian](#)"
- "[Instalar StorageGRID en VMware](#)"

Configurar y administrar el software StorageGRID

- "[Administrar StorageGRID](#)"
- "[Notas de la versión](#)"

Tipos de red StorageGRID

Los nodos de la red en un sistema StorageGRID procesan *tráfico de red*, *tráfico de administración* y *tráfico de cliente*. Debe configurar la red adecuadamente para administrar estos tres tipos de tráfico y proporcionar control y seguridad.

Tipos de tráfico

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

Puede configurar la red de las siguientes maneras:

- Solo red de cuadrícula
- Redes de cuadrícula y de administración
- Redes de cuadrícula y de clientes
- Redes de cuadrícula, de administración y de clientes

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

A los puertos internos solo se puede acceder a través de la red Grid. Los puertos externos son accesibles desde todos los tipos de red. Esta flexibilidad proporciona múltiples opciones para diseñar una implementación de StorageGRID y configurar filtrado de puertos e IP externos en conmutadores y firewalls. Ver "[comunicaciones internas del nodo de la red](#)" y "[comunicaciones externas](#)".

Interfaces de red

Los nodos StorageGRID están conectados a cada red mediante las siguientes interfaces específicas:

Red	Nombre de la interfaz
Red de cuadrícula (obligatoria)	eth0

Red	Nombre de la interfaz
Red de administración (opcional)	eth1
Red de clientes (opcional)	eth2

Para obtener detalles sobre cómo asignar puertos virtuales o físicos a interfaces de red de nodo, consulte las instrucciones de instalación:

Nodos basados en software

- ["Instalar StorageGRID en Red Hat Enterprise Linux"](#)
- ["Instalar StorageGRID en Ubuntu o Debian"](#)
- ["Instalar StorageGRID en VMware"](#)

Nodos de dispositivos

- ["Dispositivo de almacenamiento SG6160"](#)
- ["Dispositivo de almacenamiento SGF6112"](#)
- ["Dispositivo de almacenamiento SG6000"](#)
- ["Dispositivo de almacenamiento SG5800"](#)
- ["Dispositivo de almacenamiento SG5700"](#)
- ["Aparatos de servicio SG110 y SG1100"](#)
- ["Aparatos de servicio SG100 y SG1000"](#)

Información de red para cada nodo

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

- Dirección IP
- Máscara de subred
- Dirección IP de la puerta de enlace

Solo se puede configurar una combinación de dirección IP/máscara/puerta de enlace para cada una de las tres redes en cada nodo de la red. Si no desea configurar una puerta de enlace para una red, debe utilizar la dirección IP como dirección de puerta de enlace.

Grupos de alta disponibilidad

Los grupos de alta disponibilidad (HA) brindan la capacidad de agregar direcciones IP virtuales (VIP) a la interfaz de red del cliente o de la red. Para obtener más información, consulte ["Administrar grupos de alta disponibilidad"](#).

Red de cuadrícula

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



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

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



Al configurar la red Grid, debe asegurarse de que la red esté protegida contra clientes que no sean de confianza, como aquellos en Internet abierto.

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

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

Red de administración

La red de administración es opcional. Una vez configurado, se puede utilizar para el tráfico de administración y mantenimiento del sistema. La red de administración normalmente es una red privada y no necesita ser enrutable entre nodos.

Puede elegir qué nodos de la red deben tener habilitada la red de administración.

Cuando utiliza la red de administración, no es necesario que el tráfico administrativo y de mantenimiento viaje a través de la red Grid. Los usos típicos de la red de administración incluyen los siguientes:

- Acceso a las interfaces de usuario de Grid Manager y Tenant Manager.
- Acceso a servicios críticos como servidores NTP, servidores DNS, servidores de administración de claves externas (KMS) y servidores de Protocolo ligero de acceso a directorios (LDAP).
- Acceso a los registros de auditoría en los nodos de administración.
- Acceso al Protocolo Secure Shell (SSH) para mantenimiento y soporte.

La red de administración nunca se utiliza para el tráfico de la red interna. Se proporciona una puerta de enlace de red de administración que permite que la red de administración se comuniquen con múltiples subredes externas. Sin embargo, la puerta de enlace de la red de administración nunca se utiliza como puerta de enlace predeterminada del nodo.

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

- La puerta de enlace de la 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 la red de administración del nodo.

Red de clientes

La red de clientes es opcional. Cuando se configura, se utiliza para proporcionar acceso a servicios de red para aplicaciones cliente como S3. Si planea hacer que los datos de StorageGRID sean accesibles a un recurso externo (por ejemplo, un grupo de almacenamiento en la nube o el servicio de replicación StorageGRID CloudMirror), el recurso externo también puede usar la red del cliente. Los nodos de la red pueden comunicarse con cualquier subred accesible a través de la puerta de enlace de la red del cliente.

Puede elegir qué nodos de la red deben tener habilitada 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 del cliente no estará operativa hasta que se complete la instalación de la red.

Para mayor seguridad, puede especificar que la interfaz de red de cliente de un nodo no sea confiable para que la red de cliente sea más restrictiva en cuanto a qué conexiones están permitidas. Si la interfaz de red de cliente de un nodo no es confiable, la interfaz acepta conexiones salientes como las que usa la replicación de CloudMirror, pero solo acepta conexiones entrantes en puertos que se hayan configurado explícitamente como puntos finales del balanceador de carga. Ver ["Administrar los controles del firewall"](#) y ["Configurar los puntos finales del balanceador de carga"](#).

Cuando se utiliza una red de cliente, no es necesario que el tráfico del cliente viaje a través de la red de cuadrícula. El tráfico de la red se puede separar en una red segura y no enrutable. Los siguientes tipos de nodos suelen configurarse con una red de cliente:

- Nodos de puerta de enlace, porque estos nodos proporcionan acceso al servicio StorageGRID Load Balancer y acceso del cliente S3 a la red.
- Nodos de almacenamiento, porque estos nodos proporcionan acceso al protocolo S3 y a los grupos de almacenamiento en la nube y al servicio de replicación CloudMirror.
- Nodos de administración, para garantizar que los usuarios inquilinos puedan conectarse al Administrador de inquilinos sin necesidad de usar la red de administración.

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

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

Redes VLAN opcionales

Según sea necesario, puede utilizar opcionalmente redes LAN virtuales (VLAN) para el tráfico del cliente y para algunos tipos de tráfico de administrador. Sin embargo, el tráfico de la red no puede utilizar una interfaz VLAN. El tráfico interno de StorageGRID entre nodos siempre debe utilizar la red Grid en eth0.

Para admitir el uso de VLAN, debe configurar una o más interfaces en un nodo como interfaces troncales en el conmutador. Puede configurar la interfaz de red de cuadrícula (eth0) o la interfaz de red de cliente (eth2) para que sea un troncal, o puede agregar interfaces troncales al nodo.

Si eth0 está configurado como troncal, el tráfico de la red Grid fluye a través de la interfaz nativa del troncal, tal como está configurado en el conmutador. De manera similar, si eth2 está configurado como un enlace troncal y la red del cliente también está configurada en el mismo nodo, la red del cliente utiliza la VLAN nativa del puerto troncal tal como está configurada en el conmutador.

Solo se admite el tráfico administrativo entrante, como el que se utiliza para SSH, Grid Manager o Tenant Manager, a través de redes VLAN. El tráfico saliente, como el que se utiliza para NTP, DNS, LDAP, KMS y grupos de almacenamiento en la nube, no se admite en redes VLAN.



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

Ver "[Configurar interfaces VLAN](#)" para obtener instrucciones y pautas.

Las interfaces VLAN solo se utilizan en grupos HA y se les asignan direcciones VIP en el nodo activo. Ver "[Administrar grupos de alta disponibilidad](#)" para obtener instrucciones y pautas.

Ejemplos de topología de red

Topología de red de cuadrícula

La topología de red más simple se crea configurando únicamente la red Grid.

Cuando configura la red de cuadrícula, establece la dirección IP del host, la máscara de subred y la dirección IP de puerta de enlace para la interfaz eth0 para cada nodo de la red.

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

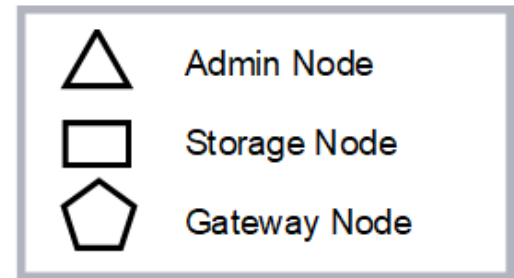
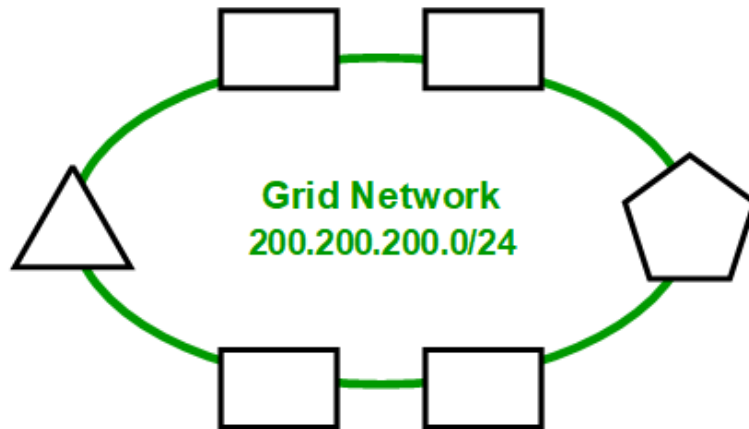
Durante la instalación, la interfaz de red Grid aplica rutas estáticas para todas las subredes en GNSL y establece la ruta predeterminada del nodo a la puerta de enlace de red Grid si hay una configurada. No se requiere GNSL si no hay una red de cliente y la puerta de enlace de la red de cuadrícula es la ruta predeterminada del nodo. También se generan rutas de host a todos los demás nodos de la red.

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



Esta topología es adecuada para implementaciones de un solo sitio que no están disponibles externamente, implementaciones de prueba de concepto o cuando un balanceador de carga de terceros actúa como límite de acceso del cliente. Cuando sea posible, la red eléctrica deberá 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 la red Grid 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 la red de administración

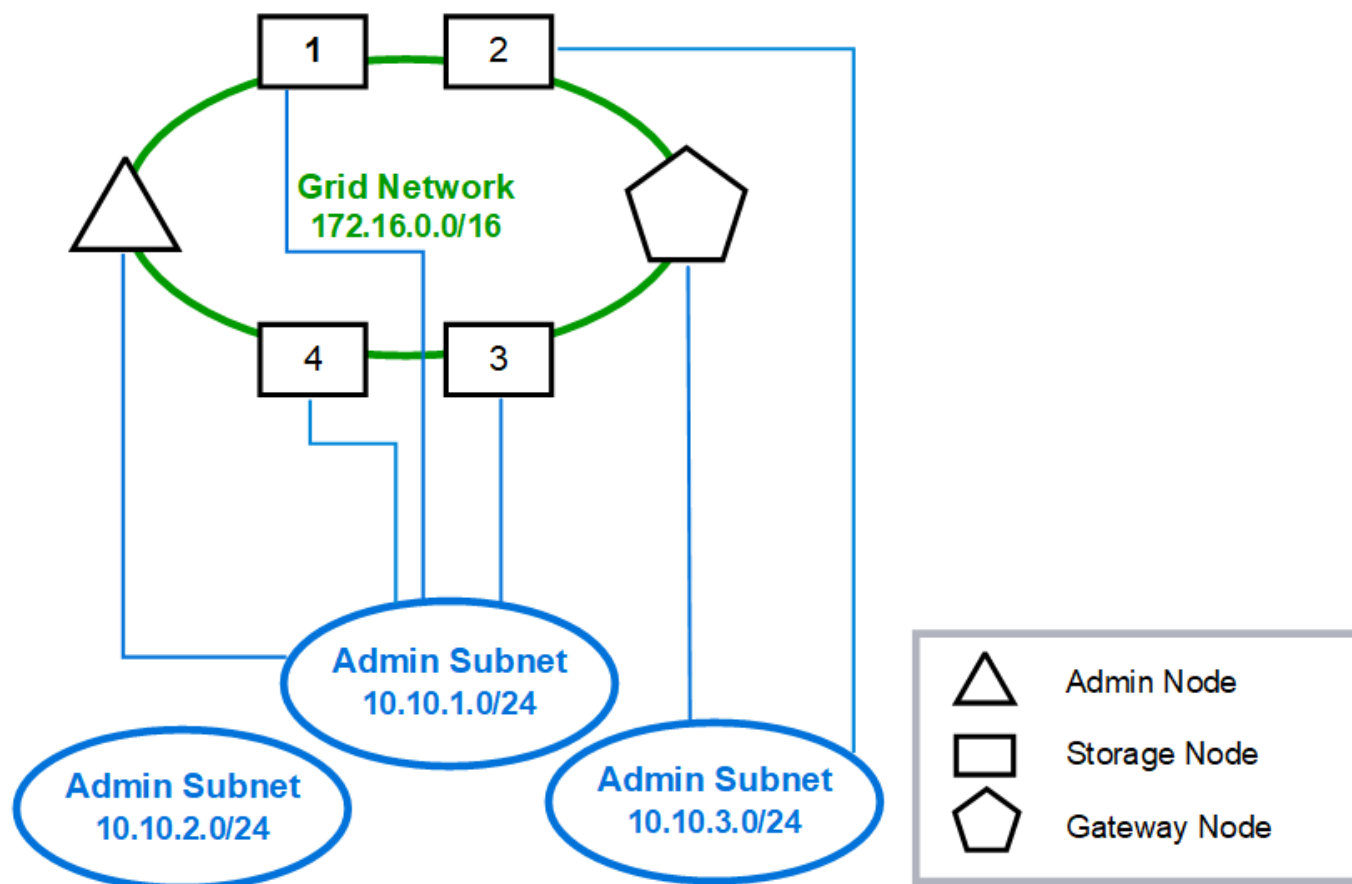
Tener una red de administración es opcional. Una forma de utilizar una red de administración y una red de cuadrícula es configurar una red de cuadrícula enrutable y una red de administración limitada para cada nodo.

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

La red de administración puede ser única para cada nodo y puede constar de varias subredes. Cada nodo se puede configurar con una Lista de subredes externas de administrador (AESL). La AESL enumera las subredes accesibles a través de la red de administración para cada nodo. El AESL también debe incluir las subredes de cualquier servicio al que la red accederá a través de la red de administración, como NTP, DNS, KMS y LDAP. Se aplican rutas estáticas para cada subred en el AESL.

En este ejemplo, la red de cuadrícula se utiliza para el tráfico relacionado con las solicitudes de clientes S3 y la gestión de objetos, mientras que la red de administración se utiliza para funciones administrativas.

Topology example: Grid and Admin Networks



GNSL → 172.16.0.0/16

AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

Nodes	Grid Network		Admin Network	
	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 red del cliente

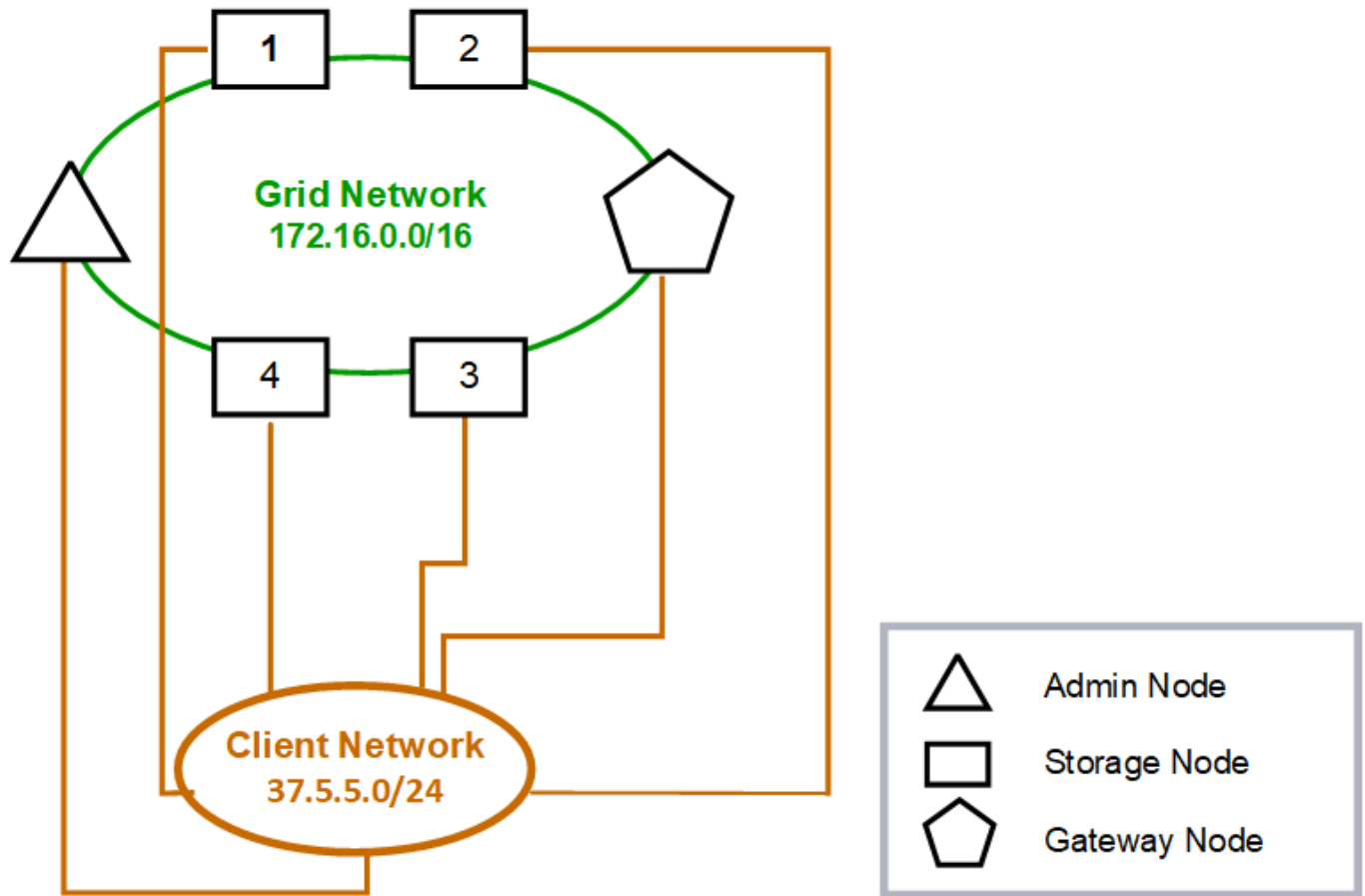
Tener una red de clientes es opcional. El uso de una red de cliente permite separar el tráfico de la red del cliente (por ejemplo, S3) del tráfico interno de la red, lo que permite que la red de la red sea más segura. El tráfico administrativo puede ser manejado por el Cliente o la Red Grid cuando la Red de Administración no está configurada.

Cuando configura la red del cliente, establece la dirección IP del host, la máscara de subred y la dirección IP de la puerta de enlace para la interfaz eth2 del nodo configurado. La red de clientes de cada nodo puede ser independiente de la red de clientes de 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 la red de cuadrícula a la puerta de enlace de la red de cliente cuando se completa la instalación. Si posteriormente se agrega una red de cliente, la puerta de enlace predeterminada del nodo cambia de la misma manera.

En este ejemplo, la red de cliente se utiliza para solicitudes de clientes S3 y para funciones administrativas, mientras que la red de cuadrícula se dedica a operaciones de gestión de objetos internos.

Topology example: Grid and Client Networks



GNSL → 172.16.0.0/16

Nodes	Grid Network	Client Network	
	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

Información relacionada

["Cambiar la configuración de la red del nodo"](#)

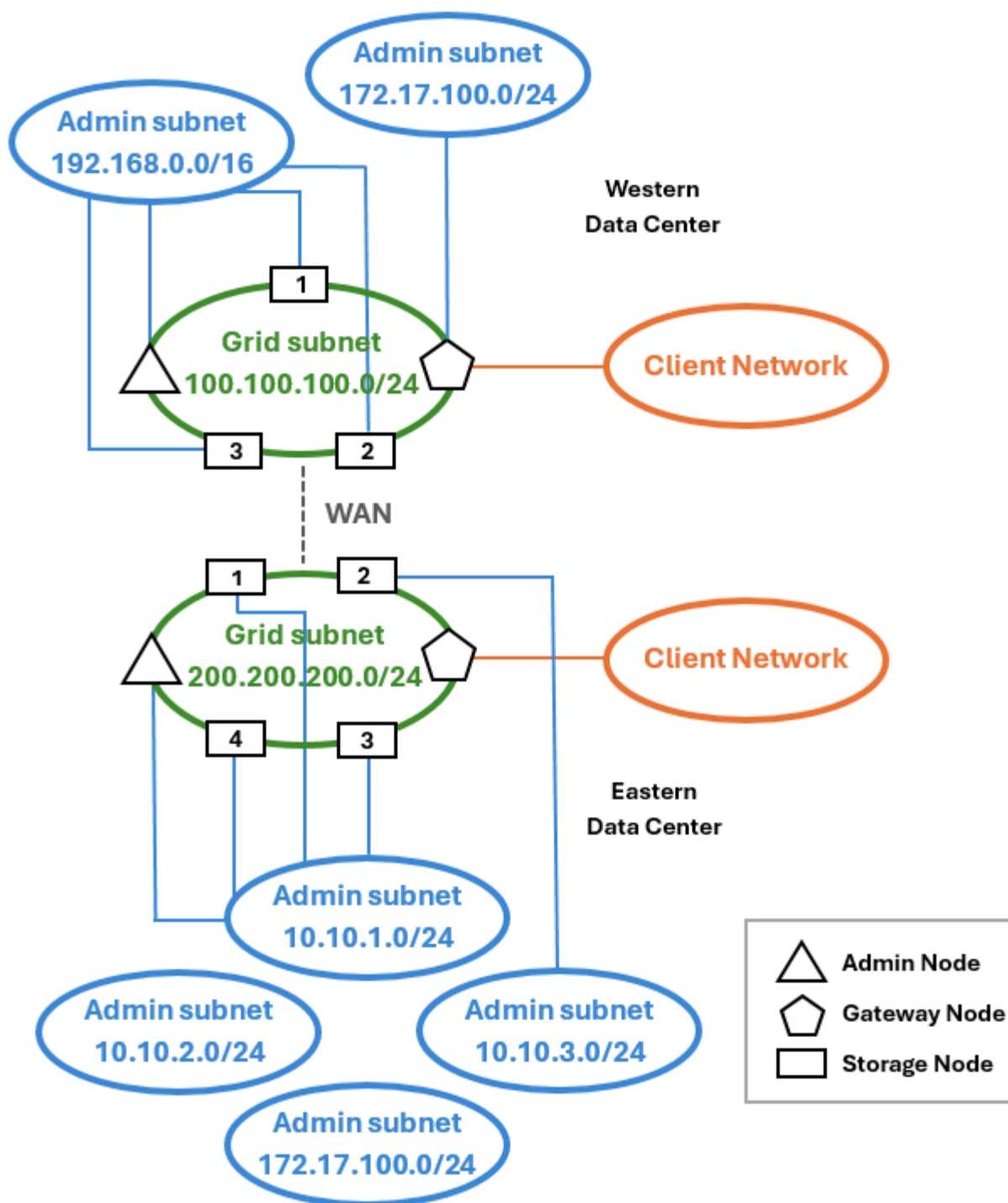
Topología para las tres redes

Puede configurar las tres redes en una topología de red que consta de una red de cuadrícula privada, redes de administración específicas del sitio limitadas y redes de cliente abiertas. El uso de puntos finales de balanceador de carga y redes de clientes no confiables puede brindar seguridad adicional si es necesario.

En este ejemplo:

- La red Grid 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 las funciones administrativas.
- La red de cliente se utiliza para el tráfico relacionado con las solicitudes de cliente S3.

Ejemplo de topología: Red, administración y redes de clientes



Requisitos de red

Debe verificar que la infraestructura y la configuración de red actuales puedan soportar el diseño de red StorageGRID planificado.

Requisitos generales de red

Todas las implementaciones de StorageGRID deben poder admitir las siguientes conexiones.

Estas conexiones pueden ocurrir 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 entrantes de un administrador al nodo, generalmente a través de SSH. Acceso mediante navegador web al Administrador de red, al Administrador de inquilinos y al Instalador de dispositivos StorageGRID .
- **Conexiones de servidor NTP:** Conexión UDP saliente que recibe una respuesta UDP entrante.

El nodo de administración principal debe poder acceder al menos a un servidor NTP.

- **Conexiones de servidor DNS:** Conexión UDP saliente que recibe una respuesta UDP entrante.
- **Conexiones de servidor LDAP/Active Directory:** Conexión TCP saliente desde el servicio de identidad en los nodos de almacenamiento.
- *** AutoSupport*:** Conexión TCP saliente desde los nodos de administración a cualquiera de los `support.netapp.com` o un proxy configurado por el cliente.
- **Servidor de administración de claves externo:** Conexión TCP saliente desde cada nodo del dispositivo con cifrado de nodo habilitado.
- Conexiones TCP entrantes desde clientes S3.
- Solicitudes salientes de servicios de la plataforma StorageGRID , como la replicación de CloudMirror o de grupos de almacenamiento en la nube.

Si StorageGRID no puede comunicarse con ninguno de los servidores NTP o DNS provistos mediante las reglas de enrutamiento predeterminadas, intentará comunicarse automáticamente 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 esa red se utilice para todos los intentos futuros de conectarse a ella.



Si bien puede utilizar estas rutas de host descubiertas automáticamente, en general debe configurar manualmente las rutas DNS y NTP para garantizar la conectividad en caso de que falle el descubrimiento automático.

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

Solo se admiten conexiones de cliente S3 y conexiones administrativas SSH, Grid Manager y Tenant Manager a través de interfaces VLAN. Las conexiones salientes, como a servidores NTP, DNS, LDAP, AutoSupport y KMS, deben realizarse directamente a través de las interfaces de red de cliente, administrador o cuadrícula. Si la interfaz está configurada como troncal para soportar interfaces VLAN, este tráfico fluirá a través de la VLAN nativa de la interfaz, tal como esté configurada en el conmutador.

Redes de área amplia (WAN) para múltiples 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 del cliente. La replicación de datos o la codificación de borrado entre sitios, la expansión de nodos o sitios, la recuperación de nodos y otras operaciones o configuraciones requerirán ancho de banda adicional.

Los requisitos reales de ancho de banda mínimo de WAN dependen de la actividad del cliente y del esquema de protección ILM. Para obtener ayuda para estimar los requisitos mínimos de ancho de banda de WAN,

comuníquese con su consultor de servicios profesionales de NetApp .

Conexiones para nodos de administración y nodos de puerta de enlace

Los nodos de administración siempre deben estar protegidos de clientes que no sean de confianza, como aquellos en Internet abierto. Debe asegurarse de que ningún cliente no confiable pueda acceder a ningún nodo de administración en la red Grid, la red de administración o la red de clientes.

Los nodos de administración y los nodos de puerta de enlace que planea agregar a grupos de alta disponibilidad deben configurarse con una dirección IP estática. Para obtener más información, consulte ["Administrar 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 Grid entre nodos Grid o entre sitios StorageGRID . Cuando se utilizan direcciones IPv4 privadas para la red de cuadrícula, dichas direcciones deben ser enrutables directamente desde cada nodo de la red en cada sitio. Sin embargo, según sea necesario, puede utilizar NAT entre clientes externos y nodos de la red, por ejemplo, para proporcionar una dirección IP pública para un nodo de puerta de enlace. El uso de NAT para unir un segmento de red pública solo es posible cuando se emplea una aplicación de tunelización que sea transparente para todos los nodos de la red, lo que significa que los nodos de la red no requieren conocimiento de direcciones IP públicas.

Requisitos específicos de la red

Siga los requisitos para cada tipo de red StorageGRID .

Puertas de enlace y enrutadores de red

- Si se configura, la puerta de enlace para una red determinada debe estar dentro de la subred de la red específica.
- Si configura una interfaz utilizando direccionamiento estático, debe especificar una dirección de puerta de enlace distinta de 0.0.0.0.
- Si no tiene una puerta de enlace, la mejor práctica es configurar la dirección de la puerta de enlace para que sea la dirección IP de la interfaz de red.

Subredes



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

El administrador de cuadrícula aplica las siguientes restricciones durante la implementación. Se proporcionan aquí para ayudar en la planificación de la red previa a la implementación.

- 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 superponerse a la subred de ninguna otra interfaz configurada en el mismo nodo.
- No utilice subredes que contengan las siguientes direcciones IPv4 para la red de cuadrícula, la red de administración o la red de cliente de ningún nodo:
 - 192.168.130.101
 - 192.168.131.101

- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

Por ejemplo, no utilice los siguientes rangos de subred para la red de cuadrícula, la red de administración o la red de cliente de ningún nodo:

- 192.168.130.0/24 porque este rango de subred contiene las direcciones IP 192.168.130.101 y 192.168.130.102
- 192.168.131.0/24 porque este rango de subred contiene las direcciones IP 192.168.131.101 y 192.168.131.102
- 198.51.100.0/24 porque este rango de subred contiene las direcciones IP 198.51.100.2 y 198.51.100.4
- La subred de la red Grid para cada nodo debe incluirse en el GNSL.
- La subred de red de administración no puede superponerse a la subred de red de cuadrícula, a la subred de red de cliente ni a ninguna subred en GNSL.
- Las subredes del AESL no pueden superponerse con ninguna subred del GNSL.
- La subred de la red del cliente no puede superponerse a la subred de la red de cuadrícula, a la subred de la red de administración, a ninguna subred de GNSL ni a ninguna subred de AESL.

Red de cuadrícula

- En el momento de la implementación, cada nodo de la red debe estar conectado a la red de la red y debe poder comunicarse con el nodo de administración principal mediante la configuración de red que especifique al implementar el nodo.
- Durante las operaciones normales de la red, cada nodo de la red debe poder comunicarse con todos los demás nodos de la red a través de la red.



La red Grid debe ser directamente enrutable 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 la red de cuadrícula (GNSL). Se crean rutas estáticas en todos los nodos para cada subred en GNSL.
- Si la interfaz de red de cuadrícula está configurada como troncal para admitir interfaces VLAN, la VLAN nativa del troncal debe ser la VLAN utilizada para el tráfico de red de cuadrícula. Todos los nodos de la red deben ser accesibles a través de la VLAN nativa troncal.

Red de administración

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

Los usos típicos de la red de administración 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 Grid o la red del cliente.



La red de administración y AESL pueden ser únicos para 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 conexiones entrantes desde subredes externas. Las rutas estáticas se generan automáticamente en cada nodo para cada subred en el AESL.

Red de clientes

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

- La red de clientes está diseñada para soportar el tráfico de los clientes S3. Si se configura, la puerta de enlace de la red del cliente se convierte en la puerta de enlace predeterminada del nodo.
- Si usa una red de cliente, puede ayudar a proteger StorageGRID de ataques hostiles al aceptar tráfico de cliente entrante solo en puntos finales del balanceador de carga configurados explícitamente. Ver ["Configurar los puntos finales del balanceador de carga"](#).
- Si la interfaz de red del cliente está configurada como un enlace troncal para admitir interfaces VLAN, considere si es necesario configurar la interfaz de red del cliente (eth2). Si está configurado, el tráfico de la red del cliente fluirá a través de la VLAN nativa del tronco, tal como se configuró en el conmutador.

Información relacionada

["Cambiar la configuración de la red del nodo"](#)

Consideraciones de red específicas de la implementación

Implementaciones de Linux

Para lograr eficiencia, confiabilidad y seguridad, el sistema StorageGRID se ejecuta en Linux como una colección de motores de contenedores. No se requiere la configuración de red relacionada con el motor de contenedores en un sistema StorageGRID.

Utilice un dispositivo que no sea de enlace, como una VLAN o un par 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 del contenedor. Hacerlo podría impedir el inicio del nodo debido a un problema del kernel con el uso de macvlan con dispositivos de enlace y puente en el espacio de nombres del contenedor.

Consulte las instrucciones de instalación para ["Red Hat Enterprise Linux"](#) o ["Ubuntu o Debian"](#) Despliegues.

Configuración de red de host para implementaciones de motores de contenedores

Antes de comenzar su implementación de StorageGRID en una plataforma de motor de contenedores, determine qué redes (Grid, Admin, Client) utilizará cada nodo. Debe asegurarse de que la interfaz de red de cada nodo esté configurada en la interfaz de host física o virtual correcta y que cada red tenga suficiente ancho de banda.

Hosts físicos

Si está utilizando hosts físicos para soportar nodos de red:

- 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 futura migración de nodos.

- Obtenga una dirección IP para el host físico.



Una interfaz física en el host puede ser utilizada por el propio host y uno o más nodos que se ejecutan en el host. Cualquier dirección IP asignada al host o a los nodos que utilizan esta interfaz debe ser única. El host y el nodo no pueden compartir direcciones IP.

- Abra los puertos necesarios para el host.
- Si pretende utilizar interfaces VLAN en StorageGRID, el host debe tener una o más interfaces troncales que proporcionen acceso a las VLAN deseadas. Estas interfaces se pueden pasar al contenedor de nodo como eth0, eth2 o como interfaces adicionales. Para agregar interfaces troncales o de acceso, consulte lo siguiente:
 - **RHEL (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Ubuntu o Debian (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **RHEL, Ubuntu o Debian (después de instalar el nodo):** ["Linux: Agregar interfaces troncales o de acceso a un nodo"](#)

Recomendaciones de ancho de banda mínimo

La siguiente tabla proporciona las recomendaciones de ancho de banda de LAN mínimo para cada tipo de nodo StorageGRID y cada tipo de red. Debe proporcionar a cada host físico o virtual suficiente ancho de banda de red para cumplir con los requisitos mínimos agregados 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		
	Red	Administración	Cliente
	Ancho de banda LAN mínimo	Administración	10 Gbps
1 Gbps	1 Gbps	Puerta	10 Gbps
1 Gbps	10 Gbps	Almacenamiento	10 Gbps
1 Gbps	10 Gbps	Archivo	10 Gbps



Esta tabla no incluye el ancho de banda SAN, que 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 separadas en cada host para proporcionar suficiente ancho de banda SAN. Para evitar la introducción de un cuello de botella, el ancho de banda de SAN para un host determinado debe coincidir aproximadamente con el ancho de banda de red del nodo de almacenamiento agregado para todos los nodos de almacenamiento que se ejecutan en ese host.

Utilice la tabla para determinar la cantidad mínima de interfaces de red a aprovisionar en cada host, según la cantidad y el tipo de nodos StorageGRID que planea ejecutar en ese host.

Por ejemplo, para ejecutar un nodo de administración, un nodo de puerta de enlace y un nodo de

almacenamiento en un solo host:

- Conecte las redes de red y de administración en el nodo de administración (requiere $10 + 1 = 11$ Gbps)
- Conecte las redes de red y de cliente en el nodo de puerta de enlace (requiere $10 + 10 = 20$ Gbps)
- Conectar la red de cuadrícula 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 podría satisfacerse con dos interfaces de 40 Gbps o cinco interfaces de 10 Gbps, potencialmente agregadas en troncales y luego compartidas por las tres o más VLAN que transportan las subredes Grid, Admin y Client locales al centro de datos físico que contiene el host.

Para conocer algunas formas recomendadas de configurar recursos físicos y de red en los hosts de su clúster StorageGRID para prepararse para su implementación de StorageGRID, consulte lo siguiente:

- ["Configurar la red del host \(Red Hat Enterprise Linux\)"](#)
- ["Configurar la red del host \(Ubuntu o Debian\)"](#)

Redes y puertos para servicios de plataforma y grupos de almacenamiento en la nube

Si planea utilizar los servicios de la plataforma StorageGRID o grupos de almacenamiento en la nube, debe configurar la red de cuadrícula y los firewalls para garantizar que se pueda llegar a los puntos finales de destino.

Redes para servicios de plataforma

Como se describe en ["Gestionar servicios de plataforma para inquilinos"](#) y ["Administrar los servicios de la plataforma"](#) Los servicios de la plataforma incluyen servicios externos que proporcionan integración de búsqueda, notificación de eventos y replicación de CloudMirror.

Los servicios de plataforma requieren acceso desde los nodos de almacenamiento que alojan el servicio StorageGRID ADC a los puntos finales de servicio externos. Algunos ejemplos de cómo proporcionar acceso incluyen:

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

Redes para grupos de almacenamiento en la nube

Los grupos de almacenamiento en la nube también requieren acceso desde los nodos de almacenamiento a los puntos finales proporcionados por el servicio externo utilizado, como Amazon S3 Glacier o Microsoft Azure Blob Storage. Para obtener más información, consulte ["¿Qué es un pool de almacenamiento en la nube?"](#).

Puertos para servicios de plataforma y grupos de almacenamiento en la nube

De forma predeterminada, los servicios de la plataforma y las comunicaciones del grupo de almacenamiento en la nube utilizan 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`

Se puede especificar un puerto diferente cuando se crea o edita el punto final. Ver ["Referencia del puerto de red"](#) .

Si utiliza un servidor proxy no transparente, también debe ["configurar los ajustes del proxy de almacenamiento"](#) para permitir que se envíen mensajes a puntos finales externos, como un punto final en Internet.

VLAN y servicios de plataforma y grupos de almacenamiento en la nube

No se pueden utilizar redes VLAN para servicios de plataforma o grupos de almacenamiento en la nube. Los puntos finales de destino deben ser accesibles a través de la red Grid, la red de administración o la red del cliente.

Nodos de dispositivos

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

Los puertos 10/25 GbE en los dispositivos StorageGRID se pueden configurar en modo de enlace fijo o agregado para conexiones a la red de cuadrícula y a la red del cliente.

Los puertos de red de administración de 1 GbE se pueden configurar en modo independiente o de respaldo activo para conexiones a la red de administración.

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

- ["Modos de enlace de puerto \(SG6160\)"](#)
- ["Modos de enlace de puerto \(SGF6112\)"](#)
- ["Modos de enlace de puerto \(controlador SG6000-CN\)"](#)
- ["Modos de enlace de puerto \(controlador SG5800\)"](#)
- ["Modos de enlace de puerto \(controlador E5700SG\)"](#)
- ["Modos de enlace de puerto \(SG110 y SG1100\)"](#)
- ["Modos de enlace de puerto \(SG100 y SG1000\)"](#)

Instalación y aprovisionamiento de redes

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

Despliegue inicial de un nodo

Cuando implementa un nodo por primera vez, debe conectarlo a la red Grid y asegurarse de que tenga 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 acceder a la configuración e instalación desde fuera de la red de cuadrícula.

Una red Grid 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 la red en subredes separadas se comuniquen con el nodo de administración principal antes de que se haya configurado la red.

Si es necesario, las subredes que contienen servidores NTP o que requieren acceso al Administrador de Grid o a la API también se pueden configurar como subredes de grid.

Registro automático de nodos con el nodo de administración principal

Una vez implementados los nodos, estos se registran en el nodo de administración principal mediante la red Grid. Luego puede utilizar el Administrador de cuadrícula, el `configure-storagegrid.py` Script de Python o API de instalación para configurar la red y aprobar los nodos registrados. Durante la configuración de la red, puede configurar múltiples subredes de red. Se crearán rutas estáticas a estas subredes a través de la puerta de enlace de la red Grid en cada nodo cuando complete la configuración de la red.

Deshabilitar la red de administración o la red de cliente

Si desea deshabilitar la red de administración o la red de clientes, puede eliminar la configuración de estas durante el proceso de aprobación del nodo o puede usar la herramienta Cambiar IP una vez completada la instalación (consulte "[Configurar direcciones IP](#)").

Pautas posteriores a la instalación

Después de completar la implementación y configuración del nodo de la red, siga estas pautas para el direccionamiento DHCP y los cambios de configuración de red.

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

Sólo se puede configurar DHCP durante la fase de implementación. No se puede configurar DHCP durante la configuración.



Los nodos se reinician cuando la configuración de la red Grid se modifica mediante DHCP, lo que puede provocar interrupciones si un cambio de DHCP afecta a varios nodos al mismo tiempo.

- Debe utilizar los procedimientos de Cambio de IP si desea cambiar direcciones IP, máscaras de subred y puertas de enlace predeterminadas para un nodo de la red. Ver "[Configurar direcciones IP](#)".
- Si realiza cambios en la configuración de red, incluidos cambios de enrutamiento y puerta de enlace, es posible que se pierda la conectividad del cliente con el nodo de administración principal y otros nodos de la red. Dependiendo de los cambios de red aplicados, es posible que sea necesario restablecer estas conexiones.

Referencia del puerto de red

Comunicaciones internas de los nodos de la red

El firewall interno de StorageGRID permite conexiones entrantes a puertos específicos en la red Grid. También se aceptan conexiones en los puertos definidos por los puntos finales del balanceador de carga.



NetApp recomienda que habilite el tráfico del Protocolo de mensajes de control de Internet (ICMP) entre los nodos de la red. Permitir el tráfico ICMP puede mejorar el rendimiento de la conmutación por error cuando no se puede acceder a un nodo de la red.

Además de ICMP y los puertos enumerados en la tabla, StorageGRID utiliza el Protocolo de redundancia de enrutador virtual (VRRP). VRRP es un protocolo de Internet que utiliza el protocolo IP número 112. StorageGRID utiliza VRRP únicamente en modo de unidifusión. VRRP solo se requiere si ["grupos de alta disponibilidad"](#) están configurados.

Directrices para nodos basados en Linux

Si las políticas de red empresarial restringen el acceso a cualquiera de estos puertos, puede reasignar los puertos en el momento de la implementación utilizando un parámetro de configuración de implementación. Para obtener más información sobre la reasignación de puertos y los parámetros de configuración de implementación, consulte:

- ["Instalar StorageGRID en Red Hat Enterprise Linux"](#)
- ["Instalar StorageGRID en Ubuntu o Debian"](#)

Directrices para nodos basados en VMware

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

Si las políticas de red empresarial restringen el acceso a cualquiera de estos puertos, puede reasignar los puertos cuando implemente nodos mediante VMware vSphere Web Client o mediante una configuración de archivo al automatizar la implementación de nodos de la red. Para obtener más información sobre la reasignación de puertos y los parámetros de configuración de implementación, consulte ["Instalar StorageGRID en VMware"](#).

Directrices para los nodos de dispositivos

Si las políticas de red empresarial restringen el acceso a cualquiera de estos puertos, puede reasignar los puertos mediante el instalador del dispositivo StorageGRID. Ver ["Opcional: Reasignar los puertos de red para el dispositivo"](#).

Puertos internos de StorageGRID

Puerto	TCP o UDP	De	A	Detalles
22	TCP	Nodo de administración principal	Todos los nodos	Para los procedimientos de mantenimiento, el nodo de administración principal debe poder comunicarse con todos los demás nodos mediante SSH en el puerto 22. Permitir el tráfico SSH desde otros nodos es opcional.
80	TCP	Accesorios	Nodo de administración principal	Los dispositivos StorageGRID lo utilizan para comunicarse con el nodo de administración principal para iniciar la instalación.
123	UDP	Todos los nodos	Todos los nodos	Servicio de protocolo de tiempo de red. Cada nodo sincroniza su hora con la de todos los demás nodos mediante NTP.

Puerto	TCP o UDP	De	A	Detalles
443	TCP	Todos los nodos	Nodo de administración principal	Se utiliza para comunicar el estado al nodo de administración principal durante la instalación y otros procedimientos de mantenimiento.
1055	TCP	Todos los nodos	Nodo de administración principal	Tráfico interno para instalación, ampliación, recuperación y otros procedimientos de mantenimiento.
1139	TCP	Nodos de almacenamiento	Nodos de almacenamiento	Tráfico interno entre nodos de almacenamiento.
1501	TCP	Todos los nodos	Nodos de almacenamiento con ADC	Informes, auditoría y configuración de tráfico interno.
1502	TCP	Todos los nodos	Nodos de almacenamiento	Tráfico interno relacionado con S3 y Swift.
1504	TCP	Todos los nodos	Nodos de administración	Servicio NMS de informes y configuración de tráfico interno.
1505	TCP	Todos los nodos	Nodos de administración	Tráfico interno del servicio AMS.
1506	TCP	Todos los nodos	Todos los nodos	Estado del servidor tráfico interno.
1507	TCP	Todos los nodos	Nodos de puerta de enlace	Balanceador de carga de tráfico interno.
1508	TCP	Todos los nodos	Nodo de administración principal	Gestión de configuración de tráfico interno.
1511	TCP	Todos los nodos	Nodos de almacenamiento	Tráfico interno de metadatos.

Puerto	TCP o UDP	De	A	Detalles
5353	UDP	Todos los nodos	Todos los nodos	Proporciona el servicio DNS de multidifusión (mDNS) utilizado para cambios de IP de red completa y para el descubrimiento del nodo de administración principal durante la instalación, expansión y recuperación. Nota: La configuración de este puerto es opcional.
7001	TCP	Nodos de almacenamiento	Nodos de almacenamiento	Comunicación entre clústeres de nodos TLS de Cassandra.
7443	TCP	Todos los nodos	Nodo de administración principal	Tráfico interno para instalación, expansión, recuperación, otros procedimientos de mantenimiento e informes de errores.
8011	TCP	Todos los nodos	Nodo de administración principal	Tráfico interno para instalación, ampliación, recuperación y otros procedimientos de mantenimiento.
8443	TCP	Nodo de administración principal	Nodos de dispositivos	Tráfico interno relacionado con el procedimiento del 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, métricas y actualizaciones de red.
10226	TCP	Nodos de almacenamiento	Nodo de administración principal	Utilizado por los dispositivos StorageGRID para reenviar paquetes de AutoSupport desde E-Series SANtricity System Manager al nodo de administración principal.
10342	TCP	Todos los nodos	Nodo de administración principal	Tráfico interno para instalación, ampliación, recuperación y otros procedimientos de mantenimiento.
18000	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento con ADC	Tráfico interno del servicio de cuentas.

Puerto	TCP o UDP	De	A	Detalles
18001	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento con ADC	Tráfico interno de la Federación de Identidad.
18002	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento	Tráfico de API interna relacionado con protocolos de objetos.
18003	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento con ADC	La plataforma atiende el tráfico interno.
18017	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento	Tráfico interno del servicio Data Mover para grupos de almacenamiento en la nube.
18019	TCP	Todos los nodos	Todos los nodos	Servicio de fragmentos de tráfico interno para codificación de borrado y replicación
18082	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento	Tráfico interno relacionado con S3.
18083	TCP	Todos los nodos	Nodos de almacenamiento	Tráfico interno relacionado con Swift.
18086	TCP	Todos los nodos	Nodos de almacenamiento	Tráfico interno relacionado con el servicio LDR.
18200	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento	Estadísticas adicionales sobre solicitudes de clientes.
19000	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento con ADC	Tráfico interno del servicio Keystone .

Información relacionada

["Comunicaciones externas"](#)

Comunicaciones externas

Los clientes necesitan comunicarse con los nodos de la red para ingerir y recuperar contenido. Los puertos utilizados dependen de los protocolos de almacenamiento de objetos elegidos. Estos puertos deben ser accesibles para el cliente.

Acceso restringido a los puertos

Si las políticas de red empresarial restringen el acceso a cualquiera de los puertos, puede realizar una de las siguientes acciones:

- Usar ["puntos finales del balanceador de carga"](#) para permitir el acceso a puertos definidos por el usuario.
- Reasignar puertos al implementar nodos. Sin embargo, no debes reasignar los puntos finales del balanceador de carga. Consulte la información sobre la reasignación de puertos para su nodo StorageGRID :
 - ["Claves de reasignación de puertos para StorageGRID en Red Hat Enterprise Linux"](#)
 - ["Claves de reasignación de puertos para StorageGRID en Ubuntu o Debian"](#)
 - ["Reasignar puertos para StorageGRID en VMware"](#)
 - ["Opcional: Reasignar los puertos de red para el dispositivo"](#)

Puertos utilizados para comunicaciones externas

La siguiente tabla muestra los puertos utilizados para el tráfico hacia los nodos.



Esta lista no incluye puertos que podrían configurarse como ["puntos finales del balanceador de carga"](#).

Puerto	TCP o UDP	Protocolo	De	A	Detalles
22	TCP	SSH	Servicio de computadora portátil	Todos los nodos	Se requiere acceso a SSH o consola para procedimientos con pasos de consola. Opcionalmente, puede utilizar el puerto 2022 en lugar del 22.
25	TCP	SMTP	Nodos de administración	Servidor de correo electrónico	Se utiliza para alertas y AutoSupport basado en correo electrónico. Puede anular la configuración del puerto predeterminado de 25 utilizando la página Servidores de correo electrónico.
53	TCP/UDP	DNS	Todos los nodos	servidores DNS	Utilizado para DNS.
67	UDP	DHCP	Todos los nodos	Servicio DHCP	Se utiliza opcionalmente para admitir la configuración de red basada en DHCP. El servicio dhclient no se ejecuta en cuadrículas configuradas estáticamente.

Puerto	TCP o UDP	Protocolo	De	A	Detalles
68	UDP	DHCP	Servicio DHCP	Todos los nodos	Se utiliza opcionalmente para admitir la configuración de red basada en DHCP. El servicio dhclient no se ejecuta en redes que utilizan direcciones IP estáticas.
80	TCP	HTTP	Explorador	Nodos de administración	El puerto 80 redirige al puerto 443 para la interfaz de usuario del nodo de administración.
80	TCP	HTTP	Explorador	Accesorios	El puerto 80 redirige al puerto 8443 para el instalador del dispositivo StorageGRID .
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 la configuración del puerto HTTP predeterminada de 80 al crear un punto final.
80	TCP	HTTP	Nodos de almacenamiento	AWS	Solicitudes de grupos de almacenamiento en la nube enviadas a destinos de AWS que utilizan HTTP. Los administradores de la red pueden anular la configuración del puerto HTTP predeterminada de 80 al configurar un grupo de almacenamiento en la nube.
111	TCP/UDP	RPCBind	Cliente NFS	Nodos de administración	Utilizado por la exportación de auditoría basada en NFS (portmap). Nota: Este puerto solo es necesario si la exportación de auditoría basada en NFS está habilitada. Nota: La compatibilidad con NFS ha quedado obsoleta y se eliminará en una versión futura.
123	UDP	NTP	Nodos NTP primarios	NTP externo	Servicio de protocolo de tiempo de red. Los nodos seleccionados como fuentes NTP principales también sincronizan las horas del reloj con las fuentes de tiempo NTP externas.

Puerto	TCP o UDP	Protocolo	De	A	Detalles
161	TCP/UDP	SNMP	Cliente SNMP	Todos los nodos	Se utiliza para sondeo SNMP. Todos los nodos proporcionan información básica; los nodos de administración también proporcionan datos de alerta. El valor predeterminado es el puerto UDP 161 cuando está configurado. Nota: Este puerto solo es obligatorio y solo se abre en el firewall del nodo si SNMP está configurado. Si planea utilizar SNMP, puede configurar puertos alternativos. Nota: Para obtener información sobre el uso de SNMP con StorageGRID, comuníquese con su representante de cuenta de NetApp .
162	TCP/UDP	Notificaciones SNMP	Todos los nodos	Destinos de notificación	Las notificaciones y trampas SNMP salientes se establecen de manera predeterminada en el puerto UDP 162. Nota: Este puerto solo es necesario si SNMP está habilitado y los destinos de notificación están configurados. Si planea utilizar SNMP, puede configurar puertos alternativos. Nota: Para obtener información sobre el uso de SNMP con StorageGRID, comuníquese con su representante de cuenta de NetApp .
389	TCP/UDP	LDAP	Nodos de almacenamiento con ADC	Directorio activo/LDAP	Se utiliza para conectarse a un servidor Active Directory o LDAP para la federación de identidad.
443	TCP	HTTPS	Explorador	Nodos de administración	Utilizado por navegadores web y clientes de API de administración para acceder al Administrador de red y al Administrador de inquilinos. Nota: Si cierra los puertos 443 o 8443 de Grid Manager, todos los usuarios que estén conectados actualmente en un puerto bloqueado, incluido usted, perderán el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones privilegiadas. Referirse a "Configurar los controles del firewall" para configurar direcciones IP privilegiadas.

Puerto	TCP o UDP	Protocolo	De	A	Detalles
443	TCP	HTTPS	Nodos de administración	Directorio activo	Utilizado por los nodos de administración que se conectan a Active Directory si el inicio de sesión único (SSO) está habilitado.
443	TCP	HTTPS	Nodos de almacenamiento con ADC	AWS	Se utiliza para mensajes de servicios de plataforma enviados a AWS u otros servicios externos que utilizan HTTPS. Los inquilinos pueden anular la configuración del puerto HTTP predeterminada de 443 al crear un punto final.
443	TCP	HTTPS	Nodos de almacenamiento	AWS	Solicitudes de grupos de almacenamiento en la nube enviadas a destinos de AWS que usan HTTPS. Los administradores de la red pueden anular la configuración del puerto HTTPS predeterminada de 443 al configurar un grupo de almacenamiento en la nube.
903	TCP	Sistema Nacional de Archivos	Cliente NFS	Nodos de administración	Utilizado por la exportación de auditoría basada en NFS(<code>rpc.mountd</code>). Nota: Este puerto solo es necesario si la exportación de auditoría basada en NFS está habilitada. Nota: La compatibilidad con NFS ha quedado obsoleta y se eliminará en una versión futura.
2022	TCP	SSH	Servicio de computadora portátil	Todos los nodos	Se requiere acceso a SSH o consola para procedimientos con pasos de consola. Opcionalmente, puede utilizar el puerto 22 en lugar del 2022.
2049	TCP	Sistema Nacional de Archivos	Cliente NFS	Nodos de administración	Utilizado por la exportación de auditoría basada en NFS (nfs). Nota: Este puerto solo es necesario si la exportación de auditoría basada en NFS está habilitada. Nota: La compatibilidad con NFS ha quedado obsoleta y se eliminará en una versión futura.

Puerto	TCP o UDP	Protocolo	De	A	Detalles
5353	UDP	mDNS	Todos los nodos	Todos los nodos	Proporciona el servicio DNS de multidifusión (mDNS) utilizado para cambios de IP de red completa y para el descubrimiento del nodo de administración principal durante la instalación, expansión y recuperación. Nota: La configuración de este puerto es opcional.
5696	TCP	KMIP	Aparato	KMS	Tráfico externo del Protocolo de interoperabilidad de administración de claves (KMIP) desde dispositivos configurados para el cifrado de nodos al Servidor de administración de claves (KMS), a menos que se especifique un puerto diferente en la página de configuración de KMS del instalador del dispositivo StorageGRID .
8022	TCP	SSH	Servicio de computadora portátil	Todos los nodos	SSH en el puerto 8022 otorga acceso al sistema operativo base en las plataformas de dispositivos y nodos virtuales para soporte y resolución de problemas. Este puerto no se utiliza para nodos basados en Linux (bare metal) y no es necesario que sea accesible entre nodos de la red o durante operaciones normales.
8443	TCP	HTTPS	Explorador	Nodos de administración	Opcional. Utilizado por navegadores web y clientes API de administración para acceder al Administrador de Grid. Se puede utilizar para separar las comunicaciones entre Grid Manager y Tenant Manager. Nota: Si cierra los puertos 443 o 8443 de Grid Manager, todos los usuarios que estén conectados actualmente en un puerto bloqueado, incluido usted, perderán el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones privilegiadas. Referirse a "Configurar los controles del firewall" para configurar direcciones IP privilegiadas.
8443	TCP	HTTPS	Explorador	Accesorios	Utilizado por navegadores web y clientes de API de administración para acceder al instalador del dispositivo StorageGRID . Nota: El puerto 443 redirige al puerto 8443 para el instalador del dispositivo StorageGRID .

Puerto	TCP o UDP	Protocolo	De	A	Detalles
9022	TCP	SSH	Servicio de computadora portátil	Accesorios	Otorga acceso a los dispositivos StorageGRID en modo de preconfiguración para soporte y resolución de problemas. No es necesario que este puerto sea accesible entre nodos de la red o durante operaciones normales.
9091	TCP	HTTPS	Servicio externo de Grafana	Nodos de administración	Utilizado por servicios externos de Grafana para el acceso seguro al servicio StorageGRID Prometheus. Nota: Este puerto solo es necesario si el acceso a Prometheus basado en certificado está habilitado.
9092	TCP	Kafka	Nodos de almacenamiento con ADC	Clúster de Kafka	Se utiliza para mensajes de servicios de plataforma enviados a un clúster de Kafka. Los inquilinos pueden anular la configuración del puerto Kafka predeterminada de 9092 al crear un punto final.
9443	TCP	HTTPS	Explorador	Nodos de administración	Opcional. Utilizado por navegadores web y clientes de API de administración para acceder al Administrador de inquilinos. Se puede utilizar para separar las comunicaciones entre Grid Manager y Tenant Manager.
18082	TCP	HTTPS	Clientes S3	Nodos de almacenamiento	Tráfico del cliente S3 directamente a los nodos de almacenamiento (HTTPS).
18083	TCP	HTTPS	Clientes rápidos	Nodos de almacenamiento	Tráfico de clientes Swift directamente a nodos de almacenamiento (HTTPS).
18084	TCP	HTTP	Clientes S3	Nodos de almacenamiento	Tráfico del cliente S3 directamente a los nodos de almacenamiento (HTTP).
18085	TCP	HTTP	Clientes rápidos	Nodos de almacenamiento	Tráfico de clientes Swift directamente a nodos de almacenamiento (HTTP).

Puerto	TCP o UDP	Protocolo	De	A	Detalles
23000-23999	TCP	HTTPS	Todos los nodos de la red de origen para la replicación entre redes	Nodos de administración y nodos de puerta de enlace en la red de destino para la replicación entre redes	Esta gama de puertos está reservada para conexiones de federación de red. Ambas redes en una conexión dada utilizan el mismo puerto.

Inicio rápido para StorageGRID

Siga estos pasos de alto nivel para configurar y utilizar cualquier sistema StorageGRID .

1

Aprender, planificar y recopilar datos

Trabaje con su representante de cuenta de NetApp para comprender las opciones y planificar su nuevo sistema StorageGRID . Considere este tipo de preguntas:

- ¿Cuántos datos de objetos espera almacenar inicialmente y a lo largo del tiempo?
- ¿Cuántos sitios necesitas?
- ¿Cuántos y qué tipos de nodos necesitas en cada sitio?
- ¿Qué redes StorageGRID utilizarás?
- ¿Quién utilizará tu cuadrícula para almacenar objetos? ¿Qué aplicaciones utilizarán?
- ¿Tiene algún requisito especial de seguridad o almacenamiento?
- ¿Necesita cumplir con algún requisito legal o reglamentario?

Opcionalmente, trabaje con su consultor de servicios profesionales de NetApp para acceder a la herramienta NetApp ConfigBuilder para completar un libro de trabajo de configuración para usar al instalar e implementar su nuevo sistema. También puede utilizar esta herramienta para ayudar a automatizar la configuración de cualquier dispositivo StorageGRID . Ver "[Automatizar la instalación y configuración de dispositivos](#)" .

Revisar "[Obtenga más información sobre StorageGRID](#)" y el "[Pautas para establecer redes](#)" .

2

Instalar nodos

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

Para completar la instalación, instale el software StorageGRID en cada dispositivo o host de software y conecte los nodos a una red. Durante este paso, usted proporciona los nombres de los sitios y nodos, los detalles de la subred y las direcciones IP de sus servidores NTP y DNS.

Aprenda cómo:

- ["Instalar el hardware del dispositivo"](#)
- ["Instalar StorageGRID en Red Hat Enterprise Linux"](#)
- ["Instalar StorageGRID en Ubuntu o Debian"](#)
- ["Instalar StorageGRID en VMware"](#)

3

Sign in y verifique el estado del sistema

Tan pronto como instale el nodo de administración principal, podrá iniciar sesión en el Administrador de Grid. Desde allí, puede revisar el estado general de su nuevo sistema, habilitar AutoSupport y correos electrónicos de alerta, y configurar nombres de dominio de puntos finales S3.

Aprenda cómo:

- ["Sign in en el Administrador de cuadrícula"](#)
- ["Monitorear la salud del sistema"](#)
- ["Configurar AutoSupport"](#)
- ["Configurar notificaciones por correo electrónico para alertas"](#)
- ["Configurar nombres de dominio de puntos finales S3"](#)

4

Configurar y administrar

Las tareas de configuración que debe realizar para un nuevo sistema StorageGRID dependen de cómo utilizará su red. Como mínimo, debe configurar el acceso al sistema, utilizar los asistentes FabricPool y S3 y administrar diversas configuraciones de almacenamiento y seguridad.

Aprenda cómo:

- ["Controlar el acceso a StorageGRID"](#)
- ["Utilice el asistente de configuración de S3"](#)
- ["Utilice el asistente de configuración de FabricPool"](#)
- ["Gestionar la seguridad"](#)
- ["Endurecimiento del sistema"](#)

5

Configurar ILM

Usted controla la ubicación y la duración de cada objeto en su sistema StorageGRID configurando una política de administración del ciclo de vida de la información (ILM) que consta de una o más reglas ILM. Las reglas de ILM indican a StorageGRID cómo crear y distribuir copias de datos de objetos y cómo administrar esas copias a lo largo del tiempo.

Aprenda cómo: ["Administrar objetos con ILM"](#)

6

Utilice StorageGRID

Una vez completada la configuración inicial, las cuentas de inquilinos de StorageGRID pueden usar aplicaciones cliente S3 para ingerir, recuperar y eliminar objetos.

Aprenda cómo:

- ["Utilice una cuenta de inquilino"](#)
- ["Utilice la API REST de S3"](#)

7

Monitorear y solucionar problemas

Cuando su sistema esté en funcionamiento, debe supervisar sus actividades periódicamente y solucionar problemas y resolver cualquier alerta. Es posible que también desee configurar un servidor syslog externo, utilizar la monitorización SNMP o recopilar datos adicionales.

Aprenda cómo:

- ["Monitorear StorageGRID"](#)
- ["Solucionar problemas de StorageGRID"](#)

8

Expandir, mantener y recuperar

Puede agregar nodos o sitios para ampliar la capacidad o funcionalidad de su sistema. También puede realizar varios procedimientos de mantenimiento para recuperarse de fallas o para mantener su sistema StorageGRID actualizado y funcionando de manera eficiente.

Aprenda cómo:

- ["Expandir una cuadrícula"](#)
- ["Mantenga su red"](#)
- ["Recuperar nodos"](#)

Instalar, actualizar y reparar StorageGRID

Dispositivos StorageGRID

Ir a ["Documentación del dispositivo StorageGRID"](#) para aprender a instalar, configurar y mantener dispositivos de almacenamiento y servicios StorageGRID .

Instalar StorageGRID en Red Hat Enterprise Linux

Inicio rápido para la instalación de StorageGRID en Red Hat Enterprise Linux

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

1

Preparación

- Conozca más sobre ["Arquitectura y topología de red de StorageGRID"](#) .
- Conozca los detalles de ["Redes StorageGRID"](#) .
- Reúne y prepara el ["Información y materiales necesarios"](#) .
- Preparar lo necesario ["CPU y RAM"](#) .
- Mantener ["requisitos de almacenamiento y rendimiento"](#) .
- ["Preparar los servidores Linux"](#) que alojará sus nodos StorageGRID .

2

Despliegue

Implementar nodos de red. Cuando se implementan nodos de red, estos se crean como parte del sistema StorageGRID y se conectan a una o más redes.

- Para implementar nodos de red basados en software en los hosts que preparó en el paso 1, use la línea de comandos de Linux y ["archivos de configuración de nodos"](#) .
- Para implementar nodos del dispositivo StorageGRID , siga las instrucciones ["Inicio rápido para la instalación de hardware"](#) .

3

Configuración

Cuando se hayan implementado todos los nodos, utilice el Administrador de cuadrícula para ["Configurar la red y completar la instalación"](#) .

Automatizar la instalación

Para ahorrar tiempo y brindar coherencia, puede automatizar la instalación del servicio de host StorageGRID y la configuración de los nodos de la red.

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

- Instalación de RHEL
- Configuración de redes y almacenamiento
- Instalación del motor de contenedores y el servicio de host StorageGRID
- Despliegue de nodos de red virtuales

Ver ["Automatice la instalación y configuración del servicio de host StorageGRID"](#) .

- Después de implementar los nodos de la red, ["automatizar la configuración del sistema StorageGRID"](#) utilizando el script de configuración de Python proporcionado en el archivo de instalación.
- ["Automatizar la instalación y configuración de nodos de red de dispositivos"](#)
- Si es un desarrollador avanzado de implementaciones de StorageGRID , automatice la instalación de nodos de la red mediante el uso de ["API REST de instalación"](#) .

Planifique y prepare la instalación en Red Hat

Información y materiales necesarios

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

Información requerida

Plan de red

Qué redes desea conectar a cada nodo de StorageGRID . StorageGRID admite múltiples redes para separación de tráfico, seguridad y conveniencia administrativa.

Ver StorageGRID ["Pautas para establecer redes"](#) .

Información de la red

Direcciones IP a asignar a cada nodo de la red y las direcciones IP de los servidores DNS y NTP.

Servidores para nodos de red

Identifique un conjunto de servidores (físicos, virtuales o ambos) que, en conjunto, proporcionen recursos suficientes para soportar la cantidad y el tipo de nodos StorageGRID que planea implementar.



Si su instalación de StorageGRID no utilizará nodos de almacenamiento del dispositivo StorageGRID (hardware), deberá utilizar almacenamiento RAID de hardware con caché de escritura respaldado por batería (BBWC). StorageGRID no admite el uso de redes de área de almacenamiento virtual (vSAN), RAID de software o ninguna protección RAID.

Migración de nodos (si es necesario)

Entender el ["Requisitos para la migración de nodos"](#) , si desea realizar mantenimiento programado en hosts físicos sin ninguna interrupción del servicio.

Información relacionada

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Materiales necesarios

Licencia de NetApp StorageGRID

Debe tener una licencia de NetApp válida y firmada digitalmente.



En el archivo de instalación de StorageGRID se incluye una licencia que no es de producción y que se puede utilizar para realizar pruebas y comprobar el concepto de las redes.

Archivo de instalación de StorageGRID

["Descargue el archivo de instalación de StorageGRID y extraiga los archivos"](#) .

Servicio de computadora portátil

El sistema StorageGRID se instala a través de una computadora portátil de servicio.

La computadora portátil de servicio debe tener:

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

Documentación de StorageGRID

- ["Notas de la versión"](#)
- ["Instrucciones para administrar StorageGRID"](#)

Descargue y extraiga los archivos de instalación de StorageGRID

Debe descargar el archivo de instalación de StorageGRID y extraer los archivos necesarios. Opcionalmente, puede verificar manualmente los archivos en el paquete de instalación.

Pasos

1. Ir a la ["Página de descargas de NetApp para StorageGRID"](#) .
2. Seleccione el botón para descargar la última versión o seleccione otra versión del menú desplegable y seleccione **Ir**.
3. Sign in con el nombre de usuario y la contraseña de su cuenta de NetApp .
4. Si aparece una declaración de Precaución/Lectura obligatoria, léala y seleccione la casilla de verificación.



Debe aplicar las revisiones necesarias 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 Acuerdo de licencia de usuario final, seleccione la casilla de verificación y luego seleccione **Aceptar y continuar**.
6. En la columna **Instalar StorageGRID**, seleccione el archivo de instalación .tgz o .zip para Red Hat Enterprise Linux.



Seleccione el .zip archivo si está ejecutando Windows en la computadora portátil de servicio.

7. Guarde el archivo de instalación.

8. Si necesita verificar el archivo de instalación:
 - a. Descargue el paquete de verificación de firma de código de StorageGRID . El nombre de archivo de este paquete utiliza el formato `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , dónde `<version-number>` es la versión del software StorageGRID .
 - b. Siga los pasos para ["verificar manualmente los archivos de instalación"](#) .
9. Extraiga los archivos del archivo de instalación.
10. Elige los archivos que necesitas.

Los archivos que necesita dependen de la topología de red planificada y de cómo implementará su 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
	Un 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.
	Paquete RPM para instalar el servicio de host StorageGRID en sus hosts RHEL.
Herramienta de scripting de implementación	Descripción
	Un script de Python utilizado para automatizar la configuración de un sistema StorageGRID .
	Un script de Python utilizado para automatizar la configuración de dispositivos StorageGRID .
	Un archivo de configuración de ejemplo para usar con el <code>configure-storagegrid.py</code> guion.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único está habilitado. También puede utilizar este script para la integración de Ping Federate.

Ruta y nombre de archivo	Descripción
	Un archivo de configuración en blanco para usar con el <code>configure-storagegrid.py</code> guion.
	Ejemplo de rol y manual de Ansible para configurar hosts RHEL para la implementación de contenedores StorageGRID . Puede personalizar el rol o el libro de jugadas según sea necesario.
	Un ejemplo de secuencia de comandos de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script de ayuda llamado por el compañero <code>storagegrid-ssoauth-azure.py</code> Script de Python para realizar interacciones de SSO con Azure.
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno de StorageGRID que no sea de producción para realizar pruebas de compatibilidad de actualización.

Verificar manualmente los archivos de instalación (opcional)

Si es necesario, puede verificar manualmente los archivos en el archivo de instalación de StorageGRID .

Antes de empezar

Tienes ["descargué el paquete de verificación"](#) desde ["Página de descargas de NetApp para StorageGRID"](#) .

Pasos

1. Extraiga los artefactos del paquete de verificación:

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Asegúrese de que se hayan extraído estos artefactos:

- Certificado de hoja: `Leaf-Cert.pem`
- Cadena de certificados: `CA-Int-Cert.pem`
- Cadena de respuesta de marca de tiempo: `TS-Cert.pem`
- Archivo de suma de comprobación: `sha256sum`

- Firma de suma de comprobación: sha256sum.sig
- Archivo de respuesta de marca de tiempo: sha256sum.sig.tsr

3. Utilice la cadena para verificar que el certificado de hoja sea válido.

Ejemplo: openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem

Resultado esperado: Leaf-Cert.pem: OK

4. Si el paso 2 falló debido a un certificado de hoja vencido, utilice el tsr archivo a verificar.

Ejemplo: openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr

Los resultados esperados incluyen: Verification: OK

5. Cree un archivo de clave pública a partir del certificado de hoja.

Ejemplo: openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub

Resultado esperado: *ninguno*

6. Utilice la clave pública para verificar la sha256sum archivo contra sha256sum.sig .

Ejemplo: openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum

Resultado esperado: Verified OK

7. Verificar el sha256sum contenido del archivo contra sumas de comprobación recién creadas.

Ejemplo: sha256sum -c sha256sum

Resultado esperado: <filename>: OK
<filename> es el nombre del archivo que descargaste.

8. ["Complete los pasos restantes"](#) para extraer y elegir los archivos apropiados del archivo de instalación.

Requisitos de software para Red Hat Enterprise Linux

Puede utilizar una máquina virtual para alojar cualquier tipo de nodo StorageGRID . Necesita una máquina virtual para cada nodo de la red.

Para instalar StorageGRID en Red Hat Enterprise Linux (RHEL), debe instalar algunos paquetes de software de terceros. Algunas distribuciones de Linux compatibles no contienen estos paquetes de forma predeterminada. Las versiones de paquetes de software en las que se prueban las instalaciones de StorageGRID incluyen las que se enumeran en esta página.

Si selecciona una distribución de Linux y una opción de instalación en tiempo de ejecución de contenedor que requiere alguno de estos paquetes, y la distribución de Linux no los instala automáticamente, instale una de las versiones enumeradas aquí si está disponible a través de su proveedor o del vendedor de soporte para su distribución de Linux. De lo contrario, utilice las versiones de paquetes predeterminadas disponibles de su proveedor.

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



La compatibilidad con Docker como motor de contenedores para implementaciones de solo software está obsoleta. Docker será reemplazado por otro motor de contenedores en una versión futura.

Versiones de Python probadas

- 3.5.2-2
- 3.6.8-2
- 3.6.8-38
- 3.6.9-1
- 3.7.3-1
- 3.8.10-0
- 3.9.2-1
- 3.9.10-2
- 3.9.16-1
- 3.10.6-1
- 3.11.2-6

Versiones de Podman probadas

- 3.2.3-0
- 3.4.4+ds1
- 4.1.1-7
- 4.2.0-11
- 4.3.1+ds1-8+b1
- 4.4.1-8
- 4.4.1-12

Versiones de Docker probadas



La compatibilidad con Docker está obsoleta y se eliminará en una versión futura.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23.0.6-1
- Docker-CE 24.0.2-1
- Docker-CE 24.0.4-1
- Docker-CE 24.0.5-1
- Docker-CE 24.0.7-1
- 1,5-2

Requisitos de CPU y RAM

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

Cada nodo de StorageGRID requiere los siguientes recursos mínimos:

- Núcleos de CPU: 8 por nodo
- RAM: depende de la RAM total disponible y de la cantidad de software que no sea StorageGRID que se ejecute en el sistema
 - Generalmente, al menos 24 GB por nodo y de 2 a 16 GB menos que la RAM total del sistema.
 - Un mínimo de 64 GB para cada inquilino que tendrá aproximadamente 5000 buckets

Los recursos de nodo de solo metadatos basados en software deben coincidir con los recursos de los nodos de almacenamiento existentes. Por ejemplo:

- Si el sitio StorageGRID existente utiliza dispositivos SG6000 o SG6100, los nodos de solo metadatos basados en software deben cumplir los siguientes requisitos mínimos:
 - 128 GB de RAM
 - CPU de 8 núcleos
 - SSD de 8 TB o almacenamiento equivalente para la base de datos Cassandra (rangedb/0)
- Si el sitio StorageGRID existente usa nodos de almacenamiento virtuales con 24 GB de RAM, CPU de 8 núcleos y 3 TB o 4 TB de almacenamiento de metadatos, los nodos solo de metadatos basados en software deben usar recursos similares (24 GB de RAM, CPU de 8 núcleos y 4 TB de almacenamiento de metadatos (rangedb/0).

Al agregar un nuevo sitio StorageGRID , la capacidad total de metadatos del nuevo sitio debe coincidir, como mínimo, con los sitios StorageGRID existentes y los recursos del nuevo sitio deben coincidir con los nodos de almacenamiento de los sitios StorageGRID existentes.

Asegúrese de que la cantidad de nodos StorageGRID que planea ejecutar en cada host físico o virtual no exceda la cantidad de núcleos de CPU o la RAM física disponible. Si los hosts no están dedicados a ejecutar StorageGRID (no recomendado), asegúrese de considerar los requisitos de recursos de las otras aplicaciones.



Supervise periódicamente el uso de su CPU y memoria para garantizar que estos recursos sigan adaptándose a su carga de trabajo. Por ejemplo, duplicar la asignación de RAM y CPU para los nodos de almacenamiento virtuales proporcionaría recursos similares a los proporcionados para los nodos del dispositivo StorageGRID . Además, si la cantidad de metadatos por nodo supera los 500 GB, considere aumentar la RAM por nodo a 48 GB o más. Para obtener información sobre cómo administrar el almacenamiento de metadatos de objetos, aumentar la configuración del espacio reservado de metadatos y monitorear el uso de CPU y memoria, consulte las instrucciones para [administrando](#) , [escucha](#) , y [actualización](#) StorageGRID.

Si el hiperprocesamiento está habilitado en los hosts físicos subyacentes, puede proporcionar 8 núcleos virtuales (4 núcleos físicos) por nodo. Si el hiperprocesamiento no está habilitado en los hosts físicos subyacentes, debe proporcionar 8 núcleos físicos por nodo.

Si utiliza máquinas virtuales como hosts y tiene control sobre el tamaño y la cantidad de máquinas virtuales, debe usar una sola máquina virtual para cada nodo StorageGRID y dimensionar la máquina virtual en

consecuencia.

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

Consulte también ["Requisitos de almacenamiento y rendimiento"](#) .

Requisitos de almacenamiento y rendimiento

Debe comprender los requisitos de almacenamiento para los nodos StorageGRID , de modo que pueda proporcionar suficiente espacio para soportar la configuración inicial y la futura expansión del almacenamiento.

Los nodos StorageGRID requieren tres categorías lógicas de almacenamiento:

- **Grupo de contenedores:** almacenamiento de nivel de rendimiento (SAS o SSD de 10 000 GB) para los contenedores de nodos, que se asignará al controlador de almacenamiento del motor de contenedores cuando instale y configure el motor de contenedores en los hosts que soportarán sus nodos StorageGRID .
- **Datos del sistema** – Almacenamiento de nivel de rendimiento (SAS o SSD de 10 000 rpm) para almacenamiento persistente por nodo de datos del sistema y registros de transacciones, que los servicios de host de StorageGRID consumirán y asignarán a nodos individuales.
- **Datos de objetos:** almacenamiento de nivel de rendimiento (SAS o SSD de 10 000 rpm) y almacenamiento masivo de nivel de capacidad (NL-SAS/SATA) para el almacenamiento persistente de datos de objetos y metadatos de objetos.

Debe utilizar dispositivos de bloque respaldados por RAID para todas las categorías de almacenamiento. No se admiten discos no redundantes, SSD ni JBOD. Puede utilizar almacenamiento RAID local o compartido para cualquiera de las categorías de almacenamiento; sin embargo, si desea utilizar la capacidad de migración de nodos en StorageGRID, debe almacenar los datos del sistema y los datos de los objetos en el almacenamiento compartido. Para obtener más información, consulte ["Requisitos de migración del contenedor de nodos"](#) .

Requisitos de rendimiento

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

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

Requisitos para los hosts que utilizan almacenamiento NetApp ONTAP

Si el nodo StorageGRID usa almacenamiento asignado desde un sistema NetApp ONTAP , confirme que el volumen no tenga habilitada una política de niveles de FabricPool . Deshabilitar la organización en niveles de FabricPool para los volúmenes utilizados con nodos StorageGRID simplifica la resolución de problemas y las

operaciones de almacenamiento.



Nunca use FabricPool para agrupar datos relacionados con StorageGRID en StorageGRID mismo. La organización de los datos de StorageGRID en niveles en StorageGRID aumenta la resolución de problemas y la complejidad operativa.

Número de hosts necesarios

Cada sitio de StorageGRID requiere un mínimo de tres nodos de almacenamiento.



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

Se pueden implementar otros tipos de nodos, como nodos de administración o nodos de puerta de enlace, en los mismos hosts o en sus propios hosts dedicados según sea necesario.

Número de volúmenes de almacenamiento para cada host

La siguiente tabla muestra la cantidad de volúmenes de almacenamiento (LUN) necesarios para cada host y el tamaño mínimo requerido para cada LUN, en función de los nodos que se implementarán en ese host.

El tamaño máximo de LUN probado es 39 TB.



Estos números son para cada host, no para toda la red.

Propósito del LUN	Categoría de almacenamiento	Número de LUN	Tamaño mínimo/LUN
Piscina de almacenamiento de motores de contenedores	Pool de contenedores	1	Número total de nodos × 100 GB
`/var/local`volumen	Datos del sistema	1 para cada nodo en este host	90 GB
Nodo de almacenamiento	Datos de objeto	3 para cada nodo de almacenamiento en este host Nota: Un nodo de almacenamiento basado en software puede tener de 1 a 48 volúmenes de almacenamiento; se recomiendan al menos 3 volúmenes de almacenamiento.	12 TB (4 TB/LUN) Ver Requisitos de almacenamiento para nodos de almacenamiento Para más información.

Propósito del LUN	Categoría de almacenamiento	Número de LUN	Tamaño mínimo/LUN
Nodo de almacenamiento (solo metadatos)	Metadatos de objetos	1	4 TB Ver Requisitos de almacenamiento para nodos de almacenamiento Para más información. Nota: Solo se requiere una rangedb para los nodos de almacenamiento de solo metadatos.
Registros de auditoría del nodo de administración	Datos del sistema	1 para cada nodo de administración en este host	200 GB
Tablas del nodo de administración	Datos del sistema	1 para cada nodo de administración en este host	200 GB



Según el nivel de auditoría configurado, el tamaño de las entradas del usuario, como el nombre de la clave del objeto S3, y la cantidad de datos del registro de auditoría que necesita conservar, es posible que deba aumentar el tamaño del LUN del registro de auditoría en cada nodo de administración. Generalmente, una cuadrícula genera aproximadamente 1 KB de datos de auditoría por operación S3, lo que significaría que un LUN de 200 GB admitiría 70 millones de operaciones por día u 800 operaciones por segundo durante dos o tres días.

Espacio mínimo de almacenamiento para un host

La siguiente tabla muestra el espacio de almacenamiento mínimo requerido 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, en función de qué nodos se implementarán en ese host.



Las instantáneas de disco no se pueden usar para restaurar nodos de la red. En su lugar, consulte la "[recuperación del nodo de la red](#)" procedimientos para cada tipo de nodo.

Tipo de nodo	Pool de contenedores	Datos del sistema	Datos de objeto
Nodo de almacenamiento	100 GB	90 GB	4.000 GB
Nodo de administración	100 GB	490 GB (3 LUN)	<i>no aplicable</i>
Nodo de puerta de enlace	100 GB	90 GB	<i>no aplicable</i>

Ejemplo: Cálculo de los requisitos de almacenamiento para un host

Supongamos 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 datos del sistema y registros de transacciones, y 12 TB de almacenamiento de nivel de capacidad para datos de objetos.

Tipo de nodo	Propósito del LUN	Número de LUN	Tamaño de LUN
Nodo de almacenamiento	Piscina de almacenamiento de motores de contenedores	1	300 GB (100 GB/nodo)
Nodo de almacenamiento	`/var/local` volumen	1	90 GB
Nodo de almacenamiento	Datos de objeto	3	12 TB (4 TB/LUN)
Nodo de administración	`/var/local` volumen	1	90 GB
Nodo de administración	Registros de auditoría del nodo de administración	1	200 GB
Nodo de administración	Tablas del nodo de administración	1	200 GB
Nodo de puerta de enlace	`/var/local` volumen	1	90 GB
Total		9	Grupo de contenedores: 300 GB Datos del sistema: 670 GB Datos del objeto: 12.000 GB

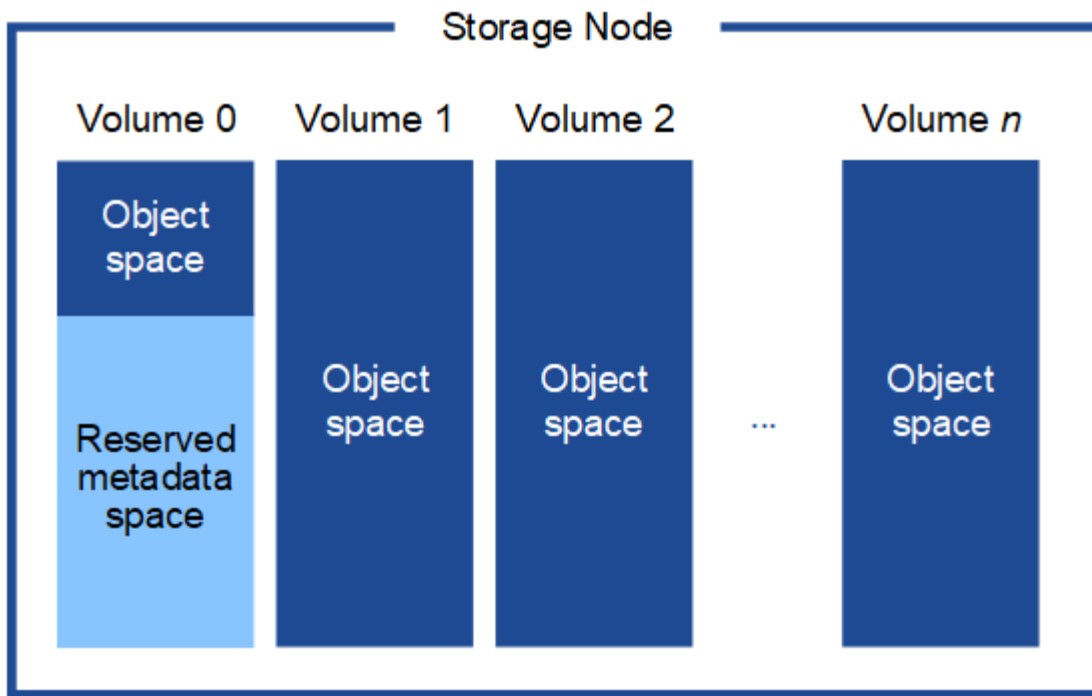
Requisitos de almacenamiento para nodos de almacenamiento

Un nodo de almacenamiento basado en software puede tener de 1 a 48 volúmenes de almacenamiento; se recomiendan 3 o más volúmenes de almacenamiento. Cada volumen de almacenamiento debe ser de 4 TB o más.



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

Como se muestra en la figura, StorageGRID reserva espacio para los metadatos de objetos 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 datos de objetos.



Para proporcionar redundancia y proteger los metadatos de los objetos contra pérdidas, StorageGRID almacena tres copias de los metadatos de todos los objetos del sistema en cada sitio. Las tres copias de metadatos de objetos se distribuyen uniformemente entre todos los nodos de almacenamiento en cada sitio.

Al instalar una cuadrícula con nodos de almacenamiento solo de metadatos, la cuadrícula también debe contener una cantidad mínima de nodos para el almacenamiento de objetos. Ver ["Tipos de nodos de almacenamiento"](#) para obtener más información sobre los nodos de almacenamiento de solo metadatos.

- Para una cuadrícula de un solo sitio, se configuran al menos dos nodos de almacenamiento para objetos y metadatos.
- Para una cuadrícula de varios sitios, se configura al menos un nodo de almacenamiento por sitio para objetos y metadatos.

Cuando asigna espacio al volumen 0 de un nuevo nodo de almacenamiento, debe asegurarse de que haya espacio adecuado para la parte de metadatos de objetos de ese nodo.

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



Si usa solo un volumen de almacenamiento para un nodo de almacenamiento y asigna 4 TB o menos al volumen, el nodo de almacenamiento podría ingresar al estado de solo lectura de almacenamiento al iniciarse y almacenar solo metadatos de objetos.



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

- Los recursos de nodo de solo metadatos basados en software deben coincidir con los recursos de los nodos de almacenamiento existentes. Por ejemplo:
 - Si el sitio StorageGRID existente utiliza dispositivos SG6000 o SG6100, los nodos de solo metadatos basados en software deben cumplir los siguientes requisitos mínimos:
 - 128 GB de RAM

- CPU de 8 núcleos
- SSD de 8 TB o almacenamiento equivalente para la base de datos Cassandra (rangedb/0)
- Si el sitio StorageGRID existente usa nodos de almacenamiento virtuales con 24 GB de RAM, CPU de 8 núcleos y 3 TB o 4 TB de almacenamiento de metadatos, los nodos solo de metadatos basados en software deben usar recursos similares (24 GB de RAM, CPU de 8 núcleos y 4 TB de almacenamiento de metadatos (rangedb/0)).

Al agregar un nuevo sitio StorageGRID , la capacidad total de metadatos del nuevo sitio debe coincidir, como mínimo, con los sitios StorageGRID existentes y los recursos del nuevo sitio deben coincidir con los nodos de almacenamiento de los sitios StorageGRID existentes.

- Si está instalando un nuevo sistema (StorageGRID 11.6 o superior) y cada nodo de almacenamiento tiene 128 GB o más de RAM, asigne 8 TB o más al volumen 0. El uso de un valor mayor para el volumen 0 puede aumentar el espacio permitido para los metadatos en cada nodo de almacenamiento.
- Al configurar diferentes nodos de almacenamiento para un sitio, utilice la misma configuración para el volumen 0 si es posible. Si un sitio contiene nodos de almacenamiento de diferentes tamaños, el nodo de almacenamiento con el volumen más pequeño (0) determinará la capacidad de metadatos de ese sitio.

Para más detalles, visite ["Administrar el almacenamiento de metadatos de objetos"](#) .

Requisitos de migración del contenedor de nodos

La función de migración de nodos le 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 del host físico sin interrumpir las operaciones de la red. Mueva todos los nodos de StorageGRID , uno a la vez, a otro host antes de desconectar el host físico. La migración de nodos solo requiere un breve tiempo de inactividad para cada nodo y no debería afectar el funcionamiento ni la disponibilidad de los servicios de la red.

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

- Nombres de interfaz de red consistentes en todos los hosts de un único centro de datos físico
- Almacenamiento compartido para metadatos de StorageGRID y volúmenes de repositorio de objetos al que pueden acceder todos los hosts en un único centro de datos físico. Por ejemplo, puede utilizar matrices de almacenamiento NetApp E-Series.

Si está utilizando hosts virtuales y la capa de hipervisor subyacente admite la migración de VM, es posible que desee utilizar esta capacidad en lugar de la función de migración de nodos en StorageGRID. En este caso, puedes ignorar estos requisitos adicionales.

Antes de realizar la migración o el mantenimiento del hipervisor, apague los nodos correctamente. Vea las instrucciones para ["apagar un nodo de la red"](#) .

VMware Live Migration no compatible

Al realizar una instalación completa en máquinas virtuales VMware, OpenStack Live Migration y VMware Live vMotion provocan saltos en el reloj de la máquina virtual y no son compatibles con nodos de red de ningún tipo. Aunque es poco frecuente, los horarios de reloj incorrectos pueden provocar la pérdida de datos o actualizaciones de configuración.

Se admite la migración en frío. En la migración en frío, se apagan los nodos StorageGRID antes de migrarlos

entre hosts. Vea las instrucciones para ["apagar un nodo de la red"](#) .

Nombres de interfaz de red consistentes

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

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

eth0 **→** **bond0.1001**

eth1 **→** **bond0.1002**

eth2 **→** **bond0.1003**

El lado izquierdo de las flechas corresponde a las interfaces tradicionales vistas desde dentro de 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 enlace 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 traslado, asumiendo que las interfaces con el mismo nombre proporcionarán la misma conectividad en Host2 que en Host1. Si Host2 no tiene interfaces con los mismos nombres, no se permitirá el movimiento.

Hay muchas formas de lograr una denominación de interfaz de red consistente en varios hosts; consulte ["Configuración de la red del host"](#) para algunos ejemplos.

Almacenamiento compartido

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

1. Durante la operación de "exportación de nodo", se extrae una pequeña cantidad de datos de estado persistentes del contenedor de nodo que se ejecuta en HostA y se almacena en caché en el volumen de datos del sistema de ese nodo. Luego, se desinstancia el contenedor de nodo en HostA.
2. Durante la operación de "importación de nodo", se crea una instancia del contenedor de nodo en HostB que utiliza la misma interfaz de red y asignaciones de almacenamiento en bloque que estaban vigentes en HostA. Luego, los datos de estado persistente almacenados en caché se insertan en la nueva instancia.

Dado este modo de operación, todos los datos del sistema del nodo y los volúmenes de almacenamiento de objetos deben ser accesibles tanto desde HostA como desde HostB para que se permita la migración y funcione. Además, deben haber sido mapeados al nodo usando nombres que garanticen que hacen referencia a los mismos LUN en HostA y HostB.

El siguiente ejemplo muestra una solución para el mapeo de dispositivos de bloque para un nodo de almacenamiento StorageGRID , donde se utiliza la multiruta DM en los hosts y se ha utilizado el campo de alias en `/etc/multipath.conf` para proporcionar nombres de dispositivos de bloque consistentes y

amigables 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`

Preparar los hosts (Red Hat)

Cómo cambian las configuraciones de todo el host durante la instalación

En sistemas físicos, StorageGRID realiza algunos cambios en todo el host `sysctl` ajustes.

Se realizan los siguientes cambios:

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

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

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

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
```

```

# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

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

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

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

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

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

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

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

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

```



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

Instalar Linux

Debe instalar StorageGRID en todos los hosts de red de Red Hat Enterprise Linux. Para obtener una lista de las versiones compatibles, utilice la herramienta Matriz de interoperabilidad de NetApp .

Antes de empezar

Asegúrese de que su sistema operativo cumpla con los requisitos mínimos de versión de kernel de StorageGRID, como se detalla a continuación. Utilice el comando `uname -r` para obtener la versión del kernel de su sistema operativo o consulte con el proveedor de su sistema operativo.

Versión de Red Hat Enterprise Linux	Versión mínima del kernel	Nombre del paquete del kernel
8.8 (obsoleto)	4.18.0-477.10.1.el8_8.x86_64	kernel-4.18.0-477.10.1.el8_8.x86_64
8,10	4.18.0-553.el8_10.x86_64	núcleo-4.18.0-553.el8_10.x86_64
9.0 (obsoleto)	5.14.0-70.22.1.el9_0.x86_64	kernel-5.14.0-70.22.1.el9_0.x86_64
9.2 (obsoleto)	5.14.0-284.11.1.el9_2.x86_64	kernel-5.14.0-284.11.1.el9_2.x86_64
9,4	5.14.0-427.18.1.el9_4.x86_64	kernel-5.14.0-427.18.1.el9_4.x86_64
9,6	5.14.0-570.18.1.el9_6.x86_64	kernel-5.14.0-570.18.1.el9_6.x86_64

Pasos

1. Instale Linux en todos los hosts de la red física o virtual de acuerdo con las instrucciones del distribuidor o su procedimiento estándar.



Si está utilizando el instalador estándar de Linux, seleccione la configuración de software "nodo de cómputo", si está disponible, o el entorno base "instalación mínima". No instale ningún entorno de escritorio gráfico.

2. Asegúrese de que todos los hosts tengan acceso a los 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 habilitado:

- a. Ejecute el siguiente comando: `$ sudo swapoff --all`
- b. Eliminar todas las entradas de intercambio de `/etc/fstab` para conservar la configuración.



No deshabilitar el intercambio por completo puede reducir gravemente el rendimiento.

Configurar la red del host (Red Hat Enterprise Linux)

Después de completar la instalación de Linux en sus hosts, es posible que necesite realizar alguna configuración adicional para preparar un conjunto de interfaces de red en cada host que sean adecuadas para mapearlas en los nodos StorageGRID que implementará más adelante.

Antes de empezar

- Usted ha revisado el ["Pautas de red de StorageGRID"](#) .
- Has revisado la información sobre ["Requisitos de migración del contenedor de nodos"](#) .
- Si está utilizando hosts virtuales, ha leído el [Consideraciones y recomendaciones para la clonación de direcciones MAC](#) antes de configurar la red del host.



Si está utilizando máquinas 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 implementados en ciertas distribuciones de Linux.

Acerca de esta tarea

Los nodos de la red deben poder acceder a la red de la red y, opcionalmente, a las redes de administración y de cliente. Puede proporcionar este acceso mediante la creación de asignaciones que asocian la interfaz física del host con las interfaces virtuales de cada nodo de la red. Al crear interfaces de host, utilice nombres descriptivos para facilitar la implementación en todos los hosts y permitir la migración.

La misma interfaz se puede compartir entre el host y uno o más nodos. Por ejemplo, puede utilizar la misma interfaz para el acceso al host y el acceso a la red de administración del nodo, para facilitar el mantenimiento del host y del nodo. Aunque se puede compartir la misma interfaz entre el host y los nodos individuales, todos deben tener direcciones IP diferentes. Las direcciones IP no se pueden compartir entre 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 en el host; puede utilizar una interfaz de red de host diferente para cada nodo; o puede hacer algo intermedio. Sin embargo, normalmente no proporcionaría la misma interfaz de red de host como interfaz de red de administración y de cuadrícula para un solo nodo, o como interfaz de red de cuadrícula para un nodo y como interfaz de red de cliente para otro.

Puedes completar esta tarea de muchas maneras. Por ejemplo, si sus hosts son máquinas virtuales y está implementando uno o dos nodos StorageGRID para cada host, puede crear la cantidad correcta de interfaces de red en el hipervisor y usar una asignación de 1 a 1. Si está implementando varios nodos en hosts físicos para uso de producción, puede aprovechar el soporte de la pila de red Linux para VLAN y LACP para tolerancia a fallas y uso compartido de ancho de banda. Las siguientes secciones proporcionan enfoques detallados para ambos ejemplos. No es necesario utilizar ninguno de estos ejemplos; puede utilizar cualquier enfoque que se ajuste a sus necesidades.



No utilice dispositivos de enlace o puente directamente como interfaz de red del contenedor. Al hacerlo se podría evitar el inicio del nodo causado por un problema del 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 enlace, como una VLAN o un par Ethernet virtual (veth). Especifique este dispositivo como la interfaz de red en el archivo de configuración del nodo.

Información relacionada

["Creación de archivos de configuración de nodos"](#)

Consideraciones y recomendaciones para la clonación de direcciones MAC

[[clonación de direcciones MAC_rhel]]

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

Habilitar la clonación de MAC

En ciertos entornos, la seguridad se puede mejorar mediante la clonación de direcciones MAC porque permite utilizar una NIC virtual dedicada para la red de administración, la red de cuadrícula y la red de cliente. Hacer que el contenedor utilice la dirección MAC de la NIC dedicada en el host le permite evitar el uso de configuraciones de red en modo promiscuo.



La clonación de direcciones MAC está diseñada para usarse con instalaciones de servidores virtuales y es posible que no funcione correctamente con todas las configuraciones de dispositivos físicos.



Si un nodo no puede iniciarse debido a que una interfaz de clonación MAC está ocupada, es posible que deba configurar el enlace como "inactivo" antes de iniciar el nodo. Además, es posible que el entorno virtual impida la clonación de MAC en una interfaz de red mientras el enlace está activo. Si un nodo no logra configurar la dirección MAC y no se inicia debido a que una interfaz está ocupada, configurar el enlace como "inactivo" antes de iniciar el nodo podría solucionar el problema.

La clonación de direcciones MAC está deshabilitada de forma predeterminada y debe configurarse mediante claves de configuración del nodo. Debes habilitarlo cuando instales 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

Establecer la clave en "verdadero" hace que el contenedor utilice 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 configurado una utilizando el `_NETWORK_MAC` clave de configuración del nodo, se utiliza esa dirección en su lugar. El host y el contenedor siempre tendrán direcciones MAC diferentes.



Habilitar la clonación de MAC en un host virtual sin habilitar también el modo promiscuo en el hipervisor podría provocar que la red del host Linux que utiliza la interfaz del host deje de funcionar.

Casos de uso de clonación de MAC

Hay dos casos de uso a considerar con la clonación de MAC:

- Clonación de MAC no habilitada: cuando el `_CLONE_MAC` Si la clave en el archivo de configuración del nodo no está configurada o está configurada como "falsa", el host usará la MAC de la NIC del host y el contenedor tendrá una MAC generada por StorageGRID a menos que se especifique una MAC en el archivo. `_NETWORK_MAC` llave. Si se establece una dirección en el `_NETWORK_MAC` clave, el contenedor tendrá la dirección especificada en la `_NETWORK_MAC` llave. Esta configuración de claves requiere el uso del modo promiscuo.
- Clonación de MAC habilitada: cuando el `_CLONE_MAC` Si la clave en el archivo de configuración del nodo está establecida en "verdadero", el contenedor utiliza la MAC de la NIC del host y el host utiliza una MAC generada por StorageGRID a menos que se especifique una MAC en el archivo. `_NETWORK_MAC` llave. Si se establece una dirección en el `_NETWORK_MAC` clave, el host utiliza la dirección especificada en lugar de una generada. En esta configuración de claves, no se debe utilizar el modo promiscuo.



Si no desea utilizar la clonación de direcciones MAC y prefiere permitir que todas las interfaces reciban y transmitan datos para direcciones MAC distintas de las asignadas por el hipervisor, asegúrese de que las propiedades de seguridad en los niveles de conmutador virtual y grupo de puertos estén configuradas en **Aceptar** para Modo promiscuo, Cambios de dirección MAC y Transmisiones falsificadas. Los valores establecidos en el conmutador virtual pueden ser anulados por los valores a nivel del grupo de puertos, así que asegúrese de que las configuraciones sean las mismas en ambos lugares.

Para habilitar la clonación de MAC, consulte la ["Instrucciones para crear archivos de configuración de nodos"](#) .

Ejemplo de clonación de MAC

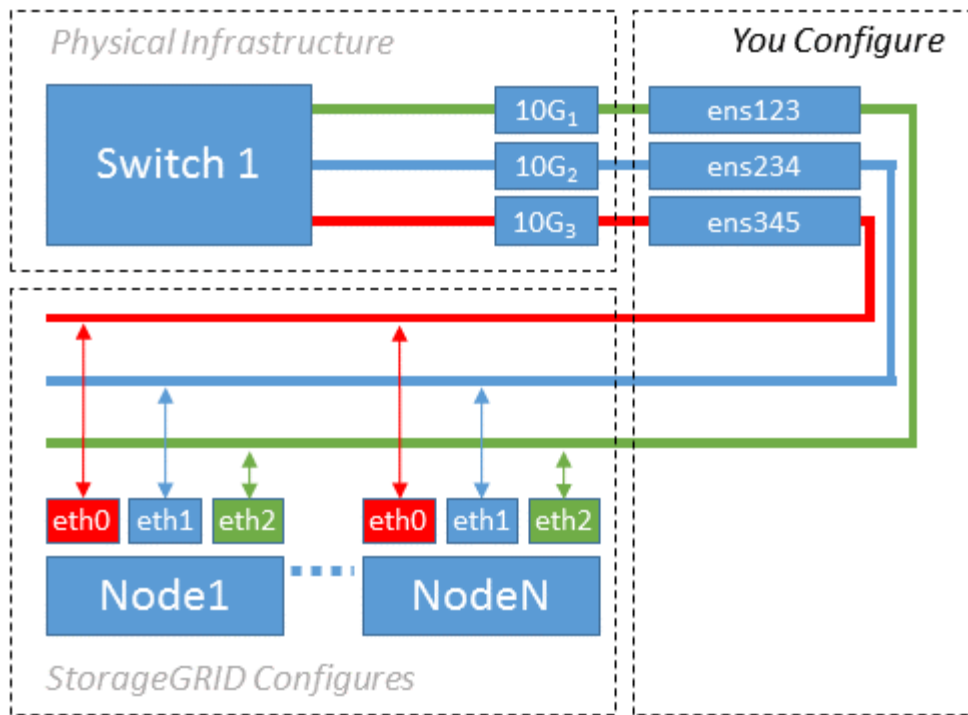
Ejemplo de clonación de MAC habilitada con un host que tiene la dirección MAC 11:22:33:44:55:66 para la interfaz ens256 y las siguientes claves en el archivo de configuración del nodo:

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

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

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

El ejemplo 1 describe un mapeo de interfaz física simple que requiere poca o ninguna configuración del lado del host.



El sistema operativo Linux crea el `ensXYZ` interfaces automáticamente durante la instalación o el arranque, o cuando las interfaces se agregan en caliente. No se requiere configuración más allá de asegurarse de que las interfaces estén configuradas para activarse automáticamente después del arranque. Tienes que determinar cuál `ensXYZ` corresponde a qué red StorageGRID (Grid, Admin o Client) para que pueda proporcionar las asignaciones correctas más adelante en el proceso de configuración.

Tenga en cuenta que la figura muestra varios nodos StorageGRID ; sin embargo, normalmente utilizaría 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 10G1 a 10G3 para el modo de acceso y colocarlos en las VLAN apropiadas.

Ejemplo 2: VLAN que transportan enlaces LACP

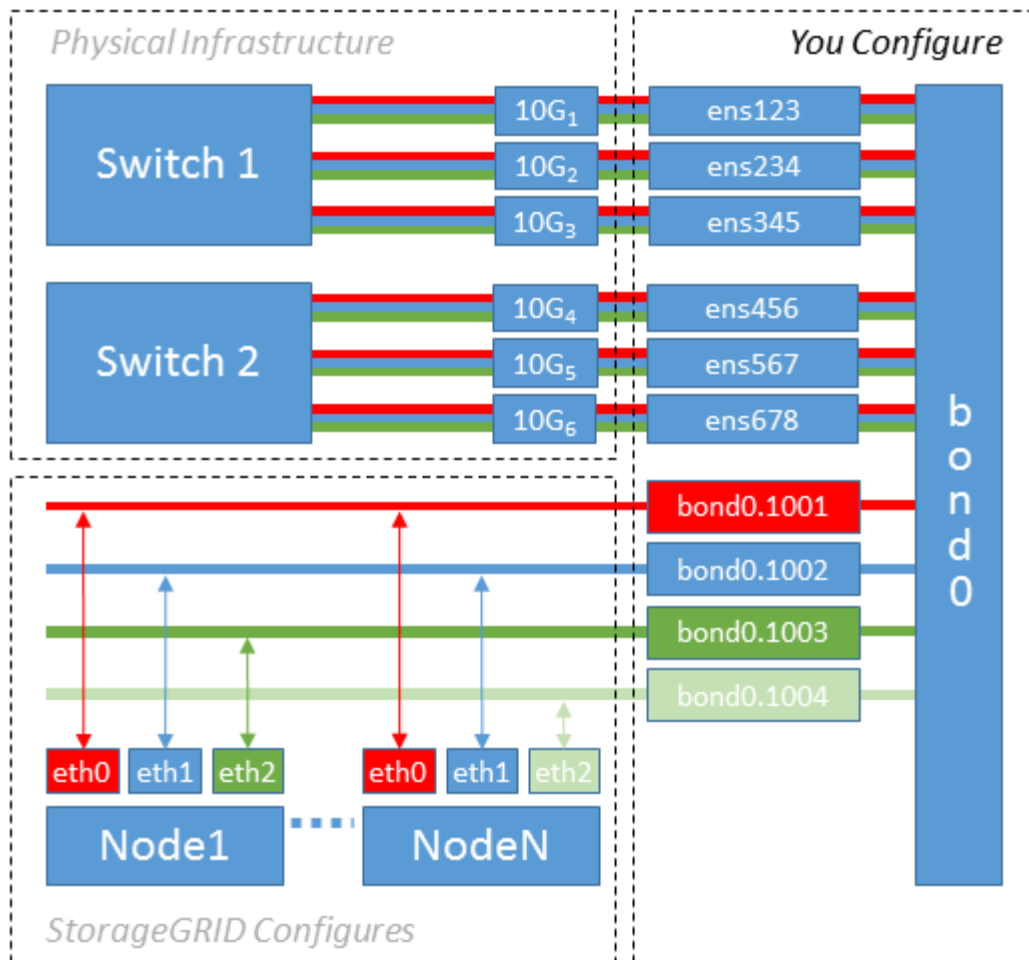
Acerca de esta tarea

El ejemplo 2 supone que está familiarizado con la vinculación de interfaces de red y con la creación de interfaces VLAN en la distribución de Linux que está utilizando.

El ejemplo 2 describe un esquema genérico, flexible y basado en VLAN que facilita compartir todo el ancho de banda de red disponible entre todos los nodos de un solo host. Este ejemplo es particularmente aplicable a hosts de hardware real.

Para entender este ejemplo, supongamos que tiene tres subredes separadas para las redes de red, administración y cliente en cada centro de datos. Las subredes están en VLAN separadas (1001, 1002 y 1003) y se presentan al host en un puerto troncal vinculado a LACP (`bond0`). Configuraría tres interfaces VLAN en el enlace: `bond0.1001`, `bond0.1002` y `bond0.1003`.

Si necesita VLAN y subredes independientes para redes de nodos en el mismo host, puede agregar interfaces VLAN en el enlace y asignarlas al host (que se muestra como `bond0.1004` en la ilustración).



Pasos

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

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

2. Cree interfaces VLAN que utilicen este enlace como su "dispositivo físico" asociado, utilizando la convención de nombres de interfaz VLAN estándar `physdev-name.VLAN ID`.

Tenga en cuenta que los pasos 1 y 2 requieren una configuración adecuada en los conmutadores de borde que terminan los otros extremos de los enlaces de red. Los puertos del conmutador de borde también deben agregarse en un canal de puerto LACP, configurarse como un enlace troncal y permitir que pasen 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/sysconfig/network-scripts"](#)

Configurar el almacenamiento del host

Debe asignar volúmenes de almacenamiento en bloque a cada host.

Antes de empezar

Ha revisado los siguientes temas, que proporcionan la información que necesita para realizar esta tarea:

- ["Requisitos de almacenamiento y rendimiento"](#)
- ["Requisitos de migración del contenedor de nodos"](#)

Acerca de esta tarea

Al asignar volúmenes de almacenamiento en bloque (LUN) a los hosts, utilice las tablas en "Requisitos de almacenamiento" para determinar lo siguiente:

- Número de volúmenes necesarios para cada host (según la cantidad y los tipos de nodos que se implementarán en ese host)
- Categoría de almacenamiento para cada volumen (es decir, datos del sistema o datos de objeto)
- 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 necesita particionar, formatear ni montar ninguno de estos volúmenes; solo necesita asegurarse de que sean visibles para los hosts.



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

Evite utilizar archivos de dispositivos especiales "sin procesar" (`/dev/sdb`, por ejemplo) mientras compone su lista de nombres de volúmenes. Estos archivos pueden cambiar durante los reinicios del host, lo que afectará el funcionamiento correcto del sistema. Si está utilizando LUN iSCSI y rutas múltiples de Device Mapper, considere usar alias de rutas múltiples en el `/dev/mapper` directorio, especialmente si su topología SAN incluye rutas de red redundantes al almacenamiento compartido. Alternativamente, puede utilizar los enlaces creados por el sistema en `/dev/disk/by-path/` para los nombres de sus 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 variarán para cada instalación.

Asigne nombres descriptivos a cada uno de estos volúmenes de almacenamiento en bloque para simplificar la instalación inicial de StorageGRID y los procedimientos de mantenimiento futuros. Si está utilizando el controlador de múltiples rutas del asignador de dispositivos para el acceso redundante a volúmenes de almacenamiento compartido, puede utilizar el `alias` campo en tu `/etc/multipath.conf` archivo.

Por ejemplo:


```

multipaths {
    multipath {
        wwid 3600a09800059d6df00005df2573c2c30
        alias docker-storage-volume-hostA
    }
    multipath {
        wwid 3600a09800059d6df00005df3573c2c30
        alias sgws-adml-var-local
    }
    multipath {
        wwid 3600a09800059d6df00005df4573c2c30
        alias sgws-adml-audit-logs
    }
    multipath {
        wwid 3600a09800059d6df00005df5573c2c30
        alias sgws-adml-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
    }
    ...
}

```

El uso del campo de alias de esta manera hace que los alias aparezcan como dispositivos de bloque en el `/dev/mapper` directorio en el host, lo que le permite especificar un nombre amigable y fácilmente validado siempre que una operación de configuración o mantenimiento requiera especificar un volumen de almacenamiento en bloque.



Si está configurando un almacenamiento compartido para admitir la migración de nodos StorageGRID y utiliza Device Mapper Multipathing, puede crear e instalar un dispositivo común `/etc/multipath.conf` en todos los hosts ubicados conjuntamente. Solo asegúrese de utilizar un volumen de almacenamiento de motor de contenedor diferente en cada host. El uso de alias e incluir el nombre de host de destino en el alias para cada LUN de volumen de almacenamiento del motor de contenedor hará que esto sea fácil de recordar y es lo recomendado.



La compatibilidad con Docker como motor de contenedores para implementaciones de solo software está obsoleta. Docker será reemplazado por otro motor de contenedores en una versión futura.

Información relacionada

["Configurar el volumen de almacenamiento del motor de contenedores"](#)

Configurar el volumen de almacenamiento del motor de contenedores

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



La compatibilidad con Docker como motor de contenedores para implementaciones de solo software está obsoleta. Docker será reemplazado por otro motor de contenedores en una versión futura.

Acerca de esta tarea

Puede omitir estos pasos si planea usar almacenamiento local para el volumen de almacenamiento de Docker o Podman y tiene suficiente espacio disponible en la partición del 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. Montar 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. Agregue una entrada para `container-storage-volume-device` a `/etc/fstab`.

Este paso garantiza que el volumen de almacenamiento se volverá a montar automáticamente después de que el host se reinicie.

Instalar Docker

El sistema StorageGRID se ejecuta en Red Hat Enterprise Linux como una colección de contenedores. Si ha elegido utilizar el motor de contenedores Docker, siga estos pasos para instalar Docker. De lo contrario, [instalar Podman](#).

Pasos

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



Si Docker no está incluido en tu distribución de Linux, puedes descargarlo del sitio web de Docker.

2. Asegúrese de que Docker se haya habilitado e iniciado ejecutando los siguientes dos comandos:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Confirme que ha instalado la versión esperada de Docker ingresando lo siguiente:

```
sudo docker version
```

Las versiones de Cliente y Servidor deben ser 1.11.0 o posteriores.

Instalar Podman

El sistema StorageGRID se ejecuta en Red Hat Enterprise Linux como una colección de contenedores. Si ha elegido utilizar el motor de contenedores Podman, siga estos pasos para instalar Podman. De lo contrario, [instalar 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 debes instalar el paquete Podman-Docker cuando instales Podman.

2. Confirme que ha instalado la versión esperada de Podman y Podman-Docker ingresando lo siguiente:

```
sudo docker version
```



El paquete Podman-Docker le permite utilizar comandos Docker.

Las versiones de Cliente y Servidor deben ser 3.2.3 o posteriores.

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

Instalar servicios de host de StorageGRID

Utilice el paquete RPM de StorageGRID para instalar los servicios de host de StorageGRID .

Acerca de esta tarea

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

Pasos

1. Copie los paquetes RPM de StorageGRID en cada uno de sus hosts o póngalos a disposición en el almacenamiento compartido.

Por ejemplo, colóquelos en el `/tmp` directorio, por lo que puede utilizar el comando de ejemplo en el siguiente paso.

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

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

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



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



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

Automatizar la instalación de StorageGRID en Red Hat Enterprise Linux

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

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

- Ya utiliza un marco de orquestación estándar, como Ansible, Puppet o Chef, para implementar y configurar hosts físicos o virtuales.
- Desea implementar varias instancias de StorageGRID .
- Está implementando una instancia de StorageGRID grande y compleja.

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

- ["Crear los archivos de configuración"](#) interactivamente durante una instalación manual.
- Prepare los archivos de configuración con anticipación (o mediante programación) para permitir la instalación automatizada utilizando marcos de orquestación estándar, como se describe en este artículo.

StorageGRID proporciona scripts de Python opcionales para automatizar la configuración de los dispositivos StorageGRID y todo el sistema StorageGRID (la "red"). Puede utilizar estos scripts directamente o puede inspeccionarlos para aprender a usarlos. ["API REST de instalación de StorageGRID"](#) En herramientas de implementación y configuración de red que usted mismo desarrolla.

Automatice la instalación y configuración del servicio de host StorageGRID

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

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

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



El manual de ejemplo no incluye los pasos necesarios para crear dispositivos de red antes de iniciar el servicio de host StorageGRID . Agregue estos pasos antes de finalizar y usar el libro de jugadas.

Puede automatizar todos los pasos para preparar los hosts e implementar nodos de red virtuales.

Ejemplo de rol y manual de estrategias de Ansible

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

Las tareas de instalación en el `storagegrid` Ejemplo de rol: utilice el `ansible.builtin.dnf` Módulo para realizar la instalación desde los archivos RPM locales o un repositorio Yum remoto. Si el módulo no está disponible o no es compatible, es posible que deba editar las tareas de Ansible adecuadas en los siguientes archivos para usarlo `yum` o `ansible.builtin.yum` módulo:

- `roles/storagegrid/tasks/rhel_install_from_repo.yml`

- `roles/storagegrid/tasks/rhel_install_from_local.yml`

Automatizar la configuración de StorageGRID

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

Antes de empezar

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

Nombre del archivo	Descripción
<code>configurar-storagegrid.py</code>	Script de Python utilizado para automatizar la configuración
<code>configure-storagegrid.sample.json</code>	Archivo de configuración de ejemplo para usar con el script
<code>configurar-storagegrid.blank.json</code>	Archivo de configuración en blanco para usar con el script

- Has 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

Puedes utilizar el `configure-storagegrid.py` Script de Python y el `configure-storagegrid.json` archivo de configuración para automatizar la configuración de su sistema StorageGRID .



También puede configurar el sistema utilizando el Administrador de Grid o la API de instalación.

Pasos

1. Inicie sesión en la máquina Linux que está utilizando para ejecutar el script de Python.
2. Cambie al directorio donde extrajo el archivo de instalación.

Por ejemplo:

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

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

3. Ejecute el script de 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 donde se está ejecutando el proceso de instalación y configuración. Debe realizar una copia de seguridad del archivo del paquete de recuperación para poder recuperar el sistema StorageGRID si uno o más nodos de la red fallan. Por ejemplo, cópielo en una ubicación de red segura y respaldada y en una ubicación de almacenamiento en la nube segura.



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

Si especificó que se generen contraseñas aleatorias, abra el `Passwords.txt` archivo y busque las contraseñas necesarias para acceder a su 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.      #####
#####
```

Su sistema StorageGRID está instalado y configurado cuando se muestra un mensaje de confirmación.

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

Información relacionada

["Instalación API REST"](#)

Implementar nodos de red virtuales (Red Hat)

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

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

Ubicación de los archivos de configuración del nodo

Coloque 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 utilizando un editor de texto, como vim o nano, o puede crearlos en otro lugar y moverlos a cada host.

Nomenclatura de los archivos de configuración de nodos

Los nombres de los archivos de configuración son significativos. El formato es `node-name.conf`, donde `node-name` Es un nombre que le asignas 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 con 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 más guiones (-)
- No debe tener más de 32 caracteres, sin incluir el `.conf` extensión

Cualquier archivo en `/etc/storagegrid/nodes` que no sigan estas convenciones de nomenclatura no serán analizados por el servicio host.

Si tiene una topología de múltiples sitios planificada para su red, un esquema de nombres de nodos típico podría ser:

```
site-nodetype-nodenumbers.conf
```

Por ejemplo, podrías utilizar `dc1-adm1.conf` para el primer nodo de administración en el centro de datos 1, y `dc2-sn3.conf` para el tercer nodo de almacenamiento en el centro de datos 2. Sin embargo, puedes utilizar cualquier esquema que desees, siempre que todos los nombres de nodos sigan las reglas de nomenclatura.

Contenido de un archivo de configuración de nodo

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

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

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

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

Claves de red de administración

IP DE ADMINISTRADOR

Valor	Designación
Dirección IPv4 de la red de cuadrícula del nodo de administración principal de la cuadrícula a la que pertenece este nodo. Utilice el mismo valor que especificó para GRID_NETWORK_IP para el nodo de la red con NODE_TYPE = VM_Admin_Node y ADMIN_ROLE = Primary. Si omite este parámetro, el nodo intentará descubrir un nodo de administración principal mediante mDNS. "Cómo los nodos de la red descubren el nodo de administración principal" Nota: Este valor se ignora y puede estar prohibido en el nodo de administración principal.	Mejores prácticas

CONFIGURACIÓN DE RED DE ADMINISTRACIÓN

Valor	Designación
DHCP, ESTÁTICO o DESHABILITADO	Opcional

ADMINISTRACIÓN_RED_ESL

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

PUERTA DE ENLACE DE RED DE ADMINISTRACIÓN

Valor	Designación
Dirección IPv4 de la puerta de enlace de la red de administración local para este nodo. Debe estar en la subred definida por ADMIN_NETWORK_IP y ADMIN_NETWORK_MASK. Este valor se ignora para las redes configuradas por DHCP. Ejemplos: 1.1.1.1 10.224.4.81	Requerido si ADMIN_NETWORK_ESL se especifica Opcional en caso contrario.

IP DE RED DE ADMINISTRACIÓN

Valor	Designación
Dirección IPv4 de este nodo en la red de administración. 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	Obligatorio cuando ADMIN_NETWORK_CONFIG = STATIC. Opcional en caso contrario.

ADMIN_RED_MAC

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

MÁSCARA DE RED DE ADMINISTRACIÓN

Valor	Designación
Máscara de red IPv4 para este nodo, en la red de administración. Especifique esta clave cuando ADMIN_NETWORK_CONFIG = STATIC; no la especifique para otros valores. Ejemplos: 255.255.255.0 255.255.248.0	Obligatorio si se especifica ADMIN_NETWORK_IP y ADMIN_NETWORK_CONFIG = STATIC. Opcional en caso contrario.

MTU DE LA RED DE ADMINISTRACIÓN

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

OBJETIVO DE LA RED DE ADMINISTRACIÓN

Valor	Designación
Nombre del dispositivo host que utilizará para el acceso a la red de administración por parte del nodo StorageGRID . Sólo 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 la 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 incluso si este nodo inicialmente no tendrá una dirección IP de red de administración. Luego, puede agregar una dirección IP de red de administración más tarde, sin tener que reconfigurar el nodo en el host. Ejemplos: bond0.1002 ens256	Mejores prácticas

TIPO DE OBJETIVO DE RED DE ADMINISTRACIÓN

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

INTERFAZ DE TIPO DE DESTINO DE RED DE ADMINISTRACIÓN CLONAR MAC

Valor	Designación
Verdadero o falso Establezca la clave en "verdadero" para que el contenedor StorageGRID utilice 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 detalles sobre la clonación de MAC: • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Red Hat Enterprise Linux)" • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)"	Mejores prácticas

ROL DE ADMINISTRADOR

Valor	Designación
Primario o no primario Esta clave solo es necesaria cuando NODE_TYPE = VM_Admin_Node; no la especifique para otros tipos de nodos.	Obligatorio cuando NODE_TYPE = VM_Admin_Node Opcional en caso contrario.

Bloquear teclas del dispositivo

BLOQUEAR REGISTROS DE AUDITORÍA DEL DISPOSITIVO

Valor	Designación
Ruta y nombre del archivo especial del dispositivo de bloque que este nodo utilizará para el almacenamiento persistente de registros de auditoría. Ejemplos: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adml-audit-logs</pre>	Obligatorio para nodos con NODE_TYPE = VM_Admin_Node. No lo especifique para otros tipos de nodos.

DISPOSITIVO DE BLOQUE RANGEDB_nnn

Valor	Designación
Ruta y nombre del archivo especial del dispositivo de bloque que este nodo utilizará para el almacenamiento de objetos persistentes. Esta clave solo es necesaria para los nodos con NODE_TYPE = VM_Storage_Node; no la especifique para otros tipos de nodos. Solo se requiere BLOCK_DEVICE_RANGEDB_000; el resto es opcional. El dispositivo de bloque especificado para BLOCK_DEVICE_RANGEDB_000 debe ser de al menos 4 TB; los demás pueden ser más pequeños. No dejes espacios vacíos. Si especifica BLOCK_DEVICE_RANGEDB_005, también debe especificar BLOCK_DEVICE_RANGEDB_004. Nota: Para compatibilidad con implementaciones existentes, se admiten claves de dos dígitos para los nodos actualizados. Ejemplos: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-sn1-rangedb-000</pre>	Requerido: BLOCK_DEVICE_RANGEDB_000 Opcional: 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

TABLAS DE DISPOSITIVOS DE BLOQUE

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

BLOQUE_DISPOSITIVO_VAR_LOCAL

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

Claves de red del cliente

CONFIGURACIÓN DE RED DEL CLIENTE

Valor	Designación
DHCP, ESTÁTICO o DESHABILITADO	Opcional

PUERTA DE ENLACE DE LA RED DEL CLIENTE

Valor	Designación

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

IP DE LA RED DEL CLIENTE

Valor	Designación
Dirección IPv4 de este nodo en la red del 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	Obligatorio cuando CLIENT_NETWORK_CONFIG = STATIC Opcional en caso contrario.

MAC DE LA RED DEL CLIENTE

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

MÁSCARA DE RED DEL CLIENTE

Valor	Designación
Máscara de red IPv4 para este nodo en la red del cliente. Especifique esta clave cuando CLIENT_NETWORK_CONFIG = STATIC; no la especifique para otros valores. Ejemplos: 255.255.255.0 255.255.248.0	Obligatorio si se especifica CLIENT_NETWORK_IP y CLIENT_NETWORK_CONFIG = STATIC Opcional en caso contrario.

MTU DE LA RED DEL CLIENTE

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

OBJETIVO DE LA RED DEL CLIENTE

Valor	Designación
Nombre del dispositivo host que utilizará para el acceso a la red del cliente por parte del nodo StorageGRID . Sólo 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 la 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 incluso si este nodo inicialmente no tendrá una dirección IP de red de cliente. Luego, puede agregar una dirección IP de red de cliente más tarde, sin tener que reconfigurar el nodo en el host. Ejemplos: <pre>bond0.1003</pre> <pre>ens423</pre>	Mejores prácticas

TIPO DE OBJETIVO DE LA RED DEL CLIENTE

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

CLIENTE_RED_TIPO_DESTINATO_INTERFAZ_CLONAR_MAC

Valor	Designación
Verdadero o falso Establezca la clave en "verdadero" para que el contenedor StorageGRID utilice la dirección MAC de la interfaz de destino del host en la red del 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 detalles sobre la clonación de MAC: • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Red Hat Enterprise Linux)" • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)"	Mejores prácticas

Claves de red de cuadrícula

CONFIGURACIÓN DE RED DE CUADRÍCULA

Valor	Designación
ESTÁTICO o DHCP El valor predeterminado es ESTÁTICO si no se especifica.	Mejores prácticas

PUERTA DE ENLACE DE RED DE CUADRÍCULA

Valor	Designación
Dirección IPv4 de la puerta de enlace de la red local para este nodo, que debe estar en la subred definida por GRID_NETWORK_IP y GRID_NETWORK_MASK. Este valor se ignora para las redes configuradas por DHCP. Si la red Grid es una subred única sin puerta de enlace, utilice la dirección de puerta de enlace estándar para la subred (XYZ1) o el valor GRID_NETWORK_IP de este nodo; cualquiera de los valores simplificará posibles expansiones futuras de la red Grid.	Requerido

IP DE RED DE CUADRÍCULA

Valor	Designación
Dirección IPv4 de este nodo en la red Grid. 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	Obligatorio cuando GRID_NETWORK_CONFIG = STATIC Opcional en caso contrario.

RED_DE_CUADRÍCULA_MAC

Valor	Designación
La dirección MAC de la interfaz de red Grid en el contenedor. Deben ser 6 pares de dígitos hexadecimales separados por dos puntos. Ejemplo: b2:9c:02:c2:27:30	Opcional Si se omite, se generará automáticamente una dirección MAC.

MÁSCARA DE RED DE CUADRÍCULA

Valor	Designación
Máscara de red IPv4 para este nodo en la red Grid. Especifique esta clave cuando GRID_NETWORK_CONFIG = STATIC; no la especifique para otros valores. Ejemplos: 255.255.255.0 255.255.248.0	Obligatorio cuando se especifica GRID_NETWORK_IP y GRID_NETWORK_CONFIG = STATIC. Opcional en caso contrario.

MTU DE LA RED DE CUADRÍCULA

Valor	Designación
La unidad de transmisión máxima (MTU) para este nodo en la red eléctrica. No especifique si GRID_NETWORK_CONFIG = DHCP. Si se especifica, el valor debe estar entre 1280 y 9216. Si se omite, se utiliza 1500. Si desea utilizar tramas jumbo, configure la MTU en un valor adecuado para tramas jumbo, como 9000. De lo contrario, mantenga el valor predeterminado. IMPORTANTE: El valor de MTU de la red debe coincidir con el valor configurado en el puerto del conmutador al que está conectado el nodo. De lo contrario, podrían ocurrir problemas de rendimiento de la red o pérdida de paquetes. IMPORTANTE: Para obtener el mejor rendimiento de la red, todos los nodos deben configurarse con valores de MTU similares en sus interfaces de red Grid. La alerta No coincide la MTU de la red de cuadrícula se activa si hay una diferencia significativa en las configuraciones de MTU para la red de cuadrícula en nodos individuales. Los valores de MTU no tienen que ser los mismos para todos los tipos de red. Ejemplos: 1500 8192	Opcional

OBJETIVO DE LA RED DE CUADRÍCULA

Valor	Designación
Nombre del dispositivo host que utilizará para el acceso a la red Grid mediante el nodo StorageGRID . Sólo 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 la 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	Requerido

TIPO DE OBJETIVO DE RED DE CUADRÍCULA

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

INTERFAZ DE TIPO DE OBJETIVO DE RED DE CUADRÍCULA CLONAR MAC

Valor	Designación
Verdadero o falso Establezca el valor de la clave en "verdadero" para que el contenedor StorageGRID utilice la dirección MAC de la interfaz de destino del host en la red Grid. 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 detalles sobre la clonación de MAC: • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Red Hat Enterprise Linux)" • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)"	Mejores prácticas

Clave de contraseña de instalación (temporal)

HASH DE CONTRASEÑA TEMPORAL PERSONALIZADO

Valor	Designación
Para el nodo de administración principal, configure una contraseña temporal predeterminada para la API de instalación de StorageGRID durante la instalación. Nota: Establezca una contraseña de instalación solo en el nodo de administración principal. Si intenta establecer una contraseña en otro tipo de nodo, la validación del archivo de configuración del nodo fallará. Establecer este valor no tiene ningún efecto una vez finalizada la instalación. Si se omite esta clave, de forma predeterminada no se establece ninguna contraseña temporal. Alternativamente, puede establecer una contraseña temporal utilizando la API de instalación de StorageGRID . Debe ser un <code>crypt()</code> Hash de contraseña SHA-512 con formato <code>\$6\$<salt>\$<password hash></code> para una contraseña de al menos 8 y no más de 32 caracteres. Este hash se puede generar utilizando herramientas CLI, como la <code>openssl passwd</code> comando en modo SHA-512.	Mejores prácticas

Interfaces clave

INTERFAZ_OBJETIVO_nnnn

Valor	Designación
Nombre y descripción opcional de una interfaz adicional que desea agregar a este nodo. Puede agregar varias interfaces adicionales a cada nodo. Para <i>nnnn</i>, especifique un número único para cada entrada <code>INTERFACE_TARGET</code> que esté agregando. Para el valor, especifique el nombre de la interfaz física en el host físico. Luego, opcionalmente, agregue una coma y proporcione una descripción de la interfaz, que se muestra en la página de interfaces de VLAN y en la página de grupos de HA. Ejemplo: <code>INTERFACE_TARGET_0001=ens256, Trunk</code> Si agrega 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 HA; no necesita configurar una interfaz VLAN.	Opcional

Clave de RAM máxima

RAM MÁXIMA

Valor	Designación
La cantidad máxima de RAM que este nodo puede consumir. Si se omite esta clave, el nodo no tiene restricciones de memoria. Al configurar este campo para un nodo de nivel de producción, especifique un valor que sea al menos 24 GB y entre 16 y 32 GB menos que la RAM total del sistema. Nota: El valor de RAM afecta el espacio reservado de metadatos real de un nodo. Ver el "Descripción de qué es el Espacio Reservado de Metadatos" . El formato para este campo es <i>numberunit</i> , dónde <i>unit</i> puede ser b , k , m , o g . Ejemplos: 24g 38654705664b Nota: Si desea utilizar esta opción, debe habilitar el soporte del kernel para cgroups de memoria.	Opcional

Claves de tipo de nodo

TIPO DE NODO

Valor	Designación
Tipo de nodo: • Nodo de administración de máquina virtual • Nodo de almacenamiento de máquina virtual • Nodo de archivo de máquina virtual • Puerta de enlace de API de máquina virtual	Requerido

TIPO DE ALMACENAMIENTO

Valor	Designación
Define el tipo de objetos que contiene un nodo de almacenamiento. Para obtener más información, consulte "Tipos de nodos de almacenamiento". Esta clave solo es necesaria para los nodos con <code>NODE_TYPE = VM_Storage_Node</code>; no la especifique para otros tipos de nodos. Tipos de almacenamiento: • conjunto • data • metadatos Nota: Si no se especifica <code>STORAGE_TYPE</code>, el tipo de nodo de almacenamiento se establece como combinado (datos y metadatos) de manera predeterminada.	Opcional

Claves de reasignación de puertos

PUERTO_REMAP

Valor	Designación
Reasigna cualquier puerto utilizado por un nodo para comunicaciones internas del nodo de la red o comunicaciones externas. La reasignación de puertos es necesaria si las políticas de red empresarial restringen uno o más puertos utilizados por StorageGRID, como se describe en "Comunicaciones internas de los nodos de la red" o "Comunicaciones externas". IMPORTANTE: No reasigne los puertos que planea usar para configurar los puntos finales del balanceador de carga. Nota: Si solo se configura <code>PORT_REMAP</code>, la asignación que especifique se utiliza tanto para las comunicaciones entrantes como para las salientes. Si también se especifica <code>PORT_REMAP_INBOUND</code>, <code>PORT_REMAP</code> se aplica solo a las comunicaciones salientes. El formato utilizado es: <i>network type/protocol/default port used by grid node/new port</i>, donde <i>network type</i> es <code>grid</code>, <code>admin</code> o <code>cliente</code>, y <i>protocol</i> es <code>tcp</code> o <code>udp</code>. Ejemplo: <code>PORT_REMAP = client/tcp/18082/443</code> También puedes reasignar varios puertos usando una lista separada por comas. Ejemplo: <code>PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80</code>	Opcional

PUERTO_REMAP_ENTRADA

Valor	Designación
Reasigna las comunicaciones entrantes al puerto especificado. Si especifica PORT_REMAP_INBOUND pero no especifica un valor para PORT_REMAP, las comunicaciones salientes para el puerto no cambian. IMPORTANTE: No reasigne los puertos que planea usar para configurar los puntos finales del balanceador de carga. El formato utilizado es: <i>network type/protocol/remapped port /default port used by grid node</i>, donde <i>network type</i> es grid, admin o cliente, y <i>protocol</i> es tcp o udp. Ejemplo: PORT_REMAP_INBOUND = grid/tcp/3022/22 También puede reasignar varios puertos entrantes utilizando una lista separada por comas. Ejemplo: PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22	Opcional

Cómo los nodos de la red descubren el nodo de administración principal

Los nodos de la red se comunican con el nodo de administración principal para su configuración y gestión. Cada nodo de la red debe conocer la dirección IP del nodo de administración principal en la red de la red.

Para garantizar que un nodo de la red pueda acceder al nodo de administración principal, puede realizar una de las siguientes acciones al implementar el nodo:

- Puede utilizar el parámetro ADMIN_IP para ingresar manualmente la dirección IP del nodo de administración principal.
- Puede omitir el parámetro ADMIN_IP para que el nodo de la red descubra el valor automáticamente. El descubrimiento automático es especialmente útil cuando la red Grid utiliza DHCP para asignar la dirección IP al nodo de administración principal.

El descubrimiento automático del nodo de administración principal se logra mediante un sistema de nombres de dominio de multidifusión (mDNS). Cuando el nodo de administración principal se inicia por primera vez, publica su dirección IP mediante mDNS. Otros nodos de la misma subred pueden entonces consultar la dirección IP y adquirirla automáticamente. Sin embargo, debido a que el tráfico IP de multidifusión normalmente no se puede enrutar a través de subredes, los nodos en otras subredes no pueden adquirir la dirección IP del nodo de administración principal directamente.

Si utiliza el descubrimiento automático:



- Debe incluir la configuración ADMIN_IP para al menos un nodo de la red en cualquier subred a la que el nodo de administración principal no esté conectado directamente. Luego, este nodo de la red publicará la dirección IP del nodo de administración principal para que otros nodos de la subred la descubran con mDNS.
- Asegúrese de que su infraestructura de red admita el paso de tráfico IP de multidifusión dentro de una subred.

Archivos de configuración de nodos de ejemplo

Puede utilizar los archivos de configuración de nodo de ejemplo para ayudar a configurar los archivos de configuración de nodo para su sistema StorageGRID . Los ejemplos muestran archivos de configuración de nodos para todos los tipos de nodos de la red.

Para la mayoría de los nodos, puede agregar información de direccionamiento de red de administrador y cliente (IP, máscara, puerta de enlace, etc.) cuando configura la red mediante el Administrador de red o la API de instalación. La excepción es el nodo de administración principal. Si desea navegar hasta la IP de la red de administración del nodo de administración principal para completar la configuración de la red (porque la red de red no está enrutada, por ejemplo), debe configurar la conexión de la 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 objetivo Red de cliente se ha configurado como una práctica recomendada, aunque la Red de cliente está deshabilitada de forma predeterminada.

Ejemplo de nodo de administración principal

Nombre de archivo de ejemplo: `/etc/storagegrid/nodes/dc1-adm1.conf`

Contenido del archivo de ejemplo:

```

NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adml-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adml-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adml-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 de nodo de almacenamiento

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

Contenido del archivo de ejemplo:

```

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 de nodo de puerta de enlace

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

Contenido del archivo de ejemplo:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dcl-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 administración no principal

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

Contenido del archivo de ejemplo:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dcl-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dcl-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dcl-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 Para cada uno de sus nodos StorageGRID , debe validar el contenido de esos archivos.

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, la salida muestra **PASSED** para cada archivo de configuración, como se muestra en el ejemplo.



Al utilizar solo un LUN en nodos de solo metadatos, es posible que reciba un mensaje de advertencia que puede ignorarse.

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



Para una instalación automatizada, puede suprimir esta salida utilizando el `-q` o `--quiet` opciones en el `storagegrid` comando (por ejemplo, `storagegrid --quiet...`). Si suprime la salida, el comando tendrá un valor de salida distinto de 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 encuentran errores de configuración, deberá corregirlos antes de continuar con la instalación.

```

Checking for misnamed node configuration files...
WARNING: ignoring /etc/storagegrid/nodes/dcl-adml
WARNING: ignoring /etc/storagegrid/nodes/dcl-sn2.conf.keep
WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dcl-adml...
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 dcl-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 dcl-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 dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes...
ERROR: GRID_NETWORK_IP = 10.1.0.4
      dcl-sn2 and dcl-sn3 have the same GRID_NETWORK_IP
ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_RANGEDB_00

```

Iniciar el servicio de host de StorageGRID

Para iniciar los nodos StorageGRID y garantizar que se reinicien después de un reinicio del 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 garantizar que la implementación esté en curso:

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

3. Si algún nodo devuelve un estado de "No en ejecución" o "Detenido", ejecute el siguiente comando:

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

4. Si ya ha habilitado e iniciado el servicio de host StorageGRID (o si no está seguro de si el servicio se ha habilitado e iniciado), ejecute también el siguiente comando:

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

Configurar la red y completar la instalación (Red Hat)

Vaya al Administrador de cuadrícula

Utilice el Administrador de cuadrícula para definir toda la información necesaria para configurar su sistema StorageGRID .

Antes de empezar

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

Pasos

1. Abra su navegador web y navegue a:

```
https://primary_admin_node_ip
```

Alternativamente, puede acceder al Administrador de cuadrícula en el puerto 8443:

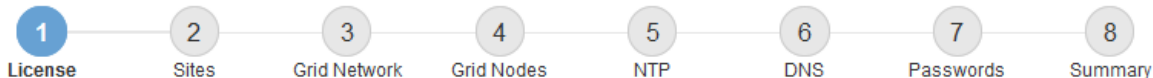
```
https://primary_admin_node_ip:8443
```

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

2. Administre una contraseña de instalador temporal según sea necesario:
 - Si ya se ha establecido una contraseña utilizando uno de estos métodos, introdúzcala para continuar.
 - Un usuario estableció la contraseña al acceder al instalador previamente
 - La contraseña se importó automáticamente desde el archivo de configuración del nodo en `/etc/storagegrid/nodes/<node_name>.conf`
 - Si no se ha establecido una contraseña, opcionalmente establezca una contraseña para proteger el instalador de StorageGRID .
3. Seleccione *Instalar un sistema StorageGRID *.

Aparece la página utilizada para configurar un sistema StorageGRID .

Install



License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File

Browse

Especifique la información de la licencia de StorageGRID

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

Pasos

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

Después de la instalación, el nombre se muestra en la parte superior del menú Nodos.

2. Seleccione **Explorar** y localice el archivo de licencia de NetApp(NLF-*unique-id*.txt) y seleccione **Abrir**.

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



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

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File NLF-959007-Internal.txt

License Serial Number

3. Seleccione **Siguiente**.

Agregar sitios

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

Pasos

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

Agregue tantos sitios adicionales como sean necesarios para su topología de cuadrícula. Puedes agregar hasta 16 sitios.

The screenshot shows the NetApp StorageGRID installation wizard. At the top is a blue header with 'NetApp® StorageGRID®' and a 'Help' dropdown. Below the header is a progress bar with eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS, 7. Passwords, and 8. Summary. Step 2, 'Sites', is currently selected and highlighted in blue. Below the progress bar, the 'Sites' section is displayed. It contains two paragraphs of text explaining single-site and multi-site deployments. Below the text are two input fields for site names. The first field is labeled 'Site Name 1' and contains the text 'Raleigh'. To its right is a minus sign icon (x). The second field is labeled 'Site Name 2' and contains the text 'Atlanta'. To its right are plus and minus icons (+ x).

3. Haga clic en **Siguiente**.

Especificar subredes de la red Grid

Debe especificar las subredes que se utilizan en la red Grid.

Acerca de esta tarea

Las entradas de subred incluyen las subredes de la red Grid para cada sitio en su sistema StorageGRID , junto con cualquier subred a la que se deba poder acceder a través de la red Grid.

Si tiene varias subredes de cuadrícula, se requiere la puerta de enlace de red de cuadrícula. Todas las subredes de la red 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 **Subred 1**.
2. Haga clic en el signo más junto a la última entrada para agregar una entrada de red adicional. Debe especificar todas las subredes para todos los sitios en la red Grid.
 - Si ya ha implementado al menos un nodo, haga clic en **Descubrir subredes de redes de cuadrícula** para completar automáticamente la Lista de subredes de redes de cuadrícula con las subredes

informadas por los nodos de cuadrícula que se han registrado con el Administrador de cuadrícula.

- Debe agregar manualmente cualquier subred para NTP, DNS, LDAP u otros servidores externos a los que se acceda a través de la puerta de enlace de Grid Network.

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 **Grid Network** 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

Grid Network

You must specify the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network for each site in your StorageGRID system. Select Discover Grid Networks to automatically add subnets based on the network configuration of all registered nodes.

Note: You must manually add any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnet 1 +

3. Haga clic en **Siguiente**.

Aprobar nodos de red pendientes

Debe aprobar cada nodo de la red antes de que pueda unirse al sistema StorageGRID .

Antes de empezar

Ha implementado todos los nodos de red del dispositivo virtual y StorageGRID .



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

Pasos

1. Revise la lista de Nodos pendientes y confirme que muestra todos los nodos de la red que implementó.



Si falta un nodo de la red, confirme que se haya implementado correctamente y que tenga la IP de red de la red correcta del nodo de administración principal configurada para ADMIN_IP.

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



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve		✖ Remove		Search		
	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address	
☒	50:6b:4b:42:d7:00	NetApp-SGA	Storage Node	StorageGRID Appliance	172.16.5.20/21	

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit		Reset		✖ Remove		Search	
	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address	
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21	
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21	
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21	
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21	
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21	

3. Haga clic en **Aprobar**.

4. En Configuración general, modifique la configuración de las siguientes propiedades, según sea necesario:

- **Sitio:** El nombre del sistema del sitio para este nodo de la cuadrícula.
- **Nombre:** El nombre del sistema para el nodo. El nombre predeterminado es el nombre que especificó cuando configuró el nodo.

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

- **Rol NTP:** El rol del Protocolo de tiempo de red (NTP) del nodo de la red. Las opciones son **Automático**, **Principal** y **Cliente**. Al seleccionar **Automático** se asigna la función principal a los nodos de administración, nodos de almacenamiento con servicios ADC, nodos de puerta de enlace y cualquier nodo de red que tenga direcciones IP no estáticas. A todos los demás nodos de la red se les asigna el rol de Cliente.



Asegúrese de que al menos dos nodos en cada sitio puedan acceder al menos a cuatro fuentes NTP externas. Si solo un nodo en un sitio puede acceder a las fuentes NTP, se producirán problemas de sincronización si ese nodo deja de funcionar. Además, designar dos nodos por sitio como fuentes NTP primarias garantiza una sincronización precisa si un sitio está aislado del resto de la red.

- **Tipo de almacenamiento** (solo nodos de almacenamiento): especifique que un nuevo nodo de almacenamiento se use exclusivamente para datos únicamente, solo metadatos o ambos. Las opciones son **Datos y metadatos** ("combinados"), **Solo datos** y **Solo metadatos**.



Ver "[Tipos de nodos de almacenamiento](#)" para obtener información sobre los requisitos para estos tipos de nodos.

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

5. En Grid Network, 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
- **Puerta de enlace**: La puerta de enlace de la red Grid. Por ejemplo: 192.168.0.1

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



Si seleccionó DHCP para la configuración de la red Grid y cambia el valor aquí, el nuevo valor se configurará como una dirección estática en el nodo. Debe asegurarse de que la dirección IP configurada no esté dentro de un grupo de direcciones DHCP.

6. Si desea configurar la red de administración para el nodo de la red, agregue o actualice las configuraciones en la sección Red de administración según sea necesario.

Introduzca las subredes de destino de las rutas que salen 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 la red de administración y cambia el valor aquí, el nuevo valor se configurará como una dirección estática en el nodo. Debe asegurarse de que la dirección IP configurada no esté dentro de un grupo de direcciones 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 podrá configurar en este cuadro de diálogo Administrador de red. En su lugar, debes seguir estos pasos:

- a. Reinicie el dispositivo: en el Instalador del dispositivo, seleccione **Avanzado > Reiniciar**.

El reinicio puede tardar varios minutos.

- b. Seleccione **Configurar redes > Configuración de enlace** y habilite las redes adecuadas.
- c. Seleccione **Configurar redes > Configuración IP** y configure las redes habilitadas.

- d. Regrese a la página de inicio y haga clic en **Iniciar instalación**.
- e. En el Administrador de cuadrícula: si el nodo figura en la tabla Nodos aprobados, elimine el nodo.
- f. Eliminar el nodo de la tabla Nodos pendientes.
- g. Espere a que el nodo vuelva a aparecer en la lista de Nodos pendientes.
- h. Confirme que puede configurar las redes adecuadas. Ya deberían estar completados con la información proporcionada en la página de Configuración de IP del Instalador del dispositivo.

Para obtener información adicional, consulte las instrucciones de instalación correspondientes al modelo de su electrodoméstico.

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



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

Dispositivos: Para un dispositivo StorageGRID , si la red del cliente no se configuró durante la instalación inicial mediante el instalador del dispositivo StorageGRID , no se podrá configurar en este cuadro de diálogo Administrador de Grid. En su lugar, debes seguir estos pasos:

- a. Reinicie el dispositivo: en el Instalador del dispositivo, seleccione **Avanzado > Reiniciar**.

El reinicio puede tardar varios minutos.

- b. Seleccione **Configurar redes > Configuración de enlace** y habilite las redes adecuadas.
- c. Seleccione **Configurar redes > Configuración IP** y configure las redes habilitadas.
- d. Regrese a la página de inicio y haga clic en **Iniciar instalación**.
- e. En el Administrador de cuadrícula: si el nodo figura en la tabla Nodos aprobados, elimine el nodo.
- f. Eliminar el nodo de la tabla Nodos pendientes.
- g. Espere a que el nodo vuelva a aparecer en la lista de Nodos pendientes.
- h. Confirme que puede configurar las redes adecuadas. Ya deberían estar completados con la información proporcionada en la página de Configuración de IP del Instalador del dispositivo.

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

8. Haga clic en **Guardar**.

La entrada del nodo de la cuadrícula se mueve a la lista de Nodos aprobados.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit

Reset

Remove

Search

	Grid Network MAC Address II	Name II	Site II	Type II	Platform II	Grid Network IPv4 Address ▼
	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

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

Debes aprobar todos los nodos que quieras en la red. Sin embargo, puede regresar 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 los nodos de la cuadrícula, haga clic en **Siguiente**.

Especifique la información del servidor de Protocolo de tiempo de red

Debe especificar la información de configuración del Protocolo de tiempo de red (NTP) para el sistema StorageGRID , de modo que las operaciones realizadas en servidores separados puedan mantenerse sincronizadas.

Acerca de esta tarea

Debe especificar direcciones IPv4 para los servidores NTP.

Debe especificar servidores NTP externos. Los servidores NTP especificados deben utilizar el protocolo NTP.

Debe especificar cuatro referencias de servidor NTP de Stratum 3 o superior para evitar problemas con la diferencia horaria.



Al especificar la fuente NTP externa para una instalación de 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 hora en versiones anteriores de Windows no es lo suficientemente preciso y Microsoft no lo admite para su uso en entornos de alta precisión, como StorageGRID.

["Límite de soporte para configurar el servicio de hora de Windows para entornos de alta precisión"](#)

Los servidores NTP externos son utilizados por los nodos a los que previamente les asignó roles NTP primarios.



Asegúrese de que al menos dos nodos en cada sitio puedan acceder al menos a cuatro fuentes NTP externas. Si solo un nodo en un sitio puede acceder a las fuentes NTP, se producirán problemas de sincronización si ese nodo deja de funcionar. Además, designar dos nodos por sitio como fuentes NTP primarias garantiza una sincronización precisa si un sitio está aislado del resto de la red.

Pasos

1. Especifique las direcciones IPv4 de 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 de servidor adicionales.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

Summary

Network Time Protocol

Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync.

Server 1

10.60.248.183

Server 2

10.227.204.142

Server 3

10.235.48.111

Server 4

0.0.0.0

+

3. Seleccione **Siguiente**.

Especificar la información del servidor DNS

Debe especificar la información de DNS para su sistema StorageGRID , de modo que pueda acceder a servidores externos utilizando nombres de host en lugar de direcciones IP.

Acerca de esta tarea

Especificando ["Información del servidor DNS"](#) le permite utilizar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP para notificaciones por correo electrónico y AutoSupport.

Para garantizar un funcionamiento correcto, especifique dos o tres servidores DNS. Si especifica más de tres, es posible que solo se utilicen tres debido a las limitaciones conocidas del sistema operativo en algunas plataformas. Si tiene restricciones de enrutamiento en su entorno, puede ["personalizar la lista de servidores DNS"](#) para que los nodos individuales (normalmente todos los nodos de un sitio) utilicen un conjunto diferente de hasta tres servidores DNS.

Si es posible, utilice servidores DNS a los que cada sitio pueda acceder localmente para garantizar que un sitio aislado pueda resolver los FQDN para destinos externos.

Pasos

1. Especifique la dirección IPv4 de 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 de servidor adicionales.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there's a blue header with "NetApp® StorageGRID®" and a "Help" link. Below the header is a progress bar with eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS (highlighted in blue), 7. Passwords, and 8. Summary. Below the progress bar, the "Domain Name Service" section is active. It contains instructions: "Enter the IP address for at least one Domain Name System (DNS) server, so that server hostnames can be used instead of IP addresses. Specifying at least two DNS servers is recommended. Configuring DNS enables server connectivity, email notifications, and NetApp AutoSupport." Below this, there are two input fields for DNS servers. "Server 1" has the IP address "10.224.223.130" and a red "X" icon to its right. "Server 2" has the IP address "10.224.223.136" and a red "+" icon to its right, indicating that more servers can be added.

La mejor práctica 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 de su sistema StorageGRID , deberá ingresar las contraseñas que se utilizarán para proteger su sistema y realizar tareas de mantenimiento.

Acerca de esta tarea

Utilice la página Instalar contraseñas para especificar la frase de contraseña de aprovisionamiento y la contraseña del usuario raíz de administración de la red.

- La frase de contraseña de aprovisionamiento se utiliza como clave de cifrado y no la almacena el sistema StorageGRID .
- Debe tener la contraseña de aprovisionamiento para los procedimientos de instalación, expansión y mantenimiento, incluida la descarga del paquete de recuperación. Por lo tanto, es importante que guardes la contraseña de aprovisionamiento en una ubicación segura.
- Puede cambiar la contraseña de aprovisionamiento desde el Administrador de Grid si tiene la actual.
- La contraseña del usuario raíz de administración de la red se puede cambiar mediante el Administrador de red.
- Las contraseñas de la consola de línea de comandos generadas aleatoriamente y de SSH se almacenan en el `Passwords.txt` archivo en el paquete de recuperación.

Pasos

1. En **Frase de contraseña de aprovisionamiento**, ingrese la frase de contraseña de aprovisionamiento que será necesaria para realizar cambios en la topología de la red de su sistema StorageGRID .

Guarde la contraseña de aprovisionamiento en un lugar seguro.



Si después de completarse la instalación desea cambiar la contraseña de aprovisionamiento más tarde, puede utilizar el Administrador de Grid. Seleccione **CONFIGURACIÓN > Control de acceso> Contraseñas de red**.

2. En **Confirmar contraseña de aprovisionamiento**, vuelva a ingresar la contraseña de aprovisionamiento para confirmarla.
3. En **Contraseña de usuario raíz de administración de red**, ingrese la contraseña que se utilizará para acceder al Administrador de red como usuario "root".

Guarde la contraseña en un lugar seguro.

4. En **Confirmar contraseña de usuario root**, vuelva a ingresar la contraseña de Grid Manager para confirmarla.

NetApp® StorageGRID®
Help

Install

1 License
2 Sites
3 Grid Network
4 Grid Nodes
5 NTP
6 DNS
7 Passwords
8 Summary

Passwords

Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step.

Provisioning
Passphrase

Confirm
Provisioning
Passphrase

Grid Management
Root User
Password

Confirm Root User
Password

☒ Create random command line passwords.

- Si está instalando una cuadrícula para fines de prueba de concepto o demostración, opcionalmente desmarque la casilla de verificación **Crear contraseñas de línea de comando aleatorias**.

Para las implementaciones de producción, siempre se deben utilizar contraseñas aleatorias por razones de seguridad. Borre **Crear contraseñas de línea de comando aleatorias** solo para cuadrículas de demostración si desea usar contraseñas predeterminadas para acceder a los nodos de la cuadrícula desde la línea de comando usando la cuenta "root" o "admin".



Se le solicitará que descargue el archivo del paquete de recuperación(`sgws-recovery-package-id-revision.zip`) después de hacer clic en **Instalar** en la página Resumen. Usted debe ["descargar este archivo"](#) para completar la instalación. Las contraseñas necesarias para acceder al sistema se almacenan en el `Passwords.txt` archivo, contenido en el archivo del paquete de recuperación.

- Haga clic en **Siguiente**.

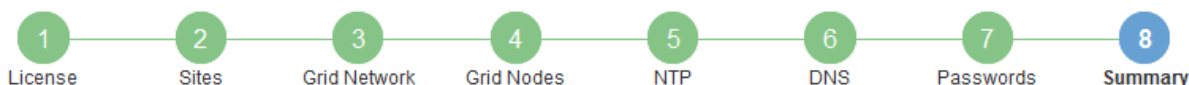
Revise su configuración y complete la instalación

Debe revisar cuidadosamente la información de configuración que ha ingresado para asegurarse de que la instalación se complete correctamente.

Pasos

- Ver la página **Resumen**.

Install



Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name	Grid1	Modify License
Passwords	Auto-generated random command line passwords	Modify Passwords

Networking

NTP	10.60.248.183 10.227.204.142 10.235.48.111	Modify NTP
DNS	10.224.223.130 10.224.223.136	Modify DNS
Grid Network	172.16.0.0/21	Modify Grid Network

Topology

Topology	Atlanta	Modify Sites	Modify Grid Nodes
	Raleigh		
	dc1-adm1	dc1-g1	dc1-s1
	dc1-s2	dc1-s3	NetApp-SGA

2. Verifique que toda la información de configuración de la red sea correcta. Utilice los enlaces Modificar en la página Resumen para volver atrás y corregir cualquier error.
3. Haga clic en **Instalar**.



Si un nodo está configurado para usar la red del cliente, la puerta de enlace predeterminada para ese nodo cambia de la red de cuadrícula a la red del cliente cuando hace clic en **Instalar**. Si pierde la conectividad, debe asegurarse de acceder al nodo de administración principal a través de una subred accesible. Ver "[Pautas para establecer redes](#)" Para más detalles.

4. Haga clic en **Descargar paquete de recuperación**.

Cuando la instalación avanza hasta el punto donde se define la topología de la red, se le solicitará que descargue el archivo del paquete de recuperación(.zip) y confirme que puede acceder correctamente al contenido de este archivo. Debe descargar el archivo del paquete de recuperación para poder recuperar el sistema StorageGRID si uno o más nodos de la red fallan. La instalación continúa en segundo plano, pero no puede completar la instalación ni acceder al sistema StorageGRID hasta que descargue y verifique este archivo.

5. Verifique que pueda extraer el contenido del .zip archivo y luego guárdelo en dos ubicaciones seguras, protegidas y separadas.



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

6. Seleccione la casilla de verificación **He descargado y verificado correctamente el archivo del paquete de recuperación** y haga clic en **Siguiente**.

Si la instalación aún está en curso, aparecerá la página de estado. Esta página indica el progreso de la instalación para cada nodo de la red.

Installation Status

If necessary, you may [Download the Recovery Package file](#) again.

Search

Name	IT	Site	IT	Grid Network IPv4 Address	Progress	IT	Stage	IT
dc1-adm1		Site1		172.16.4.215/21			Starting services	
dc1-g1		Site1		172.16.4.216/21			Complete	
dc1-s1		Site1		172.16.4.217/21			Waiting for Dynamic IP Service peers	
dc1-s2		Site1		172.16.4.218/21			Downloading hotfix from primary Admin if needed	
dc1-s3		Site1		172.16.4.219/21			Downloading hotfix from primary Admin if needed	

Cuando se alcanza la etapa Completado para todos los nodos de la red, aparece la página de inicio de sesión del Administrador de la red.

7. Sign in en Grid Manager utilizando el usuario "root" y la contraseña que especificó durante la instalación.

Pautas posteriores a la instalación

Después de completar la implementación y configuración del nodo de la red, siga estas pautas para el direccionamiento DHCP y los cambios de configuración de red.

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

Sólo se puede configurar DHCP durante la fase de implementación. No se puede configurar DHCP durante la configuración.



Los nodos se reinician cuando la configuración de la red Grid se modifica mediante DHCP, lo que puede provocar interrupciones si un cambio de DHCP afecta a varios nodos al mismo tiempo.

- Debe utilizar los procedimientos de Cambio de IP si desea cambiar direcciones IP, máscaras de subred y puertas de enlace predeterminadas para un nodo de la red. Ver "[Configurar direcciones IP](#)".
- Si realiza cambios en la configuración de red, incluidos cambios de enrutamiento y puerta de enlace, es posible que se pierda la conectividad del cliente con el nodo de administración principal y otros nodos de la red. Dependiendo de los cambios de red aplicados, es posible que sea necesario restablecer estas conexiones.

Instalación API REST

StorageGRID proporciona la API de instalación de StorageGRID para realizar tareas de instalación.

La API utiliza la plataforma API de código abierto Swagger para proporcionar la documentación de la API. Swagger permite que tanto los desarrolladores como los no desarrolladores interactúen con la API en una interfaz de usuario que ilustra cómo la API responde a los parámetros y opciones. Esta documentación asume que está familiarizado con las tecnologías web estándar y el formato de datos JSON.



Cualquier operación de API que realice utilizando la página web de Documentación de API son operaciones en vivo. 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, cualquier parámetro de URL obligatorio u opcional y una respuesta de API esperada.

API de instalación de StorageGRID

La API de instalación de StorageGRID solo está disponible cuando configura inicialmente su sistema StorageGRID y si necesita realizar una recuperación del nodo de administración principal. Se puede acceder a la API de instalación a través de HTTPS desde Grid Manager.

Para acceder a la documentación de la API, vaya a la página web de instalación en el nodo de administración principal y seleccione **Ayuda > Documentación de la API** en la barra de menú.

La API de instalación de StorageGRID incluye las siguientes secciones:

- **config** – Operaciones relacionadas con el lanzamiento del producto y las versiones de la API. Puede enumerar la versión de lanzamiento del producto y las versiones principales de la API compatibles con esa versión.
- **grid** – Operaciones de configuración a nivel de cuadrícula. Puede obtener y actualizar la configuración de la red, incluidos los detalles de la red, las subredes de la red, las contraseñas de la red y las direcciones IP del servidor NTP y DNS.
- **nodos** – Operaciones de configuración a nivel de nodo. Puede recuperar una lista de nodos de la cuadrícula, eliminar un nodo de la cuadrícula, configurar un nodo de la cuadrícula, ver un nodo de la cuadrícula y restablecer la configuración de un nodo de la cuadrícula.
- **provision** – 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.
- **recovery-package** – Operaciones para descargar el paquete de recuperación.
- **sitios** – Operaciones de configuración a nivel de sitio. Puede crear, ver, eliminar y modificar un sitio.
- **temporary-password** – Operaciones en la contraseña temporal para proteger la mgmt-api durante la instalación.

¿A dónde ir después?

Después de completar una instalación, realice las tareas de integración y configuración necesarias. Puede realizar las tareas opcionales según sea necesario.

Tareas requeridas

- "[Crear una cuenta de inquilino](#)" para el protocolo de cliente S3 que se utilizará para almacenar objetos en su sistema StorageGRID .
- "[Acceso al sistema de control](#)" mediante la configuración de grupos y cuentas de usuario. Opcionalmente, puedes "[configurar una fuente de identidad federada](#)" (como Active Directory o OpenLDAP), para que pueda importar grupos de administración y usuarios. O bien, puedes "[crear grupos y usuarios locales](#)" .

- Integrar y probar el ["S3 API"](#) aplicaciones cliente que utilizará para cargar objetos en su sistema StorageGRID .
- ["Configurar las reglas de gestión del ciclo de vida de la información \(ILM\) y la política de ILM"](#) que desea utilizar para proteger los datos del objeto.
- Si su instalación incluye nodos de almacenamiento de dispositivos, utilice SANtricity OS para completar las siguientes tareas:
 - Conéctese a cada dispositivo StorageGRID .
 - Verificar la recepción de datos de AutoSupport .

Ver ["Configurar el hardware"](#) .

- Revisar y seguir las ["Pautas de fortalecimiento del sistema StorageGRID"](#) para eliminar riesgos de seguridad.
- ["Configurar notificaciones por correo electrónico para alertas del sistema"](#) .

Tareas opcionales

- ["Actualizar las direcciones IP de los nodos de la red"](#) si han cambiado desde que planificó su implementación y generó el paquete de recuperación.
- ["Configurar el cifrado de almacenamiento"](#), si es necesario.
- ["Configurar la compresión de almacenamiento"](#) para reducir el tamaño de los objetos almacenados, si es necesario.
- ["Configurar interfaces VLAN"](#) para aislar y particionar el tráfico de la red, si es necesario.
- ["Configurar grupos de alta disponibilidad"](#) para mejorar la disponibilidad de la conexión para los clientes Grid Manager, Tenant Manager y S3, si es necesario.
- ["Configurar los puntos finales del balanceador de carga"](#) para la conectividad del cliente S3, si es necesario.

Solucionar problemas de instalación

Si ocurre algún problema durante la instalación del sistema StorageGRID , puede acceder a los archivos de registro de instalación. Es posible que el soporte técnico también necesite 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 la red)
- `/var/local/log/gdu-server.log` (se encuentra 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 saber cómo acceder a los archivos de registro, consulte ["Recopilar archivos de registro y datos del sistema"](#) .

Información relacionada

Ejemplo /etc/sysconfig/network-scripts

Puede utilizar los archivos de ejemplo para agregar cuatro interfaces físicas de Linux en un único enlace LACP y luego establecer tres interfaces VLAN que respalden el enlace para su uso como interfaces de red de cliente, administración y red de StorageGRID .

Interfaces físicas

Tenga en cuenta que los conmutadores en los otros extremos de los enlaces también deben tratar los cuatro puertos como un único canal troncal o puerto LACP y deben pasar al menos las tres VLAN referenciadas 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 enlace

/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 StorageGRID en Ubuntu o Debian

Inicio rápido para instalar StorageGRID en Ubuntu o Debian

Siga estos pasos de alto nivel para instalar un nodo StorageGRID de Ubuntu o Debian.

1

Preparación

- Conozca más sobre "[Arquitectura y topología de red de StorageGRID](#)".
- Conozca los detalles de "[Redes StorageGRID](#)".
- Reúne y prepara el "[Información y materiales necesarios](#)".
- Preparar lo necesario "[CPU y RAM](#)".
- Mantener "[requisitos de almacenamiento y rendimiento](#)".
- "[Preparar los servidores Linux](#)" que alojará sus nodos StorageGRID.

2

Despliegue

Implementar nodos de red. Cuando se implementan nodos de red, estos se crean como parte del sistema StorageGRID y se conectan a una o más redes.

- Para implementar nodos de red basados en software en los hosts que preparó en el paso 1, use la línea de comandos de Linux y ["archivos de configuración de nodos"](#) .
- Para implementar nodos del dispositivo StorageGRID , siga las instrucciones ["Inicio rápido para la instalación de hardware"](#) .

3

Configuración

Cuando se hayan implementado todos los nodos, utilice el Administrador de cuadrícula para ["Configurar la red y completar la instalación"](#) .

Automatizar la instalación

Para ahorrar tiempo y brindar coherencia, puede automatizar la instalación del servicio de host StorageGRID y la configuración de los nodos de la red.

- Utilice un marco de orquestación estándar como Ansible, Puppet o Chef para automatizar:
 - Instalación de Ubuntu o Debian
 - Configuración de redes y almacenamiento
 - Instalación del motor de contenedores y el servicio de host StorageGRID
 - Despliegue de nodos de red virtuales

Ver ["Automatice la instalación y configuración del servicio de host StorageGRID"](#) .

- Después de implementar los nodos de la red, ["automatizar la configuración del sistema StorageGRID"](#) utilizando el script de configuración de Python proporcionado en el archivo de instalación.
- ["Automatizar la instalación y configuración de nodos de red de dispositivos"](#)
- Si es un desarrollador avanzado de implementaciones de StorageGRID , automatice la instalación de nodos de la red mediante el uso de ["API REST de instalación"](#) .

Planifique y prepare la instalación en Ubuntu o Debian

Información y materiales necesarios

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

Información requerida

Plan de red

Qué redes desea conectar a cada nodo de StorageGRID . StorageGRID admite múltiples redes para separación de tráfico, seguridad y conveniencia administrativa.

Ver StorageGRID ["Pautas para establecer redes"](#) .

Información de la red

Direcciones IP a asignar a cada nodo de la red y las direcciones IP de los servidores DNS y NTP.

Servidores para nodos de red

Identifique un conjunto de servidores (físicos, virtuales o ambos) que, en conjunto, proporcionen recursos suficientes para soportar la cantidad y el tipo de nodos StorageGRID que planea implementar.



Si su instalación de StorageGRID no utilizará nodos de almacenamiento del dispositivo StorageGRID (hardware), deberá utilizar almacenamiento RAID de hardware con caché de escritura respaldado por batería (BBWC). StorageGRID no admite el uso de redes de área de almacenamiento virtual (vSAN), RAID de software o ninguna protección RAID.

Migración de nodos (si es necesario)

Entender el ["Requisitos para la migración de nodos"](#) , si desea realizar mantenimiento programado en hosts físicos sin ninguna interrupción del servicio.

Información relacionada

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Materiales necesarios

Licencia de NetApp StorageGRID

Debe tener una licencia de NetApp válida y firmada digitalmente.



En el archivo de instalación de StorageGRID se incluye una licencia que no es de producción y que se puede utilizar para realizar pruebas y comprobar el concepto de las redes.

Archivo de instalación de StorageGRID

["Descargue el archivo de instalación de StorageGRID y extraiga los archivos"](#) .

Servicio de computadora portátil

El sistema StorageGRID se instala a través de una computadora portátil de servicio.

La computadora portátil de servicio debe tener:

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

Documentación de StorageGRID

- ["Notas de la versión"](#)
- ["Instrucciones para administrar StorageGRID"](#)

Descargue y extraiga los archivos de instalación de StorageGRID

Debe descargar el archivo de instalación de StorageGRID y extraer los archivos necesarios. Opcionalmente, puede verificar manualmente los archivos en el paquete de instalación.

Pasos

1. Ir a la ["Página de descargas de NetApp para StorageGRID"](#) .
2. Seleccione el botón para descargar la última versión o seleccione otra versión del menú desplegable y

seleccione **Ir**.

3. Sign in con el nombre de usuario y la contraseña de su cuenta de NetApp .
4. Si aparece una declaración de Precaución/Lectura obligatoria, léala y seleccione la casilla de verificación.



Debe aplicar las revisiones necesarias después de instalar la versión de StorageGRID . Para obtener más información, consulte la "[Procedimiento de revisión en las instrucciones de recuperación y mantenimiento](#)"

5. Lea el Acuerdo de licencia de usuario final, seleccione la casilla de verificación y luego seleccione **Aceptar y continuar**.
6. En la columna **Instalar StorageGRID**, seleccione el archivo de instalación .tgz o .zip para Ubuntu o Debian.



Seleccione el .zip archivo si está ejecutando Windows en la computadora portátil de servicio.

7. Guarde el archivo de instalación.
8. Si necesita verificar el archivo de instalación:
 - a. Descargue el paquete de verificación de firma de código de StorageGRID . El nombre de archivo de este paquete utiliza el formato `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , dónde `<version-number>` es la versión del software StorageGRID .
 - b. Siga los pasos para "[verificar manualmente los archivos de instalación](#)" .
9. Extraiga los archivos del archivo de instalación.
10. Elige los archivos que necesitas.

Los archivos que necesita dependen de la topología de red planificada y de cómo implementará su 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
	Un 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 puede utilizar para realizar pruebas e implementaciones de prueba de concepto.
	Paquete DEB para instalar las imágenes del nodo StorageGRID en hosts Ubuntu o Debian.

Ruta y nombre de archivo	Descripción
	Suma de comprobación MD5 del archivo <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .
	Paquete DEB para instalar el servicio de host StorageGRID en hosts Ubuntu o Debian.
Herramienta de scripting de implementación	Descripción
	Un script de Python utilizado para automatizar la configuración de un sistema StorageGRID.
	Un script de Python utilizado para automatizar la configuración de dispositivos StorageGRID.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único está habilitado. También puede utilizar este script para la integración de Ping Federate.
	Un archivo de configuración de ejemplo para usar con el <code>configure-storagegrid.py</code> guion.
	Un archivo de configuración en blanco para usar con el <code>configure-storagegrid.py</code> guion.
	Ejemplo de rol y manual de estrategias de Ansible para configurar hosts Ubuntu o Debian para la implementación de contenedores StorageGRID. Puede personalizar el rol o el libro de jugadas según sea necesario.
	Un ejemplo de secuencia de comandos de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script de ayuda llamado por el compañero <code>storagegrid-ssoauth-azure.py</code> Script de Python para realizar interacciones de SSO con Azure.

Ruta y nombre de archivo	Descripción
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno de StorageGRID que no sea de producción para realizar pruebas de compatibilidad de actualización.

Verificar manualmente los archivos de instalación (opcional)

Si es necesario, puede verificar manualmente los archivos en el archivo de instalación de StorageGRID .

Antes de empezar

Tienes ["descargué el paquete de verificación"](#) desde ["Página de descargas de NetApp para StorageGRID"](#) .

Pasos

1. Extraiga los artefactos del paquete de verificación:

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Asegúrese de que se hayan extraído estos artefactos:

- Certificado de hoja: Leaf-Cert.pem
- Cadena de certificados: CA-Int-Cert.pem
- Cadena de respuesta de marca de tiempo: TS-Cert.pem
- Archivo de suma de comprobación: sha256sum
- Firma de suma de comprobación: sha256sum.sig
- Archivo de respuesta de marca de tiempo: sha256sum.sig.tsr

3. Utilice la cadena para verificar que el certificado de hoja sea válido.

Ejemplo: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

Resultado esperado: Leaf-Cert.pem: OK

4. Si el paso 2 falló debido a un certificado de hoja vencido, utilice el `tsr` archivo a verificar.

Ejemplo: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

Los resultados esperados incluyen: Verification: OK

5. Cree un archivo de clave pública a partir del certificado de hoja.

Ejemplo: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

Resultado esperado: *ninguno*

6. Utilice la clave pública para verificar la sha256sum archivo contra sha256sum.sig .

Ejemplo: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

Resultado esperado: Verified OK

7. Verificar el sha256sum contenido del archivo contra sumas de comprobación recién creadas.

Ejemplo: `sha256sum -c sha256sum`

Resultado esperado: `<filename>: OK`
`<filename>` es el nombre del archivo que descargaste.

8. ["Complete los pasos restantes"](#) para extraer y elegir los archivos de instalación adecuados.

Requisitos de software para Ubuntu y Debian

Puede utilizar una máquina virtual para alojar cualquier tipo de nodo StorageGRID . Necesita una máquina virtual para cada nodo de la red.

Para instalar StorageGRID en Ubuntu o Debian, debe instalar algunos paquetes de software de terceros. Algunas distribuciones de Linux compatibles no contienen estos paquetes de forma predeterminada. Las versiones de paquetes de software en las que se prueban las instalaciones de StorageGRID incluyen las que se enumeran en esta página.

Si selecciona una distribución de Linux y una opción de instalación en tiempo de ejecución de contenedor que requiere alguno de estos paquetes, y la distribución de Linux no los instala automáticamente, instale una de las versiones enumeradas aquí si está disponible a través de su proveedor o del vendedor de soporte para su distribución de Linux. De lo contrario, utilice las versiones de paquetes predeterminadas disponibles de su proveedor.

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



La compatibilidad con Docker como motor de contenedores para implementaciones de solo software está obsoleta. Docker será reemplazado por otro motor de contenedores en una versión futura.

Versiones de Python probadas

- 3.5.2-2
- 3.6.8-2
- 3.6.8-38
- 3.6.9-1
- 3.7.3-1
- 3.8.10-0
- 3.9.2-1

- 3.9.10-2
- 3.9.16-1
- 3.10.6-1
- 3.11.2-6

Versiones de Podman probadas

- 3.2.3-0
- 3.4.4+ds1
- 4.1.1-7
- 4.2.0-11
- 4.3.1+ds1-8+b1
- 4.4.1-8
- 4.4.1-12

Versiones de Docker probadas



La compatibilidad con Docker está obsoleta y se eliminará en una versión futura.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23.0.6-1
- Docker-CE 24.0.2-1
- Docker-CE 24.0.4-1
- Docker-CE 24.0.5-1
- Docker-CE 24.0.7-1
- 1,5-2

Requisitos de CPU y RAM

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

Cada nodo de StorageGRID requiere los siguientes recursos mínimos:

- Núcleos de CPU: 8 por nodo
- RAM: depende de la RAM total disponible y de la cantidad de software que no sea StorageGRID que se ejecute en el sistema
 - Generalmente, al menos 24 GB por nodo y de 2 a 16 GB menos que la RAM total del sistema.
 - Un mínimo de 64 GB para cada inquilino que tendrá aproximadamente 5000 buckets

Los recursos de nodo de solo metadatos basados en software deben coincidir con los recursos de los nodos de almacenamiento existentes. Por ejemplo:

- Si el sitio StorageGRID existente utiliza dispositivos SG6000 o SG6100, los nodos de solo metadatos

basados en software deben cumplir los siguientes requisitos mínimos:

- 128 GB de RAM
- CPU de 8 núcleos
- SSD de 8 TB o almacenamiento equivalente para la base de datos Cassandra (rangedb/0)
- Si el sitio StorageGRID existente usa nodos de almacenamiento virtuales con 24 GB de RAM, CPU de 8 núcleos y 3 TB o 4 TB de almacenamiento de metadatos, los nodos solo de metadatos basados en software deben usar recursos similares (24 GB de RAM, CPU de 8 núcleos y 4 TB de almacenamiento de metadatos (rangedb/0)).

Al agregar un nuevo sitio StorageGRID , la capacidad total de metadatos del nuevo sitio debe coincidir, como mínimo, con los sitios StorageGRID existentes y los recursos del nuevo sitio deben coincidir con los nodos de almacenamiento de los sitios StorageGRID existentes.

Asegúrese de que la cantidad de nodos StorageGRID que planea ejecutar en cada host físico o virtual no exceda la cantidad de núcleos de CPU o la RAM física disponible. Si los hosts no están dedicados a ejecutar StorageGRID (no recomendado), asegúrese de considerar los requisitos de recursos de las otras aplicaciones.



Supervise periódicamente el uso de su CPU y memoria para garantizar que estos recursos sigan adaptándose a su carga de trabajo. Por ejemplo, duplicar la asignación de RAM y CPU para los nodos de almacenamiento virtuales proporcionaría recursos similares a los proporcionados para los nodos del dispositivo StorageGRID . Además, si la cantidad de metadatos por nodo supera los 500 GB, considere aumentar la RAM por nodo a 48 GB o más. Para obtener información sobre cómo administrar el almacenamiento de metadatos de objetos, aumentar la configuración del espacio reservado de metadatos y monitorear el uso de CPU y memoria, consulte las instrucciones para ["administrando"](#) , ["escucha"](#) , y ["actualización"](#) StorageGRID.

Si el hiperprocesamiento está habilitado en los hosts físicos subyacentes, puede proporcionar 8 núcleos virtuales (4 núcleos físicos) por nodo. Si el hiperprocesamiento no está habilitado en los hosts físicos subyacentes, debe proporcionar 8 núcleos físicos por nodo.

Si utiliza máquinas virtuales como hosts y tiene control sobre el tamaño y la cantidad de máquinas virtuales, debe usar una sola máquina virtual para cada nodo StorageGRID y dimensionar la máquina virtual en consecuencia.

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

Consulte también ["Requisitos de almacenamiento y rendimiento"](#) .

Requisitos de almacenamiento y rendimiento

Debe comprender los requisitos de almacenamiento para los nodos StorageGRID , de modo que pueda proporcionar suficiente espacio para soportar la configuración inicial y la futura expansión del almacenamiento.

Los nodos StorageGRID requieren tres categorías lógicas de almacenamiento:

- **Grupo de contenedores:** almacenamiento de nivel de rendimiento (SAS o SSD de 10 000 GB) para los contenedores de nodos, que se asignarán al controlador de almacenamiento de Docker cuando instale y configure Docker en los hosts que soportarán sus nodos StorageGRID .
- **Datos del sistema** – Almacenamiento de nivel de rendimiento (SAS o SSD de 10 000 rpm) para almacenamiento persistente por nodo de datos del sistema y registros de transacciones, que los servicios de host de StorageGRID consumirán y asignarán a nodos individuales.
- **Datos de objetos:** almacenamiento de nivel de rendimiento (SAS o SSD de 10 000 rpm) y almacenamiento masivo de nivel de capacidad (NL-SAS/SATA) para el almacenamiento persistente de datos de objetos y metadatos de objetos.

Debe utilizar dispositivos de bloque respaldados por RAID para todas las categorías de almacenamiento. No se admiten discos no redundantes, SSD ni JBOD. Puede utilizar almacenamiento RAID local o compartido para cualquiera de las categorías de almacenamiento; sin embargo, si desea utilizar la capacidad de migración de nodos en StorageGRID, debe almacenar los datos del sistema y los datos de los objetos en el almacenamiento compartido. Para obtener más información, consulte ["Requisitos de migración del contenedor de nodos"](#) .

Requisitos de rendimiento

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

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

Requisitos para los hosts que utilizan almacenamiento NetApp ONTAP

Si el nodo StorageGRID usa almacenamiento asignado desde un sistema NetApp ONTAP , confirme que el volumen no tenga habilitada una política de niveles de FabricPool . Deshabilitar la organización en niveles de FabricPool para los volúmenes utilizados con nodos StorageGRID simplifica la resolución de problemas y las operaciones de almacenamiento.



Nunca use FabricPool para agrupar datos relacionados con StorageGRID en StorageGRID mismo. La organización de los datos de StorageGRID en niveles en StorageGRID aumenta la resolución de problemas y la complejidad operativa.

Número de hosts necesarios

Cada sitio de StorageGRID requiere un mínimo de tres nodos de almacenamiento.



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

Se pueden implementar otros tipos de nodos, como nodos de administración o nodos de puerta de enlace, en los mismos hosts o en sus propios hosts dedicados según sea necesario.

Número de volúmenes de almacenamiento para cada host

La siguiente tabla muestra la cantidad de volúmenes de almacenamiento (LUN) necesarios para cada host y el tamaño mínimo requerido para cada LUN, en función de los nodos que se implementarán en ese host.

El tamaño máximo de LUN probado es 39 TB.



Estos números son para cada host, no para toda la red.

Propósito del LUN	Categoría de almacenamiento	Número de LUN	Tamaño mínimo/LUN
Piscina de almacenamiento de motores de contenedores	Pool de contenedores	1	Número total de nodos × 100 GB
`/var/local` volumen	Datos del sistema	1 para cada nodo en este host	90 GB
Nodo de almacenamiento	Datos de objeto	3 para cada nodo de almacenamiento en este host Nota: Un nodo de almacenamiento basado en software puede tener de 1 a 48 volúmenes de almacenamiento; se recomiendan al menos 3 volúmenes de almacenamiento.	12 TB (4 TB/LUN) Ver Requisitos de almacenamiento para nodos de almacenamiento Para más información.
Nodo de almacenamiento (solo metadatos)	Metadatos de objetos	1	4 TB Ver Requisitos de almacenamiento para nodos de almacenamiento Para más información. Nota: Solo se requiere una rangedb para los nodos de almacenamiento de solo metadatos.
Registros de auditoría del nodo de administración	Datos del sistema	1 para cada nodo de administración en este host	200 GB
Tablas del nodo de administración	Datos del sistema	1 para cada nodo de administración en este host	200 GB



Según el nivel de auditoría configurado, el tamaño de las entradas del usuario, como el nombre de la clave del objeto S3, y la cantidad de datos del registro de auditoría que necesita conservar, es posible que deba aumentar el tamaño del LUN del registro de auditoría en cada nodo de administración. Generalmente, una cuadrícula genera aproximadamente 1 KB de datos de auditoría por operación S3, lo que significaría que un LUN de 200 GB admitiría 70 millones de operaciones por día u 800 operaciones por segundo durante dos o tres días.

Espacio mínimo de almacenamiento para un host

La siguiente tabla muestra el espacio de almacenamiento mínimo requerido 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, en función de qué nodos se implementarán en ese host.



Las instantáneas de disco no se pueden usar para restaurar nodos de la red. En su lugar, consulte la ["recuperación del nodo de la red"](#) procedimientos para cada tipo de nodo.

Tipo de nodo	Pool de contenedores	Datos del sistema	Datos de objeto
Nodo de almacenamiento	100 GB	90 GB	4.000 GB
Nodo de administración	100 GB	490 GB (3 LUN)	<i>no aplicable</i>
Nodo de puerta de enlace	100 GB	90 GB	<i>no aplicable</i>

Ejemplo: Cálculo de los requisitos de almacenamiento para un host

Supongamos 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 datos del sistema y registros de transacciones, y 12 TB de almacenamiento de nivel de capacidad para datos de objetos.

Tipo de nodo	Propósito del LUN	Número de LUN	Tamaño de LUN
Nodo de almacenamiento	Grupo de almacenamiento de Docker	1	300 GB (100 GB/nodo)
Nodo de almacenamiento	`/var/local` volumen	1	90 GB
Nodo de almacenamiento	Datos de objeto	3	12 TB (4 TB/LUN)
Nodo de administración	`/var/local` volumen	1	90 GB
Nodo de administración	Registros de auditoría del nodo de administración	1	200 GB
Nodo de administración	Tablas del nodo de administración	1	200 GB

Tipo de nodo	Propósito del LUN	Número de LUN	Tamaño de LUN
Nodo de puerta de enlace	`/var/local` volumen	1	90 GB
Total		9	Grupo de contenedores: 300 GB Datos del sistema: 670 GB Datos del objeto: 12.000 GB

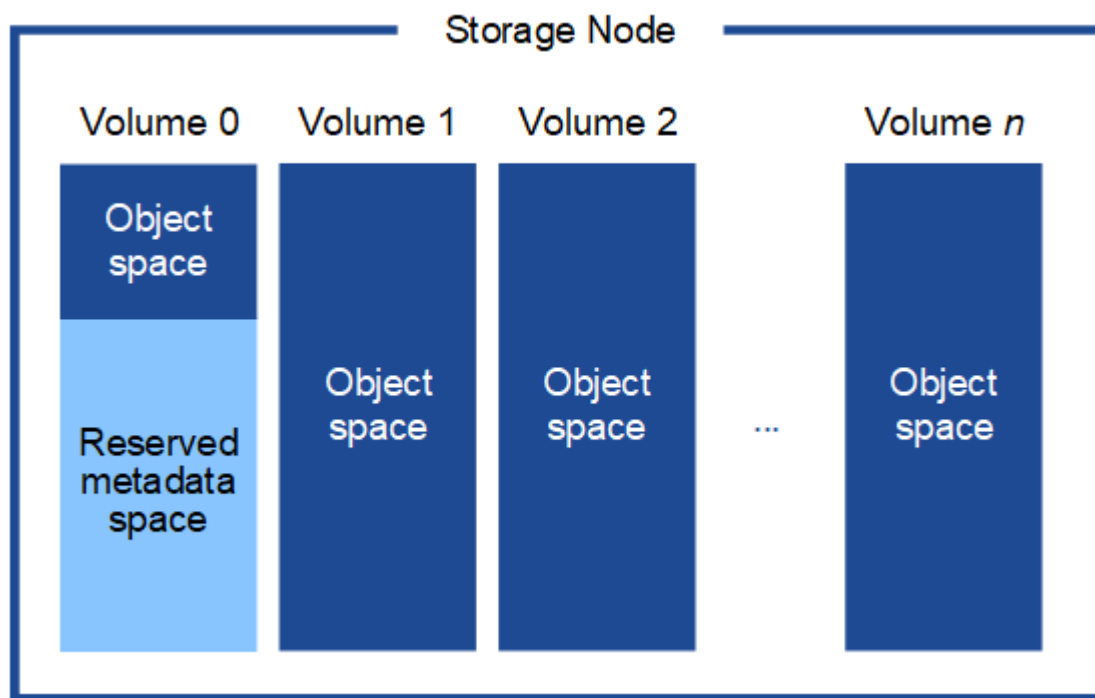
Requisitos de almacenamiento para nodos de almacenamiento

Un nodo de almacenamiento basado en software puede tener de 1 a 48 volúmenes de almacenamiento; se recomiendan 3 o más volúmenes de almacenamiento. Cada volumen de almacenamiento debe ser de 4 TB o más.



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

Como se muestra en la figura, StorageGRID reserva espacio para los metadatos de objetos 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 datos de objetos.



Para proporcionar redundancia y proteger los metadatos de los objetos contra pérdidas, StorageGRID almacena tres copias de los metadatos de todos los objetos del sistema en cada sitio. Las tres copias de metadatos de objetos se distribuyen uniformemente entre todos los nodos de almacenamiento en cada sitio.

Al instalar una cuadrícula con nodos de almacenamiento solo de metadatos, la cuadrícula también debe contener una cantidad mínima de nodos para el almacenamiento de objetos. Ver ["Tipos de nodos de almacenamiento"](#) para obtener más información sobre los nodos de almacenamiento de solo metadatos.

- Para una cuadrícula de un solo sitio, se configuran al menos dos nodos de almacenamiento para objetos y metadatos.
- Para una cuadrícula de varios sitios, se configura al menos un nodo de almacenamiento por sitio para objetos y metadatos.

Cuando asigna espacio al volumen 0 de un nuevo nodo de almacenamiento, debe asegurarse de que haya espacio adecuado para la parte de metadatos de objetos de ese nodo.

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



Si usa solo un volumen de almacenamiento para un nodo de almacenamiento y asigna 4 TB o menos al volumen, el nodo de almacenamiento podría ingresar al estado de solo lectura de almacenamiento al iniciarse y almacenar solo metadatos de objetos.



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

- Los recursos de nodo de solo metadatos basados en software deben coincidir con los recursos de los nodos de almacenamiento existentes. Por ejemplo:
 - Si el sitio StorageGRID existente utiliza dispositivos SG6000 o SG6100, los nodos de solo metadatos basados en software deben cumplir los siguientes requisitos mínimos:
 - 128 GB de RAM
 - CPU de 8 núcleos
 - SSD de 8 TB o almacenamiento equivalente para la base de datos Cassandra (rangedb/0)
 - Si el sitio StorageGRID existente usa nodos de almacenamiento virtuales con 24 GB de RAM, CPU de 8 núcleos y 3 TB o 4 TB de almacenamiento de metadatos, los nodos solo de metadatos basados en software deben usar recursos similares (24 GB de RAM, CPU de 8 núcleos y 4 TB de almacenamiento de metadatos (rangedb/0)).

Al agregar un nuevo sitio StorageGRID, la capacidad total de metadatos del nuevo sitio debe coincidir, como mínimo, con los sitios StorageGRID existentes y los recursos del nuevo sitio deben coincidir con los nodos de almacenamiento de los sitios StorageGRID existentes.

- Si está instalando un nuevo sistema (StorageGRID 11.6 o superior) y cada nodo de almacenamiento tiene 128 GB o más de RAM, asigne 8 TB o más al volumen 0. El uso de un valor mayor para el volumen 0 puede aumentar el espacio permitido para los metadatos en cada nodo de almacenamiento.
- Al configurar diferentes nodos de almacenamiento para un sitio, utilice la misma configuración para el volumen 0 si es posible. Si un sitio contiene nodos de almacenamiento de diferentes tamaños, el nodo de almacenamiento con el volumen más pequeño (0) determinará la capacidad de metadatos de ese sitio.

Para más detalles, visite ["Administrar el almacenamiento de metadatos de objetos"](#).

Requisitos de migración del contenedor de nodos

La función de migración de nodos le 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 del host físico sin interrumpir las operaciones de la red. Mueva todos los nodos de StorageGRID , uno a la vez, a otro host antes de desconectar el host físico. La migración de nodos solo requiere un breve tiempo de inactividad para cada nodo y no debería afectar el funcionamiento ni la disponibilidad de los servicios de la red.

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

- Nombres de interfaz de red consistentes en todos los hosts de un único centro de datos físico
- Almacenamiento compartido para metadatos de StorageGRID y volúmenes de repositorio de objetos al que pueden acceder todos los hosts en un único centro de datos físico. Por ejemplo, puede utilizar matrices de almacenamiento NetApp E-Series.

Si está utilizando hosts virtuales y la capa de hipervisor subyacente admite la migración de VM, es posible que desee utilizar esta capacidad en lugar de la función de migración de nodos en StorageGRID. En este caso, puedes ignorar estos requisitos adicionales.

Antes de realizar la migración o el mantenimiento del hipervisor, apague los nodos correctamente. Vea las instrucciones para ["apagar un nodo de la red"](#) .

VMware Live Migration no compatible

Al realizar una instalación completa en máquinas virtuales VMware, OpenStack Live Migration y VMware Live vMotion provocan saltos en el reloj de la máquina virtual y no son compatibles con nodos de red de ningún tipo. Aunque es poco frecuente, los horarios de reloj incorrectos pueden provocar la pérdida de datos o actualizaciones de configuración.

Se admite la migración en frío. En la migración en frío, se apagan los nodos StorageGRID antes de migrarlos entre hosts. Vea las instrucciones para ["apagar un nodo de la red"](#) .

Nombres de interfaz de red consistentes

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

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

eth0 **→** **bond0.1001**

eth1 **→** **bond0.1002**

eth2 **→** **bond0.1003**

El lado izquierdo de las flechas corresponde a las interfaces tradicionales vistas desde dentro de 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 enlace 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 traslado, asumiendo que las interfaces con el mismo nombre proporcionarán la misma conectividad en Host2 que en Host1. Si Host2 no tiene interfaces con los mismos nombres, no se permitirá el movimiento.

Hay muchas formas de lograr una denominación de interfaz de red consistente en varios hosts; consulte ["Configurar la red del host"](#) para algunos ejemplos.

Almacenamiento compartido

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

Pasos

1. Durante la operación de "exportación de nodo", se extrae una pequeña cantidad de datos de estado persistentes del contenedor de nodo que se ejecuta en HostA y se almacena en caché en el volumen de datos del sistema de ese nodo. Luego, se desinstancia el contenedor de nodo en HostA.
2. Durante la operación de "importación de nodo", se crea una instancia del contenedor de nodo en HostB que utiliza la misma interfaz de red y asignaciones de almacenamiento en bloque que estaban vigentes en HostA. Luego, los datos de estado persistente almacenados en caché se insertan en la nueva instancia.

Dado este modo de operación, todos los datos del sistema del nodo y los volúmenes de almacenamiento de objetos deben ser accesibles tanto desde HostA como desde HostB para que se permita la migración y funcione. Además, deben haber sido mapeados al nodo usando nombres que garanticen que hacen referencia a los mismos LUN en HostA y HostB.

El siguiente ejemplo muestra una solución para el mapeo de dispositivos de bloque para un nodo de almacenamiento StorageGRID, donde se utiliza la multiruta DM en los hosts y se ha utilizado el campo de alias en `/etc/multipath.conf` para proporcionar nombres de dispositivos de bloque consistentes y amigables 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
```

Preparar los hosts (Ubuntu o Debian)

Cómo cambian las configuraciones de todo el host durante la instalación

En sistemas físicos, StorageGRID realiza algunos cambios en todo el host `sysctl` ajustes.

Se realizan los siguientes cambios:


```

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

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

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

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

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

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

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

```

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

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

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

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

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

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

Instalar Linux

Debe instalar StorageGRID en todos los hosts de red Ubuntu o Debian. Para obtener una lista de las versiones compatibles, utilice la herramienta Matriz de interoperabilidad de NetApp .

Antes de empezar

Asegúrese de que su sistema operativo cumpla con los requisitos mínimos de versión de kernel de StorageGRID, como se detalla a continuación. Utilice el comando `uname -r` para obtener la versión del kernel de su sistema operativo o consulte con el proveedor de su sistema operativo.

Nota: La compatibilidad con las versiones 18.04 y 20.04 de Ubuntu ha quedado obsoleta y se eliminará en una versión futura.

Versión de Ubuntu	Versión mínima del kernel	Nombre del paquete del kernel
18.04.6 (obsoleto)	5.4.0-150-genérico	imagen-de-linux-5.4.0-150-genérica/actualizaciones-bionic,seguridad-bionic,ahora 5.4.0-150.167~18.04.1
20.04.5 (obsoleto)	5.4.0-131-genérico	imagen-de-linux-5.4.0-131-genérica/actualizaciones-focales, ahora 5.4.0-131.147
22.04.1	5.15.0-47-genérico	imagen-de-linux-5.15.0-47-genérica/actualizaciones-de-jammy,seguridad-de-jammy,ahora 5.15.0-47.51
24.04	6.8.0-31-genérico	imagen-de-linux-6.8.0-31-genérica/noble,ahora 6.8.0-31.31

Nota: El soporte para la versión 11 de Debian ha quedado obsoleto y se eliminará en una versión futura.

Versión de Debian	Versión mínima del kernel	Nombre del paquete del kernel
11 (obsoleto)	5.10.0-18-amd64	imagen de Linux 5.10.0-18-amd64/estable, ahora 5.10.150-1
12	6.1.0-9-amd64	imagen de Linux 6.1.0-9-amd64/estable, ahora 6.1.27-1

Pasos

1. Instale Linux en todos los hosts de la red física o virtual de acuerdo con las instrucciones del distribuidor o su procedimiento estándar.



No instale ningún entorno de escritorio gráfico. Al instalar Ubuntu, debes seleccionar **utilidades del sistema estándar**. Se recomienda seleccionar **Servidor OpenSSH** para habilitar el acceso ssh a sus hosts Ubuntu. Todas las demás opciones pueden permanecer desactivadas.

2. Asegúrese de que todos los hosts tengan acceso a los repositorios de paquetes de Ubuntu o Debian.
3. Si el intercambio está habilitado:
 - a. Ejecute el siguiente comando: `$ sudo swapoff --all`
 - b. Eliminar todas las entradas de intercambio de `/etc/fstab` para conservar la configuración.



No deshabilitar el intercambio por completo puede reducir gravemente el rendimiento.

Comprender la instalación del perfil de AppArmor

Si está operando en un entorno Ubuntu autoimplementado y utiliza el sistema de control de acceso obligatorio AppArmor, los perfiles de AppArmor asociados con los paquetes que instale en el sistema base podrían ser bloqueados por los paquetes correspondientes instalados con StorageGRID.

De forma predeterminada, los perfiles de AppArmor se instalan para los paquetes que instala en el sistema operativo base. Cuando ejecuta estos paquetes desde el contenedor del sistema StorageGRID , los perfiles de AppArmor se bloquean. Los paquetes base DHCP, MySQL, NTP y tcdump entran en conflicto con AppArmor, y otros paquetes base también podrían entrar en conflicto.

Tiene dos opciones para gestionar los perfiles de AppArmor:

- Deshabilite los perfiles individuales para los paquetes instalados en el sistema base que se superponen con los paquetes en el contenedor del sistema StorageGRID . Cuando deshabilita perfiles individuales, aparece una entrada en los archivos de registro de StorageGRID que indica que AppArmor está habilitado.

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
```

- Desactivar AppArmor por completo. Para Ubuntu 9.10 o posterior, siga las instrucciones de la comunidad en línea de Ubuntu: "[Desactivar AppArmor](#)". Es posible que no sea posible deshabilitar AppArmor por completo en versiones más nuevas de Ubuntu.

Después de deshabilitar AppArmor, no aparecerán entradas que indiquen que AppArmor está habilitado en los archivos de registro de StorageGRID .

Configurar la red del host (Ubuntu o Debian)

Después de completar la instalación de Linux en sus hosts, es posible que necesite realizar alguna configuración adicional para preparar un conjunto de interfaces de red en cada host que sean adecuadas para mapearlas en los nodos StorageGRID que implementará más adelante.

Antes de empezar

- Usted ha revisado el "[Pautas de red de StorageGRID](#)".
- Ha revisado la información sobre "[Requisitos de migración del contenedor de nodos](#)".
- Si está utilizando hosts virtuales, ha leído el [Consideraciones y recomendaciones para la clonación de direcciones MAC](#) antes de configurar la red del host.



Si está utilizando máquinas 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 implementados en ciertas distribuciones de Linux.

Acerca de esta tarea

Los nodos de la red deben poder acceder a la red de la red y, opcionalmente, a las redes de administración y

de cliente. Puede proporcionar este acceso mediante la creación de asignaciones que asocian la interfaz física del host con las interfaces virtuales de cada nodo de la red. Al crear interfaces de host, utilice nombres descriptivos para facilitar la implementación en todos los hosts y permitir la migración.

La misma interfaz se puede compartir entre el host y uno o más nodos. Por ejemplo, puede utilizar la misma interfaz para el acceso al host y el acceso a la red de administración del nodo, para facilitar el mantenimiento del host y del nodo. Aunque se puede compartir la misma interfaz entre el host y los nodos individuales, todos deben tener direcciones IP diferentes. Las direcciones IP no se pueden compartir entre 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 en el host; puede utilizar una interfaz de red de host diferente para cada nodo; o puede hacer algo intermedio. Sin embargo, normalmente no proporcionaría la misma interfaz de red de host como interfaz de red de administración y de cuadrícula para un solo nodo, o como interfaz de red de cuadrícula para un nodo y como interfaz de red de cliente para otro.

Puedes completar esta tarea de muchas maneras. Por ejemplo, si sus hosts son máquinas virtuales y está implementando uno o dos nodos StorageGRID para cada host, puede crear la cantidad correcta de interfaces de red en el hipervisor y usar una asignación de 1 a 1. Si está implementando varios nodos en hosts físicos para uso de producción, puede aprovechar el soporte de la pila de red Linux para VLAN y LACP para tolerancia a fallas y uso compartido de ancho de banda. Las siguientes secciones proporcionan enfoques detallados para ambos ejemplos. No es necesario utilizar ninguno de estos ejemplos; puede utilizar cualquier enfoque que se ajuste a sus necesidades.



No utilice dispositivos de enlace o puente directamente como interfaz de red del contenedor. Al hacerlo se podría evitar el inicio del nodo causado por un problema del 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 enlace, como una VLAN o un par 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

[[clonación de direcciones MAC en Ubuntu]]

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

Habilitar la clonación de MAC

En ciertos entornos, la seguridad se puede mejorar mediante la clonación de direcciones MAC porque permite utilizar una NIC virtual dedicada para la red de administración, la red de cuadrícula y la red de cliente. Hacer que el contenedor utilice la dirección MAC de la NIC dedicada en el host le permite evitar el uso de configuraciones de red en modo promiscuo.



La clonación de direcciones MAC está diseñada para usarse con instalaciones de servidores virtuales y es posible que no funcione correctamente con todas las configuraciones de dispositivos físicos.



Si un nodo no puede iniciarse debido a que una interfaz de clonación MAC está ocupada, es posible que deba configurar el enlace como "inactivo" antes de iniciar el nodo. Además, es posible que el entorno virtual impida la clonación de MAC en una interfaz de red mientras el enlace está activo. Si un nodo no logra configurar la dirección MAC y no se inicia debido a que una interfaz está ocupada, configurar el enlace como "inactivo" antes de iniciar el nodo podría solucionar el problema.

La clonación de direcciones MAC está deshabilitada de forma predeterminada y debe configurarse mediante claves de configuración del nodo. Debes habilitarlo cuando instales 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

Establecer la clave en "verdadero" hace que el contenedor utilice 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 configurado una utilizando el `_NETWORK_MAC` clave de configuración del nodo, se utiliza esa dirección en su lugar. El host y el contenedor siempre tendrán direcciones MAC diferentes.



Habilitar la clonación de MAC en un host virtual sin habilitar también el modo promiscuo en el hipervisor podría provocar que la red del host Linux que utiliza la interfaz del host deje de funcionar.

Casos de uso de clonación de MAC

Hay dos casos de uso a considerar con la clonación de MAC:

- Clonación de MAC no habilitada: cuando el `_CLONE_MAC` Si la clave en el archivo de configuración del nodo no está configurada o está configurada como "falsa", el host usará la MAC de la NIC del host y el contenedor tendrá una MAC generada por StorageGRID a menos que se especifique una MAC en el archivo. `_NETWORK_MAC` llave. Si se establece una dirección en el `_NETWORK_MAC` clave, el contenedor tendrá la dirección especificada en la `_NETWORK_MAC` llave. Esta configuración de claves requiere el uso del modo promiscuo.
- Clonación de MAC habilitada: cuando el `_CLONE_MAC` Si la clave en el archivo de configuración del nodo está establecida en "verdadero", el contenedor utiliza la MAC de la NIC del host y el host utiliza una MAC generada por StorageGRID a menos que se especifique una MAC en el archivo. `_NETWORK_MAC` llave. Si se establece una dirección en el `_NETWORK_MAC` clave, el host utiliza la dirección especificada en lugar de una generada. En esta configuración de claves, no se debe utilizar el modo promiscuo.



Si no desea utilizar la clonación de direcciones MAC y prefiere permitir que todas las interfaces reciban y transmitan datos para direcciones MAC distintas de las asignadas por el hipervisor, asegúrese de que las propiedades de seguridad en los niveles de conmutador virtual y grupo de puertos estén configuradas en **Aceptar** para Modo promiscuo, Cambios de dirección MAC y Transmisiones falsificadas. Los valores establecidos en el conmutador virtual pueden ser anulados por los valores a nivel del grupo de puertos, así que asegúrese de que las configuraciones sean las mismas en ambos lugares.

Para habilitar la clonación de MAC, consulte la ["Instrucciones para crear archivos de configuración de nodos"](#).

Ejemplo de clonación de MAC

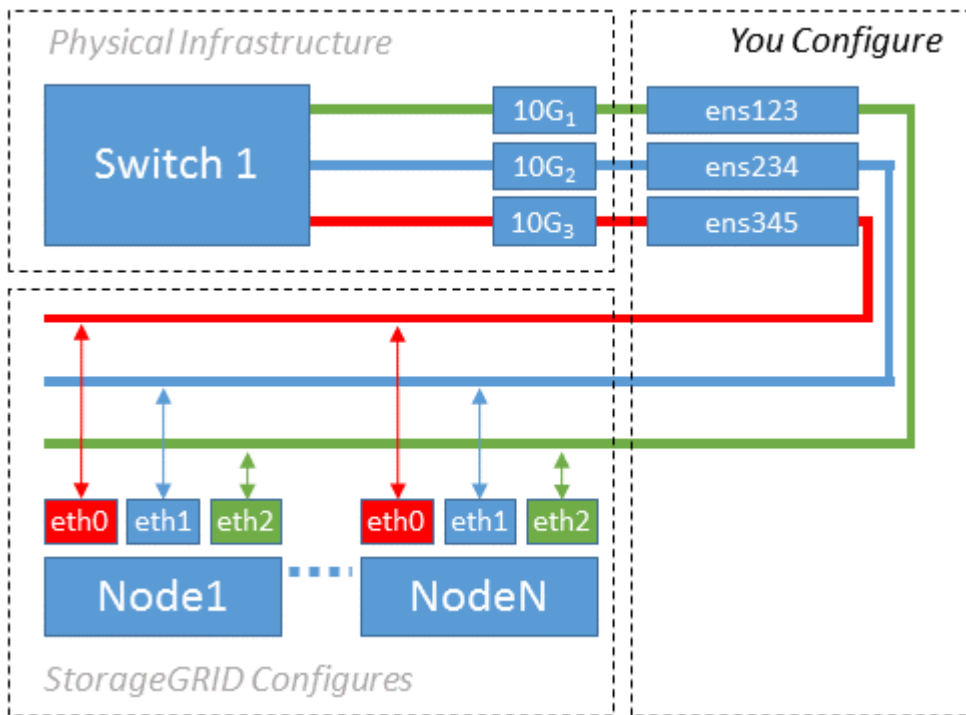
Ejemplo de clonación de MAC habilitada con un host que tiene la dirección MAC 11:22:33:44:55:66 para la interfaz ens256 y las siguientes claves en el archivo de configuración del nodo:

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

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

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

El ejemplo 1 describe un mapeo de interfaz física simple que requiere poca o ninguna configuración del lado del host.



El sistema operativo Linux crea las interfaces ensXYZ automáticamente durante la instalación o el arranque, o cuando las interfaces se agregan en caliente. No se requiere configuración más allá de asegurarse de que las interfaces estén configuradas para activarse automáticamente después del arranque. Debe determinar qué ensXYZ corresponde a qué red StorageGRID (Grid, Admin o Client) para poder proporcionar las asignaciones correctas más adelante en el proceso de configuración.

Tenga en cuenta que la figura muestra varios nodos StorageGRID ; sin embargo, normalmente utilizaría 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 10G₁ a 10G₃ para el modo de acceso y colocarlos en las VLAN apropiadas.

Ejemplo 2: VLAN que transportan enlaces LACP

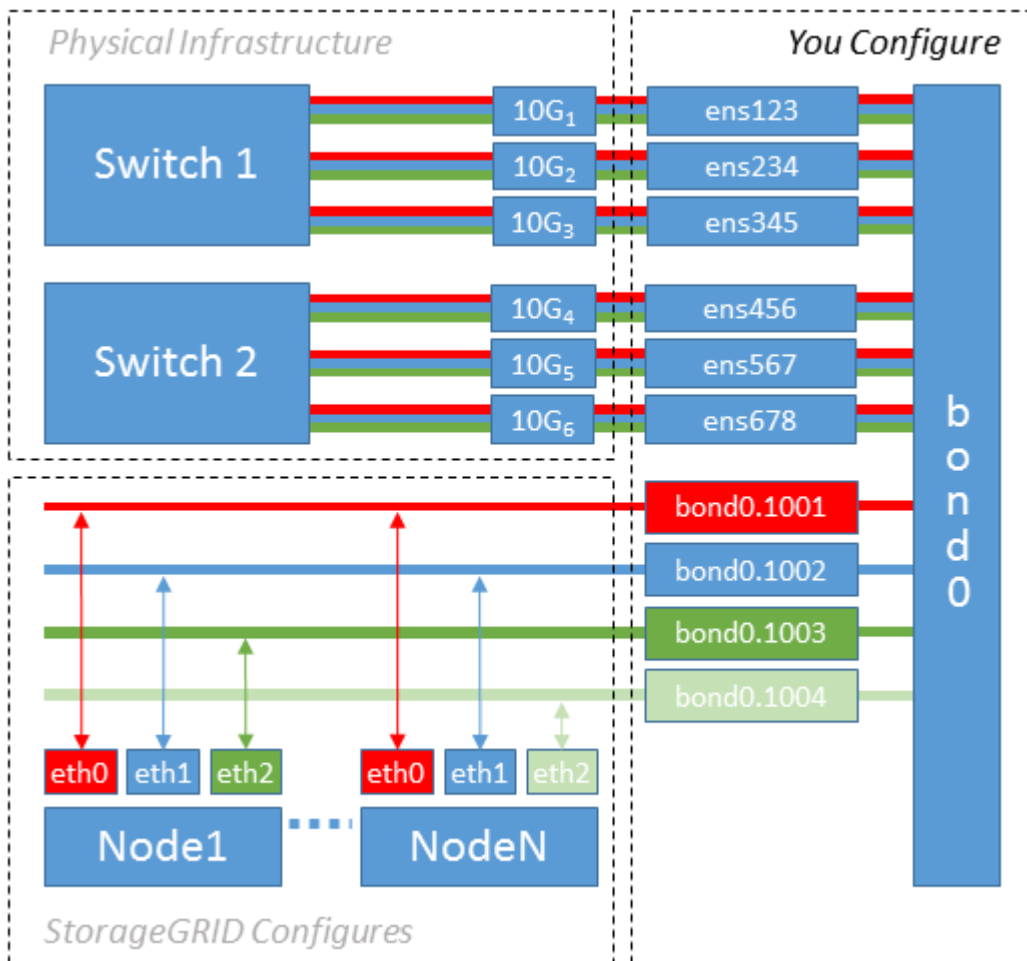
El ejemplo 2 supone que está familiarizado con la vinculación de interfaces de red y con la creación de interfaces VLAN en la distribución de Linux que está utilizando.

Acerca de esta tarea

El ejemplo 2 describe un esquema genérico, flexible y basado en VLAN que facilita compartir todo el ancho de banda de red disponible entre todos los nodos de un solo host. Este ejemplo es particularmente aplicable a hosts de hardware real.

Para entender este ejemplo, supongamos que tiene tres subredes separadas para las redes de red, administración y cliente en cada centro de datos. Las subredes están en VLAN separadas (1001, 1002 y 1003) y se presentan al host en un puerto troncal vinculado a LACP (bond0). Configuraría tres interfaces VLAN en el enlace: bond0.1001, bond0.1002 y bond0.1003.

Si necesita VLAN y subredes independientes para redes de nodos en el mismo host, puede agregar interfaces VLAN en el enlace y asignarlas al host (que se muestra como bond0.1004 en la ilustración).



Pasos

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

Utilice el mismo nombre para el enlace en cada host, por ejemplo, bond0.

2. Cree interfaces VLAN que utilicen este enlace como su "dispositivo físico" asociado, utilizando la

convención de nombres de interfaz VLAN estándar `physdev-name.VLAN ID`.

Tenga en cuenta que los pasos 1 y 2 requieren una configuración adecuada en los conmutadores de borde que terminan los otros extremos de los enlaces de red. Los puertos del conmutador de borde también deben agregarse en un canal de puerto LACP, configurarse como un enlace troncal y permitir que pasen todas las VLAN requeridas.

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

Información relacionada

["Ejemplo /etc/network/interfaces"](#)

Configurar el almacenamiento del host

Debe asignar volúmenes de almacenamiento en bloque a cada host.

Antes de empezar

Ha revisado los siguientes temas, que proporcionan la información que necesita para realizar esta tarea:

- ["Requisitos de almacenamiento y rendimiento"](#)
- ["Requisitos de migración del contenedor de nodos"](#)

Acerca de esta tarea

Al asignar volúmenes de almacenamiento en bloque (LUN) a los hosts, utilice las tablas en "Requisitos de almacenamiento" para determinar lo siguiente:

- Número de volúmenes necesarios para cada host (según la cantidad y los tipos de nodos que se implementarán en ese host)
- Categoría de almacenamiento para cada volumen (es decir, datos del sistema o datos de objeto)
- 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 necesita particionar, formatear ni montar ninguno de estos volúmenes; solo necesita asegurarse de que sean visibles para los hosts.



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

Evite utilizar archivos de dispositivos especiales "sin procesar" (`/dev/sdb`, por ejemplo) mientras compone su lista de nombres de volúmenes. Estos archivos pueden cambiar durante los reinicios del host, lo que afectará el funcionamiento correcto del sistema. Si está utilizando LUN iSCSI y rutas múltiples de Device Mapper, considere usar alias de rutas múltiples en el `/dev/mapper` directorio, especialmente si su topología SAN incluye rutas de red redundantes al almacenamiento compartido. Alternativamente, puede utilizar los enlaces creados por el sistema en `/dev/disk/by-path/` para los nombres de sus 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 variarán para cada instalación.

Asigne nombres descriptivos a cada uno de estos volúmenes de almacenamiento en bloque para simplificar la instalación inicial de StorageGRID y los procedimientos de mantenimiento futuros. Si está utilizando el controlador de múltiples rutas del asignador de dispositivos para el acceso redundante a volúmenes de almacenamiento compartido, puede utilizar el `alias` campo en tu `/etc/multipath.conf` archivo.

Por ejemplo:

```

multipaths {
    multipath {
        wwid 3600a09800059d6df00005df2573c2c30
        alias docker-storage-volume-hostA
    }
    multipath {
        wwid 3600a09800059d6df00005df3573c2c30
        alias sgws-adml-var-local
    }
    multipath {
        wwid 3600a09800059d6df00005df4573c2c30
        alias sgws-adml-audit-logs
    }
    multipath {
        wwid 3600a09800059d6df00005df5573c2c30
        alias sgws-adml-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
    }
    ...
}

```

El uso del campo de alias de esta manera hace que los alias aparezcan como dispositivos de bloque en el `/dev/mapper` directorio en el host, lo que le permite especificar un nombre amigable y fácilmente validado siempre que una operación de configuración o mantenimiento requiera especificar un volumen de almacenamiento en bloque.

Si está configurando un almacenamiento compartido para admitir la migración de nodos StorageGRID y utiliza Device Mapper Multipathing, puede crear e instalar un dispositivo común `/etc/multipath.conf` en todos los hosts ubicados conjuntamente. Solo asegúrese de utilizar un volumen de almacenamiento Docker diferente en cada host. El uso de alias e incluir el nombre de host de destino en el alias para cada LUN de volumen de almacenamiento de Docker hará que esto sea fácil de recordar y es lo recomendado.



La compatibilidad con Docker como motor de contenedores para implementaciones de solo software está obsoleta. Docker será reemplazado por otro motor de contenedores en una versión futura.

Información relacionada

- ["Requisitos de almacenamiento y rendimiento"](#)
- ["Requisitos de migración del contenedor de nodos"](#)

Configurar el volumen de almacenamiento del motor de contenedores

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



La compatibilidad con Docker como motor de contenedores para implementaciones de solo software está obsoleta. Docker será reemplazado por otro motor de contenedores en una versión futura.

Acerca de esta tarea

Puede omitir estos pasos si planea usar almacenamiento local para el volumen de almacenamiento de Docker y tiene suficiente espacio disponible en la partición del 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. Agregue una entrada para `docker-storage-volume-device` a `/etc/fstab`.

Este paso garantiza que el volumen de almacenamiento se volverá a montar automáticamente después de que el host se reinicie.

Instalar Docker

El sistema StorageGRID se ejecuta en Linux como una colección de contenedores Docker. Antes de poder instalar StorageGRID, debe instalar Docker.



La compatibilidad con Docker como motor de contenedores para implementaciones de solo software está obsoleta. Docker será reemplazado por otro motor de contenedores en una versión futura.

Pasos

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



Si Docker no está incluido en tu distribución de Linux, puedes descargarlo del sitio web de Docker.

2. Asegúrese de que Docker se haya habilitado e iniciado ejecutando los siguientes dos comandos:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Confirme que ha instalado la versión esperada de Docker ingresando lo siguiente:

```
sudo docker version
```

Las versiones de Cliente y Servidor deben ser 1.11.0 o posteriores.

Información relacionada

["Configurar el almacenamiento del host"](#)

Instalar servicios de host de StorageGRID

Utilice el paquete DEB de StorageGRID para instalar los servicios de host de StorageGRID .

Acerca de esta tarea

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

Pasos

1. Copie los paquetes DEB de StorageGRID en cada uno de sus hosts o póngalos a disposición en el almacenamiento compartido.

Por ejemplo, colóquelos en el /tmp directorio, por lo que puede utilizar el comando de ejemplo en el siguiente paso.

2. Inicie sesión en cada host como root o usando una cuenta con permiso sudo y ejecute los siguientes comandos.

Debes instalar el `images` paquete primero, y el `service` paquete segundo. Si colocó los paquetes en un directorio distinto de /tmp , modifique el comando para reflejar la ruta que utilizó.

```
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 que se puedan instalar los paquetes StorageGRID. El `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` El comando fallará hasta que lo hayas hecho.

Automatizar la instalación (Ubuntu o Debian)

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

Acerca de esta tarea

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

- Ya utiliza un marco de orquestación estándar, como Ansible, Puppet o Chef, para implementar y configurar hosts físicos o virtuales.
- Desea implementar varias instancias de StorageGRID.
- Está implementando una instancia de StorageGRID grande y compleja.

El servicio de host StorageGRID se instala mediante un paquete y se controla mediante archivos de configuración que se pueden crear de forma interactiva durante una instalación manual o prepararse con anticipación (o mediante programación) para permitir la instalación automatizada mediante marcos de orquestación estándar. StorageGRID proporciona scripts de Python opcionales para automatizar la configuración de los dispositivos StorageGRID y de todo el sistema StorageGRID (la "red"). Puede usar estos scripts directamente o puede inspeccionarlos para aprender a usar la API REST de instalación de StorageGRID en las herramientas de configuración e implementación de la red que desarrolle usted mismo.

Automatice la instalación y configuración del servicio de host StorageGRID

Puede automatizar la instalación del servicio de host StorageGRID utilizando 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 pueden prepararse con anticipación (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 playbooks o recetas debería ser sencillo.

Puedes automatizar estas tareas:

1. Instalación de Linux
2. Configuración de Linux
3. Configuración de interfaces de red del host para cumplir con los requisitos de StorageGRID
4. Configuración del almacenamiento del host para cumplir con los requisitos de StorageGRID
5. Instalación de Docker
6. Instalación del servicio de host StorageGRID
7. Creación de archivos de configuración de nodos StorageGRID en `/etc/storagegrid/nodes`
8. Validación de archivos de configuración de nodos de StorageGRID
9. Iniciar el servicio de host StorageGRID

Ejemplo de rol y manual de estrategias de Ansible

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

Automatizar la configuración de StorageGRID

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

Antes de empezar

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

Nombre del archivo	Descripción
<code>configurar-storagegrid.py</code>	Script de Python utilizado para automatizar la configuración
<code>configure-storagegrid.sample.json</code>	Archivo de configuración de ejemplo para usar con el script
<code>configurar-storagegrid.blank.json</code>	Archivo de configuración en blanco para usar con el script

- Has 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

Puedes utilizar el `configure-storagegrid.py` Script de Python y el `configure-storagegrid.json` archivo de configuración para automatizar la configuración de su sistema StorageGRID .



También puede configurar el sistema utilizando el Administrador de Grid o la API de instalación.

Pasos

1. Inicie sesión en la máquina Linux que está utilizando para ejecutar el script de Python.
2. Cambie al directorio donde extrajo el archivo de instalación.

Por ejemplo:

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

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

3. Ejecute el script de 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 donde se está ejecutando el proceso de instalación y configuración. Debe realizar una copia de seguridad del archivo del paquete de recuperación para poder recuperar el sistema StorageGRID si uno o más nodos de la red fallan. Por ejemplo, cópielo en una ubicación de red segura y respaldada y en una ubicación de almacenamiento en la nube segura.



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

Si especificó que se deben generar contraseñas aleatorias, abra el `Passwords.txt` archivo y busque las contraseñas necesarias para acceder a su 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.      #####
#####
```

Su sistema StorageGRID está instalado y configurado cuando se muestra un mensaje de confirmación.

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

Información relacionada

["Instalación API REST"](#)

Implementar nodos de red virtuales (Ubuntu o Debian)

Crear archivos de configuración de nodo para implementaciones de Ubuntu o Debian

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

Ubicación de los archivos de configuración del nodo

Coloque 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 utilizando un editor de texto, como vim o nano, o puede crearlos en otro lugar y moverlos a cada host.

Nomenclatura de los archivos de configuración de nodos

Los nombres de los archivos de configuración son significativos. El formato es `node-name.conf`, donde `node-name` Es un nombre que le asignas 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 con 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 más guiones (-)
- No debe tener más de 32 caracteres, sin incluir el `.conf` extensión

Cualquier archivo en `/etc/storagegrid/nodes` que no sigan estas convenciones de nomenclatura no serán analizados por el servicio host.

Si tiene una topología de múltiples sitios planificada para su red, un esquema de nombres de nodos típico podría ser:

`site-nodetype-nodenum.conf`

Por ejemplo, podrías utilizar `dc1-adm1.conf` para el primer nodo de administración en el centro de datos 1, y `dc2-sn3.conf` para el tercer nodo de almacenamiento en el centro de datos 2. Sin embargo, puedes utilizar cualquier esquema que desees, siempre que todos los nombres de nodos sigan las reglas de nomenclatura.

Contenido de un archivo de configuración de nodo

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

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

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

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

Claves de red de administración

IP DE ADMINISTRADOR

Valor	Designación
Dirección IPv4 de la red de cuadrícula del nodo de administración principal de la cuadrícula a la que pertenece este nodo. Utilice el mismo valor que especificó para GRID_NETWORK_IP para el nodo de la red con NODE_TYPE = VM_Admin_Node y ADMIN_ROLE = Primary. Si omite este parámetro, el nodo intentará descubrir un nodo de administración principal mediante mDNS. "Cómo los nodos de la red descubren el nodo de administración principal" Nota: Este valor se ignora y puede estar prohibido en el nodo de administración principal.	Mejores prácticas

CONFIGURACIÓN DE RED DE ADMINISTRACIÓN

Valor	Designación
DHCP, ESTÁTICO o DESHABILITADO	Opcional

ADMINISTRACIÓN_RED_ESL

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

PUERTA DE ENLACE DE RED DE ADMINISTRACIÓN

Valor	Designación
Dirección IPv4 de la puerta de enlace de la red de administración local para este nodo. Debe estar en la subred definida por ADMIN_NETWORK_IP y ADMIN_NETWORK_MASK. Este valor se ignora para las redes configuradas por DHCP. Ejemplos: 1.1.1.1 10.224.4.81	Requerido si ADMIN_NETWORK_ESL se especifica Opcional en caso contrario.

IP DE RED DE ADMINISTRACIÓN

Valor	Designación
Dirección IPv4 de este nodo en la red de administración. 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	Obligatorio cuando ADMIN_NETWORK_CONFIG = STATIC. Opcional en caso contrario.

ADMIN_RED_MAC

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

MÁSCARA DE RED DE ADMINISTRACIÓN

Valor	Designación
Máscara de red IPv4 para este nodo, en la red de administración. Especifique esta clave cuando ADMIN_NETWORK_CONFIG = STATIC; no la especifique para otros valores. Ejemplos: 255.255.255.0 255.255.248.0	Obligatorio si se especifica ADMIN_NETWORK_IP y ADMIN_NETWORK_CONFIG = STATIC. Opcional en caso contrario.

MTU DE LA RED DE ADMINISTRACIÓN

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

OBJETIVO DE LA RED DE ADMINISTRACIÓN

Valor	Designación
Nombre del dispositivo host que utilizará para el acceso a la red de administración por parte del nodo StorageGRID . Sólo 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 la 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 incluso si este nodo inicialmente no tendrá una dirección IP de red de administración. Luego, puede agregar una dirección IP de red de administración más tarde, sin tener que reconfigurar el nodo en el host. Ejemplos: bond0.1002 ens256	Mejores prácticas

TIPO DE OBJETIVO DE RED DE ADMINISTRACIÓN

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

INTERFAZ DE TIPO DE DESTINO DE RED DE ADMINISTRACIÓN CLONAR MAC

Valor	Designación
Verdadero o falso Establezca la clave en "verdadero" para que el contenedor StorageGRID utilice 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 detalles sobre la clonación de MAC: • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Red Hat Enterprise Linux)" • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)"	Mejores prácticas

ROL DE ADMINISTRADOR

Valor	Designación
Primario o no primario Esta clave solo es necesaria cuando NODE_TYPE = VM_Admin_Node; no la especifique para otros tipos de nodos.	Obligatorio cuando NODE_TYPE = VM_Admin_Node Opcional en caso contrario.

Bloquear teclas del dispositivo

BLOQUEAR REGISTROS DE AUDITORÍA DEL DISPOSITIVO

Valor	Designación
Ruta y nombre del archivo especial del dispositivo de bloque que este nodo utilizará para el almacenamiento persistente de registros de auditoría. Ejemplos: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adml-audit-logs</pre>	Obligatorio para nodos con NODE_TYPE = VM_Admin_Node. No lo especifique para otros tipos de nodos.

DISPOSITIVO DE BLOQUE RANGEDB_nnn

Valor	Designación
Ruta y nombre del archivo especial del dispositivo de bloque que este nodo utilizará para el almacenamiento de objetos persistentes. Esta clave solo es necesaria para los nodos con <code>NODE_TYPE = VM_Storage_Node</code>; no la especifique para otros tipos de nodos. Solo se requiere <code>BLOCK_DEVICE_RANGEDB_000</code>; el resto es opcional. El dispositivo de bloque especificado para <code>BLOCK_DEVICE_RANGEDB_000</code> debe ser de al menos 4 TB; los demás pueden ser más pequeños. No dejes espacios vacíos. Si especifica <code>BLOCK_DEVICE_RANGEDB_005</code>, también debe especificar <code>BLOCK_DEVICE_RANGEDB_004</code>. Nota: Para compatibilidad con implementaciones existentes, se admiten claves de dos dígitos para los nodos actualizados. Ejemplos: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-sn1-rangedb-000</pre>	Requerido: <code>BLOCK_DEVICE_RANGEDB_000</code> Opcional: <code>BLOCK_DEVICE_RANGEDB_001</code> <code>BLOCK_DEVICE_RANGEDB_002</code> <code>BLOCK_DEVICE_RANGEDB_003</code> <code>BLOCK_DEVICE_RANGEDB_004</code> <code>BLOCK_DEVICE_RANGEDB_005</code> <code>BLOCK_DEVICE_RANGEDB_006</code> <code>BLOCK_DEVICE_RANGEDB_007</code> <code>BLOCK_DEVICE_RANGEDB_008</code> <code>BLOCK_DEVICE_RANGEDB_009</code> <code>BLOCK_DEVICE_RANGEDB_010</code> <code>BLOCK_DEVICE_RANGEDB_011</code> <code>BLOCK_DEVICE_RANGEDB_012</code> <code>BLOCK_DEVICE_RANGEDB_013</code> <code>BLOCK_DEVICE_RANGEDB_014</code> <code>BLOCK_DEVICE_RANGEDB_015</code>

TABLAS DE DISPOSITIVOS DE BLOQUE

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

BLOQUE_DISPOSITIVO_VAR_LOCAL

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

Claves de red del cliente

CONFIGURACIÓN DE RED DEL CLIENTE

Valor	Designación
DHCP, ESTÁTICO o DESHABILITADO	Opcional

PUERTA DE ENLACE DE LA RED DEL CLIENTE

Valor	Designación

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

IP DE LA RED DEL CLIENTE

Valor	Designación
Dirección IPv4 de este nodo en la red del 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	Obligatorio cuando CLIENT_NETWORK_CONFIG = STATIC Opcional en caso contrario.

MAC DE LA RED DEL CLIENTE

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

MÁSCARA DE RED DEL CLIENTE

Valor	Designación
Máscara de red IPv4 para este nodo en la red del cliente. Especifique esta clave cuando CLIENT_NETWORK_CONFIG = STATIC; no la especifique para otros valores. Ejemplos: 255.255.255.0 255.255.248.0	Obligatorio si se especifica CLIENT_NETWORK_IP y CLIENT_NETWORK_CONFIG = STATIC Opcional en caso contrario.

MTU DE LA RED DEL CLIENTE

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

OBJETIVO DE LA RED DEL CLIENTE

Valor	Designación
Nombre del dispositivo host que utilizará para el acceso a la red del cliente por parte del nodo StorageGRID . Sólo 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 la 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 incluso si este nodo inicialmente no tendrá una dirección IP de red de cliente. Luego, puede agregar una dirección IP de red de cliente más tarde, sin tener que reconfigurar el nodo en el host. Ejemplos: <pre>bond0.1003</pre> <pre>ens423</pre>	Mejores prácticas

TIPO DE OBJETIVO DE LA RED DEL CLIENTE

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

CLIENTE_RED_TIPO_DESTINATO_INTERFAZ_CLONAR_MAC

Valor	Designación
Verdadero o falso Establezca la clave en "verdadero" para que el contenedor StorageGRID utilice la dirección MAC de la interfaz de destino del host en la red del 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 detalles sobre la clonación de MAC: • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Red Hat Enterprise Linux)" • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)"	Mejores prácticas

Claves de red de cuadrícula

CONFIGURACIÓN DE RED DE CUADRÍCULA

Valor	Designación
ESTÁTICO o DHCP El valor predeterminado es ESTÁTICO si no se especifica.	Mejores prácticas

PUERTA DE ENLACE DE RED DE CUADRÍCULA

Valor	Designación
Dirección IPv4 de la puerta de enlace de la red local para este nodo, que debe estar en la subred definida por GRID_NETWORK_IP y GRID_NETWORK_MASK. Este valor se ignora para las redes configuradas por DHCP. Si la red Grid es una subred única sin puerta de enlace, utilice la dirección de puerta de enlace estándar para la subred (XYZ1) o el valor GRID_NETWORK_IP de este nodo; cualquiera de los valores simplificará posibles expansiones futuras de la red Grid.	Requerido

IP DE RED DE CUADRÍCULA

Valor	Designación
Dirección IPv4 de este nodo en la red Grid. 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	Obligatorio cuando GRID_NETWORK_CONFIG = STATIC Opcional en caso contrario.

RED_DE_CUADRÍCULA_MAC

Valor	Designación
La dirección MAC de la interfaz de red Grid en el contenedor. Deben ser 6 pares de dígitos hexadecimales separados por dos puntos. Ejemplo: b2:9c:02:c2:27:30	Opcional Si se omite, se generará automáticamente una dirección MAC.

MÁSCARA DE RED DE CUADRÍCULA

Valor	Designación
Máscara de red IPv4 para este nodo en la red Grid. Especifique esta clave cuando GRID_NETWORK_CONFIG = STATIC; no la especifique para otros valores. Ejemplos: 255.255.255.0 255.255.248.0	Obligatorio cuando se especifica GRID_NETWORK_IP y GRID_NETWORK_CONFIG = STATIC. Opcional en caso contrario.

MTU DE LA RED DE CUADRÍCULA

Valor	Designación
La unidad de transmisión máxima (MTU) para este nodo en la red eléctrica. No especifique si GRID_NETWORK_CONFIG = DHCP. Si se especifica, el valor debe estar entre 1280 y 9216. Si se omite, se utiliza 1500. Si desea utilizar tramas jumbo, configure la MTU en un valor adecuado para tramas jumbo, como 9000. De lo contrario, mantenga el valor predeterminado. IMPORTANTE: El valor de MTU de la red debe coincidir con el valor configurado en el puerto del conmutador al que está conectado el nodo. De lo contrario, podrían ocurrir problemas de rendimiento de la red o pérdida de paquetes. IMPORTANTE: Para obtener el mejor rendimiento de la red, todos los nodos deben configurarse con valores de MTU similares en sus interfaces de red Grid. La alerta No coincide la MTU de la red de cuadrícula se activa si hay una diferencia significativa en las configuraciones de MTU para la red de cuadrícula en nodos individuales. Los valores de MTU no tienen que ser los mismos para todos los tipos de red. Ejemplos: 1500 8192	Opcional

OBJETIVO DE LA RED DE CUADRÍCULA

Valor	Designación
Nombre del dispositivo host que utilizará para el acceso a la red Grid mediante el nodo StorageGRID . Sólo 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 la 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	Requerido

TIPO DE OBJETIVO DE RED DE CUADRÍCULA

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

INTERFAZ DE TIPO DE OBJETIVO DE RED DE CUADRÍCULA CLONAR MAC

Valor	Designación
Verdadero o falso Establezca el valor de la clave en "verdadero" para que el contenedor StorageGRID utilice la dirección MAC de la interfaz de destino del host en la red Grid. 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 detalles sobre la clonación de MAC: • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Red Hat Enterprise Linux)" • "Consideraciones y recomendaciones para la clonación de direcciones MAC (Ubuntu o Debian)"	Mejores prácticas

Clave de contraseña de instalación (temporal)

HASH DE CONTRASEÑA TEMPORAL PERSONALIZADO

Valor	Designación
Para el nodo de administración principal, configure una contraseña temporal predeterminada para la API de instalación de StorageGRID durante la instalación. Nota: Establezca una contraseña de instalación solo en el nodo de administración principal. Si intenta establecer una contraseña en otro tipo de nodo, la validación del archivo de configuración del nodo fallará. Establecer este valor no tiene ningún efecto una vez finalizada la instalación. Si se omite esta clave, de forma predeterminada no se establece ninguna contraseña temporal. Alternativamente, puede establecer una contraseña temporal utilizando la API de instalación de StorageGRID . Debe ser un <code>crypt()</code> Hash de contraseña SHA-512 con formato <code>\$6\$<salt>\$<password hash></code> para una contraseña de al menos 8 y no más de 32 caracteres. Este hash se puede generar utilizando herramientas CLI, como la <code>openssl passwd</code> comando en modo SHA-512.	Mejores prácticas

Interfaces clave

INTERFAZ_OBJETIVO_nnnn

Valor	Designación
Nombre y descripción opcional de una interfaz adicional que desea agregar a este nodo. Puede agregar varias interfaces adicionales a cada nodo. Para <i>nnnn</i>, especifique un número único para cada entrada <code>INTERFACE_TARGET</code> que esté agregando. Para el valor, especifique el nombre de la interfaz física en el host físico. Luego, opcionalmente, agregue una coma y proporcione una descripción de la interfaz, que se muestra en la página de interfaces de VLAN y en la página de grupos de HA. Ejemplo: <code>INTERFACE_TARGET_0001=ens256, Trunk</code> Si agrega 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 HA; no necesita configurar una interfaz VLAN.	Opcional

Clave de RAM máxima

RAM MÁXIMA

Valor	Designación
La cantidad máxima de RAM que este nodo puede consumir. Si se omite esta clave, el nodo no tiene restricciones de memoria. Al configurar este campo para un nodo de nivel de producción, especifique un valor que sea al menos 24 GB y entre 16 y 32 GB menos que la RAM total del sistema. Nota: El valor de RAM afecta el espacio reservado de metadatos real de un nodo. Ver el "Descripción de qué es el Espacio Reservado de Metadatos" . El formato para este campo es <i>numberunit</i> , dónde <i>unit</i> puede ser b , k , m , o g . Ejemplos: 24g 38654705664b Nota: Si desea utilizar esta opción, debe habilitar el soporte del kernel para cgroups de memoria.	Opcional

Claves de tipo de nodo

TIPO DE NODO

Valor	Designación
Tipo de nodo: • Nodo de administración de máquina virtual • Nodo de almacenamiento de máquina virtual • Nodo de archivo de máquina virtual • Puerta de enlace de API de máquina virtual	Requerido

TIPO DE ALMACENAMIENTO

Valor	Designación
Define el tipo de objetos que contiene un nodo de almacenamiento. Para obtener más información, consulte "Tipos de nodos de almacenamiento". Esta clave solo es necesaria para los nodos con <code>NODE_TYPE = VM_Storage_Node</code>; no la especifique para otros tipos de nodos. Tipos de almacenamiento: • conjunto • data • metadatos Nota: Si no se especifica <code>STORAGE_TYPE</code>, el tipo de nodo de almacenamiento se establece como combinado (datos y metadatos) de manera predeterminada.	Opcional

Claves de reasignación de puertos

PUERTO_REMAP

Valor	Designación
Reasigna cualquier puerto utilizado por un nodo para comunicaciones internas del nodo de la red o comunicaciones externas. La reasignación de puertos es necesaria si las políticas de red empresarial restringen uno o más puertos utilizados por StorageGRID, como se describe en "Comunicaciones internas de los nodos de la red" o "Comunicaciones externas". IMPORTANTE: No reasigne los puertos que planea usar para configurar los puntos finales del balanceador de carga. Nota: Si solo se configura <code>PORT_REMAP</code>, la asignación que especifique se utiliza tanto para las comunicaciones entrantes como para las salientes. Si también se especifica <code>PORT_REMAP_INBOUND</code>, <code>PORT_REMAP</code> se aplica solo a las comunicaciones salientes. El formato utilizado es: <i>network type/protocol/default port used by grid node/new port</i>, donde <i>network type</i> es <code>grid</code>, <code>admin</code> o <code>cliente</code>, y <i>protocol</i> es <code>tcp</code> o <code>udp</code>. Ejemplo: <code>PORT_REMAP = client/tcp/18082/443</code> También puedes reasignar varios puertos usando una lista separada por comas. Ejemplo: <code>PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80</code>	Opcional

PUERTO_REMAP_ENTRADA

Valor	Designación
Reasigna las comunicaciones entrantes al puerto especificado. Si especifica PORT_REMAP_INBOUND pero no especifica un valor para PORT_REMAP, las comunicaciones salientes para el puerto no cambian. IMPORTANTE: No reasigne los puertos que planea usar para configurar los puntos finales del balanceador de carga. El formato utilizado es: <i>network type/protocol/remapped port /default port used by grid node</i>, donde <i>network type</i> es grid, admin o cliente, y <i>protocol</i> es tcp o udp. Ejemplo: PORT_REMAP_INBOUND = grid/tcp/3022/22 También puede reasignar varios puertos entrantes utilizando una lista separada por comas. Ejemplo: PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22	Opcional

Cómo los nodos de la red descubren el nodo de administración principal

Los nodos de la red se comunican con el nodo de administración principal para su configuración y gestión. Cada nodo de la red debe conocer la dirección IP del nodo de administración principal en la red de la red.

Para garantizar que un nodo de la red pueda acceder al nodo de administración principal, puede realizar una de las siguientes acciones al implementar el nodo:

- Puede utilizar el parámetro ADMIN_IP para ingresar manualmente la dirección IP del nodo de administración principal.
- Puede omitir el parámetro ADMIN_IP para que el nodo de la red descubra el valor automáticamente. El descubrimiento automático es especialmente útil cuando la red Grid utiliza DHCP para asignar la dirección IP al nodo de administración principal.

El descubrimiento automático del nodo de administración principal se logra mediante un sistema de nombres de dominio de multidifusión (mDNS). Cuando el nodo de administración principal se inicia por primera vez, publica su dirección IP mediante mDNS. Otros nodos de la misma subred pueden entonces consultar la dirección IP y adquirirla automáticamente. Sin embargo, debido a que el tráfico IP de multidifusión normalmente no se puede enrutar a través de subredes, los nodos en otras subredes no pueden adquirir la dirección IP del nodo de administración principal directamente.

Si utiliza el descubrimiento automático:



- Debe incluir la configuración ADMIN_IP para al menos un nodo de la red en cualquier subred a la que el nodo de administración principal no esté conectado directamente. Luego, este nodo de la red publicará la dirección IP del nodo de administración principal para que otros nodos de la subred la descubran con mDNS.
- Asegúrese de que su infraestructura de red admita el paso de tráfico IP de multidifusión dentro de una subred.

Archivos de configuración de nodos de ejemplo

Puede utilizar los archivos de configuración de nodo de ejemplo para ayudar a configurar los archivos de configuración de nodo para su sistema StorageGRID . Los ejemplos muestran archivos de configuración de nodos para todos los tipos de nodos de la red.

Para la mayoría de los nodos, puede agregar información de direccionamiento de red de administrador y cliente (IP, máscara, puerta de enlace, etc.) cuando configura la red mediante el Administrador de red o la API de instalación. La excepción es el nodo de administración principal. Si desea navegar hasta la IP de la red de administración del nodo de administración principal para completar la configuración de la red (porque la red de red no está enrutada, por ejemplo), debe configurar la conexión de la 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 objetivo Red de cliente se ha configurado como una práctica recomendada, aunque la Red de cliente está deshabilitada de forma predeterminada.

Ejemplo de nodo de administración principal

Nombre de archivo de ejemplo: `/etc/storagegrid/nodes/dc1-adm1.conf`

Contenido del archivo de ejemplo:

```

NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adml-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adml-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adml-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 de nodo de almacenamiento

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

Contenido del archivo de ejemplo:

```

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 de nodo de puerta de enlace

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

Contenido del archivo de ejemplo:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dcl-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 administración no principal

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

Contenido del archivo de ejemplo:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dcl-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dcl-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dcl-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 Para cada uno de sus nodos StorageGRID , debe validar el contenido de esos archivos.

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, la salida muestra **PASSED** para cada archivo de configuración, como se muestra en el ejemplo.



Al utilizar solo un LUN en nodos de solo metadatos, es posible que reciba un mensaje de advertencia que puede ignorarse.

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



Para una instalación automatizada, puede suprimir esta salida utilizando el `-q` o `--quiet` opciones en el `storagegrid` comando (por ejemplo, `storagegrid --quiet...`). Si suprime la salida, el comando tendrá un valor de salida distinto de 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 encuentran errores de configuración, deberá corregirlos antes de continuar con la instalación.

```

Checking for misnamed node configuration files...
WARNING: ignoring /etc/storagegrid/nodes/dcl-adml
WARNING: ignoring /etc/storagegrid/nodes/dcl-sn2.conf.keep
WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dcl-adml...
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 dcl-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 dcl-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 dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes...
ERROR: GRID_NETWORK_IP = 10.1.0.4
      dcl-sn2 and dcl-sn3 have the same GRID_NETWORK_IP
ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_RANGEDB_00

```

Iniciar el servicio de host de StorageGRID

Para iniciar los nodos StorageGRID y garantizar que se reinicien después de un reinicio del 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 garantizar que la implementación esté en curso:

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

3. Si algún nodo devuelve un estado de "No en ejecución" o "Detenido", ejecute el siguiente comando:

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

4. Si ya ha habilitado e iniciado el servicio de host StorageGRID (o si no está seguro de si el servicio se ha habilitado e iniciado), ejecute también el siguiente comando:

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

Configurar la red y completar la instalación (Ubuntu o Debian)

Vaya al Administrador de cuadrícula

Utilice el Administrador de cuadrícula para definir toda la información necesaria para configurar su sistema StorageGRID .

Antes de empezar

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

Pasos

1. Abra su navegador web y navegue a:

```
https://primary_admin_node_ip
```

Alternativamente, puede acceder al Administrador de cuadrícula en el puerto 8443:

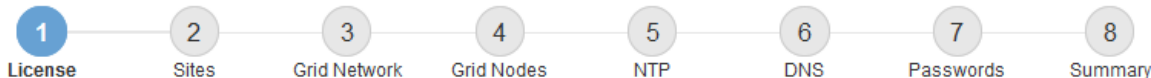
```
https://primary_admin_node_ip:8443
```

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

2. Administre una contraseña de instalador temporal según sea necesario:
 - Si ya se ha establecido una contraseña utilizando uno de estos métodos, introdúzcala para continuar.
 - Un usuario estableció la contraseña al acceder al instalador previamente
 - La contraseña se importó automáticamente desde el archivo de configuración del nodo en `/etc/storagegrid/nodes/<node_name>.conf`
 - Si no se ha establecido una contraseña, opcionalmente establezca una contraseña para proteger el instalador de StorageGRID .
3. Seleccione ***Instalar un sistema StorageGRID ***.

Aparece la página utilizada para configurar un sistema StorageGRID .

Install



License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File

Browse

Especifique la información de la licencia de StorageGRID

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

Pasos

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

Después de la instalación, el nombre se muestra en la parte superior del menú Nodos.

2. Seleccione **Explorar** y localice el archivo de licencia de NetApp(NLF-*unique-id*.txt) y seleccione **Abrir**.

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



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

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File NLF-959007-Internal.txt

License Serial Number

3. Seleccione **Siguiente**.

Agregar sitios

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

Pasos

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

Agregue tantos sitios adicionales como sean necesarios para su topología de cuadrícula. Puedes agregar hasta 16 sitios.

The screenshot shows the NetApp StorageGRID installation wizard. At the top, there's a blue header with 'NetApp® StorageGRID®' and a 'Help' dropdown. Below the header is a progress bar with eight steps: 1. License, 2. Sites (current step), 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS, 7. Passwords, and 8. Summary. Below the progress bar, the 'Sites' section is displayed. It contains two paragraphs explaining single-site and multi-site deployments. Below the text, there are two input fields for 'Site Name'. The first field is labeled 'Site Name 1' and contains the text 'Raleigh'. To its right is a minus sign icon. The second field is labeled 'Site Name 2' and contains the text 'Atlanta'. To its right are plus and minus sign icons.

3. Haga clic en **Siguiente**.

Especificar subredes de la red Grid

Debe especificar las subredes que se utilizan en la red Grid.

Acerca de esta tarea

Las entradas de subred incluyen las subredes de la red Grid para cada sitio en su sistema StorageGRID , junto con cualquier subred a la que se deba poder acceder a través de la red Grid.

Si tiene varias subredes de cuadrícula, se requiere la puerta de enlace de red de cuadrícula. Todas las subredes de la red 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 **Subred 1**.
2. Haga clic en el signo más junto a la última entrada para agregar una entrada de red adicional. Debe especificar todas las subredes para todos los sitios en la red Grid.
 - Si ya ha implementado al menos un nodo, haga clic en **Descubrir subredes de redes de cuadrícula** para completar automáticamente la Lista de subredes de redes de cuadrícula con las subredes

informadas por los nodos de cuadrícula que se han registrado con el Administrador de cuadrícula.

- Debe agregar manualmente cualquier subred para NTP, DNS, LDAP u otros servidores externos a los que se acceda a través de la puerta de enlace de Grid Network.

3. Haga clic en **Siguiente**.

Aprobar nodos de red pendientes

Debe aprobar cada nodo de la red antes de que pueda unirse al sistema StorageGRID .

Antes de empezar

Ha implementado todos los nodos de red del dispositivo virtual y StorageGRID .



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

Pasos

1. Revise la lista de Nodos pendientes y confirme que muestra todos los nodos de la red que implementó.



Si falta un nodo de la red, confirme que se haya implementado correctamente y que tenga la IP de red de la red correcta del nodo de administración principal configurada para ADMIN_IP.

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



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve		✖ Remove		Search		
	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address	
☒	50:6b:4b:42:d7:00	NetApp-SGA	Storage Node	StorageGRID Appliance	172.16.5.20/21	

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit		Reset		✖ Remove		Search	
	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address	
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21	
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21	
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21	
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21	
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21	

3. Haga clic en **Aprobar**.

4. En Configuración general, modifique la configuración de las siguientes propiedades, según sea necesario:

- **Sitio:** El nombre del sistema del sitio para este nodo de la cuadrícula.
- **Nombre:** El nombre del sistema para el nodo. El nombre predeterminado es el nombre que especificó cuando configuró el nodo.

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

- **Rol NTP:** El rol del Protocolo de tiempo de red (NTP) del nodo de la red. Las opciones son **Automático**, **Principal** y **Cliente**. Al seleccionar **Automático** se asigna la función principal a los nodos de administración, nodos de almacenamiento con servicios ADC, nodos de puerta de enlace y cualquier nodo de red que tenga direcciones IP no estáticas. A todos los demás nodos de la red se les asigna el rol de Cliente.



Asegúrese de que al menos dos nodos en cada sitio puedan acceder al menos a cuatro fuentes NTP externas. Si solo un nodo en un sitio puede acceder a las fuentes NTP, se producirán problemas de sincronización si ese nodo deja de funcionar. Además, designar dos nodos por sitio como fuentes NTP primarias garantiza una sincronización precisa si un sitio está aislado del resto de la red.

- **Tipo de almacenamiento** (solo nodos de almacenamiento): especifique que un nuevo nodo de almacenamiento se use exclusivamente para datos únicamente, solo metadatos o ambos. Las opciones son **Datos y metadatos** ("combinados"), **Solo datos** y **Solo metadatos**.



Ver "[Tipos de nodos de almacenamiento](#)" para obtener información sobre los requisitos para estos tipos de nodos.

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

5. En Grid Network, 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
- **Puerta de enlace**: La puerta de enlace de la red Grid. Por ejemplo: 192.168.0.1

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



Si seleccionó DHCP para la configuración de la red Grid y cambia el valor aquí, el nuevo valor se configurará como una dirección estática en el nodo. Debe asegurarse de que la dirección IP configurada no esté dentro de un grupo de direcciones DHCP.

6. Si desea configurar la red de administración para el nodo de la red, agregue o actualice las configuraciones en la sección Red de administración según sea necesario.

Introduzca las subredes de destino de las rutas que salen 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 la red de administración y cambia el valor aquí, el nuevo valor se configurará como una dirección estática en el nodo. Debe asegurarse de que la dirección IP configurada no esté dentro de un grupo de direcciones 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 podrá configurar en este cuadro de diálogo Administrador de red. En su lugar, debes seguir estos pasos:

- Reinicie el dispositivo: en el Instalador del dispositivo, seleccione **Avanzado > Reiniciar**.

El reinicio puede tardar varios minutos.

- Seleccione **Configurar redes > Configuración de enlace** y habilite las redes adecuadas.
- Seleccione **Configurar redes > Configuración IP** y configure las redes habilitadas.

- d. Regrese a la página de inicio y haga clic en **Iniciar instalación**.
- e. En el Administrador de cuadrícula: si el nodo figura en la tabla Nodos aprobados, elimine el nodo.
- f. Eliminar el nodo de la tabla Nodos pendientes.
- g. Espere a que el nodo vuelva a aparecer en la lista de Nodos pendientes.
- h. Confirme que puede configurar las redes adecuadas. Ya deberían estar completados con la información proporcionada en la página de Configuración de IP del Instalador del dispositivo.

Para obtener información adicional, consulte la ["Inicio rápido para la instalación de hardware"](#) para localizar instrucciones para su electrodoméstico.

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



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

Dispositivos: Para un dispositivo StorageGRID , si la red del cliente no se configuró durante la instalación inicial mediante el instalador del dispositivo StorageGRID , no se podrá configurar en este cuadro de diálogo Administrador de Grid. En su lugar, debes seguir estos pasos:

- a. Reinicie el dispositivo: en el Instalador del dispositivo, seleccione **Avanzado > Reiniciar**.

El reinicio puede tardar varios minutos.

- b. Seleccione **Configurar redes > Configuración de enlace** y habilite las redes adecuadas.
- c. Seleccione **Configurar redes > Configuración IP** y configure las redes habilitadas.
- d. Regrese a la página de inicio y haga clic en **Iniciar instalación**.
- e. En el Administrador de cuadrícula: si el nodo figura en la tabla Nodos aprobados, elimine el nodo.
- f. Eliminar el nodo de la tabla Nodos pendientes.
- g. Espere a que el nodo vuelva a aparecer en la lista de Nodos pendientes.
- h. Confirme que puede configurar las redes adecuadas. Ya deberían estar completados con la información proporcionada en la página de Configuración de IP del Instalador del dispositivo.

Para obtener información sobre cómo instalar dispositivos StorageGRID , consulte la ["Inicio rápido para la instalación de hardware"](#) para localizar instrucciones para su electrodoméstico.

8. Haga clic en **Guardar**.

La entrada del nodo de la cuadrícula se mueve a la lista de Nodos aprobados.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit

Reset

Remove

Search

	Grid Network MAC Address II	Name II	Site II	Type II	Platform II	Grid Network IPv4 Address ▼
	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

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

Debes aprobar todos los nodos que quieras en la red. Sin embargo, puede regresar 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 los nodos de la cuadrícula, haga clic en **Siguiente**.

Especifique la información del servidor de Protocolo de tiempo de red

Debe especificar la información de configuración del Protocolo de tiempo de red (NTP) para el sistema StorageGRID , de modo que las operaciones realizadas en servidores separados puedan mantenerse sincronizadas.

Acerca de esta tarea

Debe especificar direcciones IPv4 para los servidores NTP.

Debe especificar servidores NTP externos. Los servidores NTP especificados deben utilizar el protocolo NTP.

Debe especificar cuatro referencias de servidor NTP de Stratum 3 o superior para evitar problemas con la diferencia horaria.



Al especificar la fuente NTP externa para una instalación de 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 hora en versiones anteriores de Windows no es lo suficientemente preciso y Microsoft no lo admite para su uso en entornos de alta precisión, como StorageGRID.

["Límite de soporte para configurar el servicio de hora de Windows para entornos de alta precisión"](#)

Los servidores NTP externos son utilizados por los nodos a los que previamente les asignó roles NTP primarios.



Asegúrese de que al menos dos nodos en cada sitio puedan acceder al menos a cuatro fuentes NTP externas. Si solo un nodo en un sitio puede acceder a las fuentes NTP, se producirán problemas de sincronización si ese nodo deja de funcionar. Además, designar dos nodos por sitio como fuentes NTP primarias garantiza una sincronización precisa si un sitio está aislado del resto de la red.

Pasos

- 1. Especifique las direcciones IPv4 de 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 de servidor adicionales.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

Summary

Network Time Protocol

Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync.

Server 1

10.60.248.183

Server 2

10.227.204.142

Server 3

10.235.48.111

Server 4

0.0.0.0

+

- 3. Seleccione **Siguiente**.

Información relacionada

["Pautas para establecer redes"](#)

Especificar la información del servidor DNS

Debe especificar la información de DNS para su sistema StorageGRID , de modo que pueda acceder a servidores externos utilizando nombres de host en lugar de direcciones IP.

Acerca de esta tarea

Especificando ["Información del servidor DNS"](#) le permite utilizar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP para notificaciones por correo electrónico y AutoSupport.

Para garantizar un funcionamiento correcto, especifique dos o tres servidores DNS. Si especifica más de tres, es posible que solo se utilicen tres debido a las limitaciones conocidas del sistema operativo en algunas plataformas. Si tiene restricciones de enrutamiento en su entorno, puede ["personalizar la lista de servidores DNS"](#) para que los nodos individuales (normalmente todos los nodos de un sitio) utilicen un conjunto diferente de hasta tres servidores DNS.

Si es posible, utilice servidores DNS a los que cada sitio pueda acceder localmente para garantizar que un sitio aislado pueda resolver los FQDN para destinos externos.

Pasos

1. Especifique la dirección IPv4 de 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 de servidor adicionales.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there's a blue header with "NetApp® StorageGRID®" and a "Help" link. Below the header is a progress bar with eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS (highlighted in blue), 7. Passwords, and 8. Summary. Below the progress bar, the "Domain Name Service" section is active. It contains a text box with instructions: "Enter the IP address for at least one Domain Name System (DNS) server, so that server hostnames can be used instead of IP addresses. Specifying at least two DNS servers is recommended. Configuring DNS enables server connectivity, email notifications, and NetApp AutoSupport." Below this, there are two input fields for DNS servers. "Server 1" has the IP address "10.224.223.130" and a red "X" icon to its right. "Server 2" has the IP address "10.224.223.136" and a red "+" icon to its right, indicating that more servers can be added.

La mejor práctica 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 de su sistema StorageGRID , deberá ingresar las contraseñas que se utilizarán para proteger su sistema y realizar tareas de mantenimiento.

Acerca de esta tarea

Utilice la página Instalar contraseñas para especificar la frase de contraseña de aprovisionamiento y la contraseña del usuario raíz de administración de la red.

- La frase de contraseña de aprovisionamiento se utiliza como clave de cifrado y no la almacena el sistema StorageGRID .
- Debe tener la contraseña de aprovisionamiento para los procedimientos de instalación, expansión y mantenimiento, incluida la descarga del paquete de recuperación. Por lo tanto, es importante que guardes la contraseña de aprovisionamiento en una ubicación segura.
- Puede cambiar la contraseña de aprovisionamiento desde el Administrador de Grid si tiene la actual.
- La contraseña del usuario raíz de administración de la red se puede cambiar mediante el Administrador de red.
- Las contraseñas de la consola de línea de comandos generadas aleatoriamente y de SSH se almacenan en el `Passwords.txt` archivo en el paquete de recuperación.

Pasos

1. En **Frase de contraseña de aprovisionamiento**, ingrese la frase de contraseña de aprovisionamiento que será necesaria para realizar cambios en la topología de la red de su sistema StorageGRID .

Guarde la contraseña de aprovisionamiento en un lugar seguro.



Si después de completarse la instalación desea cambiar la contraseña de aprovisionamiento más tarde, puede utilizar el Administrador de Grid. Seleccione **CONFIGURACIÓN > Control de acceso > Contraseñas de red**.

2. En **Confirmar contraseña de aprovisionamiento**, vuelva a ingresar la contraseña de aprovisionamiento para confirmarla.
3. En **Contraseña de usuario raíz de administración de red**, ingrese la contraseña que se utilizará para acceder al Administrador de red como usuario "root".

Guarde la contraseña en un lugar seguro.

4. En **Confirmar contraseña de usuario root**, vuelva a ingresar la contraseña de Grid Manager para confirmarla.

NetApp® StorageGRID®
Help

Install

1 License
2 Sites
3 Grid Network
4 Grid Nodes
5 NTP
6 DNS
7 Passwords
8 Summary

Passwords

Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step.

Provisioning Passphrase

.....

Confirm Provisioning Passphrase

.....

Grid Management Root User Password

.....

Confirm Root User Password

.....

☒ Create random command line passwords.

- Si está instalando una cuadrícula para fines de prueba de concepto o demostración, opcionalmente desmarque la casilla de verificación **Crear contraseñas de línea de comando aleatorias**.

Para las implementaciones de producción, siempre se deben utilizar contraseñas aleatorias por razones de seguridad. Borre **Crear contraseñas de línea de comando aleatorias** solo para cuadrículas de demostración si desea usar contraseñas predeterminadas para acceder a los nodos de la cuadrícula desde la línea de comando usando la cuenta "root" o "admin".



Se le solicitará que descargue el archivo del paquete de recuperación(`sgws-recovery-package-id-revision.zip`) después de hacer clic en **Instalar** en la página Resumen. Usted debe ["descargar este archivo"](#) para completar la instalación. Las contraseñas necesarias para acceder al sistema se almacenan en el `Passwords.txt` archivo, contenido en el archivo del paquete de recuperación.

- Haga clic en **Siguiente**.

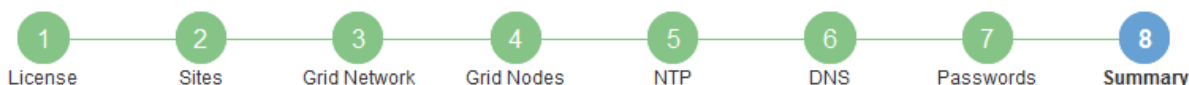
Revise su configuración y complete la instalación

Debe revisar cuidadosamente la información de configuración que ha ingresado para asegurarse de que la instalación se complete correctamente.

Pasos

- Ver la página **Resumen**.

Install



Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name	Grid1	Modify License
Passwords	Auto-generated random command line passwords	Modify Passwords

Networking

NTP	10.60.248.183 10.227.204.142 10.235.48.111	Modify NTP
DNS	10.224.223.130 10.224.223.136	Modify DNS
Grid Network	172.16.0.0/21	Modify Grid Network

Topology

Topology	Atlanta	Modify Sites	Modify Grid Nodes
	Raleigh		
	dc1-adm1	dc1-g1	dc1-s1
	dc1-s2	dc1-s3	NetApp-SGA

2. Verifique que toda la información de configuración de la red sea correcta. Utilice los enlaces Modificar en la página Resumen para volver atrás y corregir cualquier error.
3. Haga clic en **Instalar**.



Si un nodo está configurado para usar la red del cliente, la puerta de enlace predeterminada para ese nodo cambia de la red de cuadrícula a la red del cliente cuando hace clic en **Instalar**. Si pierde la conectividad, debe asegurarse de acceder al nodo de administración principal a través de una subred accesible. Ver "[Pautas para establecer redes](#)" Para más detalles.

4. Haga clic en **Descargar paquete de recuperación**.

Cuando la instalación avanza hasta el punto donde se define la topología de la red, se le solicitará que descargue el archivo del paquete de recuperación(.zip) y confirme que puede acceder correctamente al contenido de este archivo. Debe descargar el archivo del paquete de recuperación para poder recuperar el sistema StorageGRID si uno o más nodos de la red fallan. La instalación continúa en segundo plano, pero no puede completar la instalación ni acceder al sistema StorageGRID hasta que descargue y verifique este archivo.

5. Verifique que pueda extraer el contenido del .zip archivo y luego guárdelo en dos ubicaciones seguras, protegidas y separadas.



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

6. Seleccione la casilla de verificación **He descargado y verificado correctamente el archivo del paquete de recuperación** y haga clic en **Siguiente**.

Si la instalación aún está en curso, aparecerá la página de estado. Esta página indica el progreso de la instalación para cada nodo de la red.

Installation Status

If necessary, you may [Download the Recovery Package file](#) again.

Name	IT	Site	IT	Grid Network IPv4 Address	Progress	IT	Stage	IT
dc1-adm1		Site1		172.16.4.215/21			Starting services	
dc1-g1		Site1		172.16.4.216/21			Complete	
dc1-s1		Site1		172.16.4.217/21			Waiting for Dynamic IP Service peers	
dc1-s2		Site1		172.16.4.218/21			Downloading hotfix from primary Admin if needed	
dc1-s3		Site1		172.16.4.219/21			Downloading hotfix from primary Admin if needed	

Cuando se alcanza la etapa Completado para todos los nodos de la red, aparece la página de inicio de sesión del Administrador de la red.

7. Sign in en Grid Manager utilizando el usuario "root" y la contraseña que especificó durante la instalación.

Pautas posteriores a la instalación

Después de completar la implementación y configuración del nodo de la red, siga estas pautas para el direccionamiento DHCP y los cambios de configuración de red.

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

Sólo se puede configurar DHCP durante la fase de implementación. No se puede configurar DHCP durante la configuración.



Los nodos se reinician cuando la configuración de la red Grid se modifica mediante DHCP, lo que puede provocar interrupciones si un cambio de DHCP afecta a varios nodos al mismo tiempo.

- Debe utilizar los procedimientos de Cambio de IP si desea cambiar direcciones IP, máscaras de subred y puertas de enlace predeterminadas para un nodo de la red. Ver "[Configurar direcciones IP](#)".
- Si realiza cambios en la configuración de red, incluidos cambios de enrutamiento y puerta de enlace, es posible que se pierda la conectividad del cliente con el nodo de administración principal y otros nodos de la red. Dependiendo de los cambios de red aplicados, es posible que sea necesario restablecer estas conexiones.

Instalación API REST

StorageGRID proporciona la API de instalación de StorageGRID para realizar tareas de instalación.

La API utiliza la plataforma API de código abierto Swagger para proporcionar la documentación de la API. Swagger permite que tanto los desarrolladores como los no desarrolladores interactúen con la API en una interfaz de usuario que ilustra cómo la API responde a los parámetros y opciones. Esta documentación asume que está familiarizado con las tecnologías web estándar y el formato de datos JSON.



Cualquier operación de API que realice utilizando la página web de Documentación de API son operaciones en vivo. 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, cualquier parámetro de URL obligatorio u opcional y una respuesta de API esperada.

API de instalación de StorageGRID

La API de instalación de StorageGRID solo está disponible cuando configura inicialmente su sistema StorageGRID y si necesita realizar una recuperación del nodo de administración principal. Se puede acceder a la API de instalación a través de HTTPS desde Grid Manager.

Para acceder a la documentación de la API, vaya a la página web de instalación en el nodo de administración principal y seleccione **Ayuda > Documentación de la API** en la barra de menú.

La API de instalación de StorageGRID incluye las siguientes secciones:

- **config** – Operaciones relacionadas con el lanzamiento del producto y las versiones de la API. Puede enumerar la versión de lanzamiento del producto y las versiones principales de la API compatibles con esa versión.
- **grid** – Operaciones de configuración a nivel de cuadrícula. Puede obtener y actualizar la configuración de la red, incluidos los detalles de la red, las subredes de la red, las contraseñas de la red y las direcciones IP del servidor NTP y DNS.
- **nodos** – Operaciones de configuración a nivel de nodo. Puede recuperar una lista de nodos de la cuadrícula, eliminar un nodo de la cuadrícula, configurar un nodo de la cuadrícula, ver un nodo de la cuadrícula y restablecer la configuración de un nodo de la cuadrícula.
- **provision** – 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.
- **recovery-package** – Operaciones para descargar el paquete de recuperación.
- **sitios** – Operaciones de configuración a nivel de sitio. Puede crear, ver, eliminar y modificar un sitio.
- **temporary-password** – Operaciones en la contraseña temporal para proteger la mgmt-api durante la instalación.

Información relacionada

["Automatizar la instalación"](#)

¿A dónde ir después?

Después de completar una instalación, realice las tareas de integración y configuración necesarias. Puede realizar las tareas opcionales según sea necesario.

Tareas requeridas

- ["Crear una cuenta de inquilino"](#) para el protocolo de cliente S3 que se utilizará para almacenar objetos en su sistema StorageGRID .

- ["Acceso al sistema de control"](#) mediante la configuración de grupos y cuentas de usuario. Opcionalmente, puedes ["configurar una fuente de identidad federada"](#) (como Active Directory o OpenLDAP), para que pueda importar grupos de administración y usuarios. O bien, puedes ["crear grupos y usuarios locales"](#) .
- Integrar y probar el ["S3 API"](#) aplicaciones cliente que utilizará para cargar objetos en su sistema StorageGRID .
- ["Configurar las reglas de gestión del ciclo de vida de la información \(ILM\) y la política de ILM"](#) que desea utilizar para proteger los datos del objeto.
- Si su instalación incluye nodos de almacenamiento de dispositivos, utilice SANtricity OS para completar las siguientes tareas:
 - Conéctese a cada dispositivo StorageGRID .
 - Verificar la recepción de datos de AutoSupport .

Ver ["Configurar el hardware"](#) .

- Revisar y seguir las ["Pautas de fortalecimiento del sistema StorageGRID"](#) para eliminar riesgos de seguridad.
- ["Configurar notificaciones por correo electrónico para alertas del sistema"](#) .

Tareas opcionales

- ["Actualizar las direcciones IP de los nodos de la red"](#) si han cambiado desde que planificó su implementación y generó el paquete de recuperación.
- ["Configurar el cifrado de almacenamiento"](#), si es necesario.
- ["Configurar la compresión de almacenamiento"](#) para reducir el tamaño de los objetos almacenados, si es necesario.
- ["Configurar interfaces VLAN"](#) para aislar y particionar el tráfico de la red, si es necesario.
- ["Configurar grupos de alta disponibilidad"](#) para mejorar la disponibilidad de la conexión para los clientes Grid Manager, Tenant Manager y S3, si es necesario.
- ["Configurar los puntos finales del balanceador de carga"](#) para la conectividad del cliente S3, si es necesario.

Solucionar problemas de instalación

Si ocurre algún problema durante la instalación del sistema StorageGRID , puede acceder a los archivos de registro de instalación. Es posible que el soporte técnico también necesite 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 la red)
- `/var/local/log/gdu-server.log` (se encuentra 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 saber cómo acceder a los archivos de registro, consulte ["Recopilar archivos de registro y datos del sistema"](#) .

Información relacionada

["Solucionar problemas de un sistema StorageGRID"](#)

Ejemplo /etc/network/interfaces

El `/etc/network/interfaces` El archivo 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 solo enlace LACP y luego establecerá tres interfaces VLAN que sustentan el enlace para su uso como interfaces de red de cliente, administrador y red de StorageGRID .

Interfaces físicas

Tenga en cuenta que los conmutadores en los otros extremos de los enlaces también deben tratar los cuatro puertos como un único canal troncal o puerto LACP y deben pasar al menos las tres VLAN referenciadas 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 enlace

```
# 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
```

Instalar StorageGRID en VMware

Inicio rápido para la instalación de StorageGRID en VMware

Siga estos pasos de alto nivel para instalar un nodo VMware StorageGRID .

1

Preparación

- Conozca más sobre ["Arquitectura y topología de red de StorageGRID"](#) .
- Conozca los detalles de ["Redes StorageGRID"](#) .
- Reúne y prepara el ["Información y materiales necesarios"](#) .
- Instalar y configurar ["VMware vSphere Hypervisor, vCenter y los hosts ESX"](#) .
- Preparar lo necesario ["CPU y RAM"](#) .
- Mantener ["requisitos de almacenamiento y rendimiento"](#) .

2

Despliegue

Implementar nodos de red. Cuando se implementan nodos de red, estos se crean como parte del sistema StorageGRID y se conectan a una o más redes.

- Utilice VMware vSphere Web Client, un archivo .vmdk y un conjunto de plantillas de archivos .ovf para ["Implementar los nodos basados en software como máquinas virtuales \(VM\)"](#) en los servidores que preparó en el paso 1.
- Para implementar nodos del dispositivo StorageGRID, siga las instrucciones ["Inicio rápido para la instalación de hardware"](#).

3

Configuración

Cuando se hayan implementado todos los nodos, utilice el Administrador de cuadrícula para ["Configurar la red y completar la instalación"](#).

Automatizar la instalación

Para ahorrar tiempo y brindar coherencia, puede automatizar la implementación y la configuración de los nodos de la red y la configuración del sistema StorageGRID.

- ["Automatice la implementación de nodos de red mediante VMware vSphere"](#).
- Después de implementar los nodos de la red, ["automatizar la configuración del sistema StorageGRID"](#) utilizando el script de configuración de Python proporcionado en el archivo de instalación.
- ["Automatizar la instalación y configuración de nodos de red de dispositivos"](#)
- Si es un desarrollador avanzado de implementaciones de StorageGRID, automatice la instalación de nodos de la red mediante el uso de ["API REST de instalación"](#).

Planificar y prepararse para la instalación en VMware

Información y materiales necesarios

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

Información requerida

Plan de red

Qué redes desea conectar a cada nodo de StorageGRID. StorageGRID admite múltiples redes para separación de tráfico, seguridad y conveniencia administrativa.

Ver StorageGRID ["Pautas para establecer redes"](#).

Información de la red

Direcciones IP a asignar a cada nodo de la red y las direcciones IP de los servidores DNS y NTP.

Servidores para nodos de red

Identifique un conjunto de servidores (físicos, virtuales o ambos) que, en conjunto, proporcionen recursos suficientes para soportar la cantidad y el tipo de nodos StorageGRID que planea implementar.



Si su instalación de StorageGRID no utilizará nodos de almacenamiento del dispositivo StorageGRID (hardware), deberá utilizar almacenamiento RAID de hardware con caché de escritura respaldado por batería (BBWC). StorageGRID no admite el uso de redes de área de almacenamiento virtual (vSAN), RAID de software o ninguna protección RAID.

Información relacionada

["Herramienta de matriz de interoperabilidad de NetApp"](#)

Materiales necesarios

Licencia de NetApp StorageGRID

Debe tener una licencia de NetApp válida y firmada digitalmente.



En el archivo de instalación de StorageGRID se incluye una licencia que no es de producción y que se puede utilizar para realizar pruebas y comprobar el concepto de las redes.

Archivo de instalación de StorageGRID

["Descargue el archivo de instalación de StorageGRID y extraiga los archivos"](#) .

Servicio de computadora portátil

El sistema StorageGRID se instala a través de una computadora portátil de servicio.

La computadora portátil de servicio debe tener:

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

Documentación de StorageGRID

- ["Notas de la versión"](#)
- ["Instrucciones para administrar StorageGRID"](#)

Descargue y extraiga los archivos de instalación de StorageGRID

Debe descargar los archivos de instalación de StorageGRID y extraer los archivos. Opcionalmente, puede verificar manualmente los archivos en el paquete de instalación.

Pasos

1. Ir a la ["Página de descargas de NetApp para StorageGRID"](#) .
2. Seleccione el botón para descargar la última versión o seleccione otra versión del menú desplegable y seleccione **Ir**.
3. Sign in con el nombre de usuario y la contraseña de su cuenta de NetApp .
4. Si aparece una declaración de Precaución/Lectura obligatoria, léala y seleccione la casilla de verificación.



Debe aplicar las revisiones necesarias después de instalar la versión de StorageGRID . Para obtener más información, consulte la ["Procedimiento de revisión en las instrucciones de recuperación y mantenimiento"](#)

5. Lea el Acuerdo de licencia de usuario final, seleccione la casilla de verificación y luego seleccione **Aceptar y continuar**.
6. En la columna **Instalar StorageGRID**, seleccione el archivo de instalación .tgz o .zip para VMware.



Utilice el .zip archivo si está ejecutando Windows en la computadora portátil de servicio.

7. Guarde el archivo de instalación.
8. Si necesita verificar el archivo de instalación:
 - a. Descargue el paquete de verificación de firma de código de StorageGRID . El nombre de archivo de este paquete utiliza el formato `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , dónde <version-number> es la versión del software StorageGRID .
 - b. Siga los pasos para ["verificar manualmente los archivos de instalación"](#) .
9. Extraiga los archivos del archivo de instalación.
10. Elige los archivos que necesitas.

Los archivos que necesita dependen de la topología de red planificada y de cómo implementará su 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
	Un 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 la máquina virtual que se utiliza como plantilla para crear máquinas virtuales de nodo de cuadrícula.
	El archivo de plantilla de formato de virtualización abierta(.ovf) y archivo de manifiesto(.mf) para implementar el nodo de administración principal.
	El archivo de plantilla(.ovf) y archivo de manifiesto(.mf) para implementar nodos de administración no principales.
	El archivo de plantilla(.ovf) y archivo de manifiesto(.mf) para implementar nodos de puerta de enlace.

Ruta y nombre de archivo	Descripción
	El archivo de plantilla(<code>.ovf</code>) y archivo de manifiesto(<code>.mf</code>) para implementar nodos de almacenamiento basados en máquinas virtuales.
Herramienta de scripting de implementación	Descripción
	Un script de shell Bash utilizado para automatizar la implementación de nodos de red virtuales.
	Un archivo de configuración de ejemplo para usar con el <code>deploy-vsphere-ovftool.sh</code> guion.
	Un script de Python utilizado para automatizar la configuración de un sistema StorageGRID .
	Un script de Python utilizado para automatizar la configuración de dispositivos StorageGRID .
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único (SSO) está habilitado. También puede utilizar este script para la integración de Ping Federate.
	Un archivo de configuración de ejemplo para usar con el <code>configure-storagegrid.py</code> guion.
	Un archivo de configuración en blanco para usar con el <code>configure-storagegrid.py</code> guion.
	Un ejemplo de secuencia de comandos de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script de ayuda llamado por el compañero <code>storagegrid-ssoauth-azure.py</code> Script de Python para realizar interacciones de SSO con Azure.

Ruta y nombre de archivo	Descripción
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno de StorageGRID que no sea de producción para realizar pruebas de compatibilidad de actualización.

Verificar manualmente los archivos de instalación (opcional)

Si es necesario, puede verificar manualmente los archivos en el archivo de instalación de StorageGRID .

Antes de empezar

Tienes ["descargué el paquete de verificación"](#) desde ["Página de descargas de NetApp para StorageGRID"](#) .

Pasos

1. Extraiga los artefactos del paquete de verificación:

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Asegúrese de que se hayan extraído estos artefactos:

- Certificado de hoja: Leaf-Cert.pem
- Cadena de certificados: CA-Int-Cert.pem
- Cadena de respuesta de marca de tiempo: TS-Cert.pem
- Archivo de suma de comprobación: sha256sum
- Firma de suma de comprobación: sha256sum.sig
- Archivo de respuesta de marca de tiempo: sha256sum.sig.tsr

3. Utilice la cadena para verificar que el certificado de hoja sea válido.

Ejemplo: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

Resultado esperado: Leaf-Cert.pem: OK

4. Si el paso 2 falló debido a un certificado de hoja vencido, utilice el `tsr` archivo a verificar.

Ejemplo: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

Los resultados esperados incluyen: Verification: OK

5. Cree un archivo de clave pública a partir del certificado de hoja.

Ejemplo: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

Resultado esperado: *ninguno*

6. Utilice la clave pública para verificar la sha256sum archivo contra sha256sum.sig .

Ejemplo: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

Resultado esperado: Verified OK

7. Verificar el sha256sum contenido del archivo contra sumas de comprobación recién creadas.

Ejemplo: `sha256sum -c sha256sum`

Resultado esperado: `<filename>: OK`
`<filename>` es el nombre del archivo que descargaste.

8. ["Complete los pasos restantes"](#) para extraer y elegir los archivos de instalación adecuados.

Requisitos de software para VMware

Puede utilizar una máquina virtual para alojar cualquier tipo de nodo StorageGRID . Necesita una máquina virtual para cada nodo de la red.

Hipervisor VMware vSphere

Debe instalar VMware vSphere Hypervisor en un servidor físico preparado. El hardware debe estar configurado correctamente (incluidas las versiones de firmware y la configuración del BIOS) antes de instalar el software VMware.

- Configure la red en el hipervisor según sea necesario para admitir la red para el sistema StorageGRID que está instalando.

["Pautas para establecer 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 la red.
- Si crea más de un almacén de datos, asigne un nombre a cada uno para poder identificar fácilmente qué almacén de datos usar para cada nodo de la cuadrícula cuando cree máquinas virtuales.

Requisitos de configuración del host ESX



Debe configurar correctamente el protocolo de tiempo de red (NTP) en cada host ESX. Si la hora del host es incorrecta, podrían ocurrir efectos negativos, incluida la pérdida de datos.

Requisitos de configuración de VMware

Debe instalar y configurar VMware vSphere y vCenter antes de implementar nodos StorageGRID .

Para conocer las versiones compatibles del software VMware vSphere Hypervisor y VMware vCenter Server, consulte la ["Herramienta de matriz de interoperabilidad de NetApp"](#) .

Para conocer los pasos necesarios para instalar estos productos VMware, consulte la documentación de VMware.

Requisitos de CPU y RAM

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

Cada nodo de StorageGRID requiere los siguientes recursos mínimos:

- Núcleos de CPU: 8 por nodo
- RAM: depende de la RAM total disponible y de la cantidad de software que no sea StorageGRID que se ejecute en el sistema
 - Generalmente, al menos 24 GB por nodo y de 2 a 16 GB menos que la RAM total del sistema.
 - Un mínimo de 64 GB para cada inquilino que tendrá aproximadamente 5000 buckets

Los recursos de nodo de solo metadatos basados en software deben coincidir con los recursos de los nodos de almacenamiento existentes. Por ejemplo:

- Si el sitio StorageGRID existente utiliza dispositivos SG6000 o SG6100, los nodos de solo metadatos basados en software deben cumplir los siguientes requisitos mínimos:
 - 128 GB de RAM
 - CPU de 8 núcleos
 - SSD de 8 TB o almacenamiento equivalente para la base de datos Cassandra (rangedb/0)
- Si el sitio StorageGRID existente usa nodos de almacenamiento virtuales con 24 GB de RAM, CPU de 8 núcleos y 3 TB o 4 TB de almacenamiento de metadatos, los nodos solo de metadatos basados en software deben usar recursos similares (24 GB de RAM, CPU de 8 núcleos y 4 TB de almacenamiento de metadatos (rangedb/0)).

Al agregar un nuevo sitio StorageGRID , la capacidad total de metadatos del nuevo sitio debe coincidir, como mínimo, con los sitios StorageGRID existentes y los recursos del nuevo sitio deben coincidir con los nodos de almacenamiento de los sitios StorageGRID existentes.

VMware admite un nodo por máquina virtual. Asegúrese de que el nodo StorageGRID no exceda la RAM física disponible. Cada máquina virtual debe estar dedicada a ejecutar StorageGRID.



Supervise periódicamente el uso de su CPU y memoria para garantizar que estos recursos sigan adaptándose a su carga de trabajo. Por ejemplo, duplicar la asignación de RAM y CPU para los nodos de almacenamiento virtuales proporcionaría recursos similares a los proporcionados para los nodos del dispositivo StorageGRID . Además, si la cantidad de metadatos por nodo supera los 500 GB, considere aumentar la RAM por nodo a 48 GB o más. Para obtener información sobre cómo administrar el almacenamiento de metadatos de objetos, aumentar la configuración del espacio reservado de metadatos y monitorear el uso de CPU y memoria, consulte las instrucciones para [administrando](#) , [escucha](#) , y [actualización](#) StorageGRID.

Si el hiperprocesamiento está habilitado en los hosts físicos subyacentes, puede proporcionar 8 núcleos virtuales (4 núcleos físicos) por nodo. Si el hiperprocesamiento no está habilitado en los hosts físicos subyacentes, debe proporcionar 8 núcleos físicos por nodo.

Si utiliza máquinas virtuales como hosts y tiene control sobre el tamaño y la cantidad de máquinas virtuales, debe usar una sola máquina virtual para cada nodo StorageGRID y dimensionar la máquina virtual en consecuencia.

Consulte también ["Requisitos de almacenamiento y rendimiento"](#) .

Requisitos de almacenamiento y rendimiento

Debe comprender los requisitos de almacenamiento y rendimiento de los nodos StorageGRID alojados en máquinas virtuales, de modo que pueda proporcionar suficiente espacio para soportar la configuración inicial y la futura expansión del almacenamiento.

Requisitos de rendimiento

El rendimiento del volumen del sistema operativo y del primer volumen de almacenamiento afecta significativamente el rendimiento general del sistema. Asegúrese de que estos proporcionen un rendimiento de disco adecuado en términos de latencia, operaciones de entrada/salida por segundo (IOPS) y rendimiento.

Todos los nodos de StorageGRID requieren que la unidad del sistema operativo y todos los volúmenes de almacenamiento tengan habilitado el almacenamiento en caché de escritura diferida. La caché debe estar en un medio protegido o persistente.

Requisitos para máquinas virtuales que utilizan almacenamiento NetApp ONTAP

Si está implementando un nodo StorageGRID como una máquina virtual con almacenamiento asignado desde un sistema NetApp ONTAP , ha confirmado que el volumen no tiene habilitada una política de niveles de FabricPool . Por ejemplo, si un nodo StorageGRID se ejecuta como una máquina virtual en un host VMware, asegúrese de que el volumen que respalda el almacén de datos para el nodo no tenga una política de niveles de FabricPool habilitada. Deshabilitar la organización en niveles de FabricPool para los volúmenes utilizados con nodos StorageGRID simplifica la resolución de problemas y las operaciones de almacenamiento.



Nunca use FabricPool para agrupar datos relacionados con StorageGRID en StorageGRID mismo. La organización de los datos de StorageGRID en niveles en StorageGRID aumenta la resolución de problemas y la complejidad operativa.

Número de máquinas virtuales necesarias

Cada sitio de StorageGRID requiere un mínimo de tres nodos de almacenamiento.

Requisitos de almacenamiento por tipo de nodo

En un entorno de producción, las máquinas virtuales para los nodos StorageGRID deben cumplir diferentes requisitos, según los tipos de nodos.



Las instantáneas de disco no se pueden usar para restaurar nodos de la red. En su lugar, consulte la ["recuperación del nodo de la red"](#) procedimientos para cada tipo de nodo.

Tipo de nodo	Almacenamiento
Nodo de administración	LUN de 100 GB para SO
	LUN de 200 GB para tablas de nodos de administración
	LUN de 200 GB para el registro de auditoría del nodo de administración

Tipo de nodo	Almacenamiento
Nodo de almacenamiento	LUN de 100 GB para SO 3 LUN para cada nodo de almacenamiento en este host Nota: Un nodo de almacenamiento puede tener de 1 a 16 LUN de almacenamiento; se recomiendan al menos 3 LUN de almacenamiento. Tamaño mínimo por LUN: 4 TB Tamaño máximo de LUN probado: 39 TB.
Nodo de almacenamiento (solo metadatos)	LUN de 100 GB para SO 1 LUN Tamaño mínimo por LUN: 4 TB Tamaño máximo de LUN probado: 39 TB. Nota: Solo se requiere una rangedb para los nodos de almacenamiento de solo metadatos.
Nodo de puerta de enlace	LUN de 100 GB para SO



Según el nivel de auditoría configurado, el tamaño de las entradas del usuario, como el nombre de la clave del objeto S3, y la cantidad de datos del registro de auditoría que necesita conservar, es posible que deba aumentar el tamaño del LUN del registro de auditoría en cada nodo de administración. Generalmente, una cuadrícula genera aproximadamente 1 KB de datos de auditoría por operación S3, lo que significaría que un LUN de 200 GB admitiría 70 millones de operaciones por día u 800 operaciones por segundo durante dos o tres días.

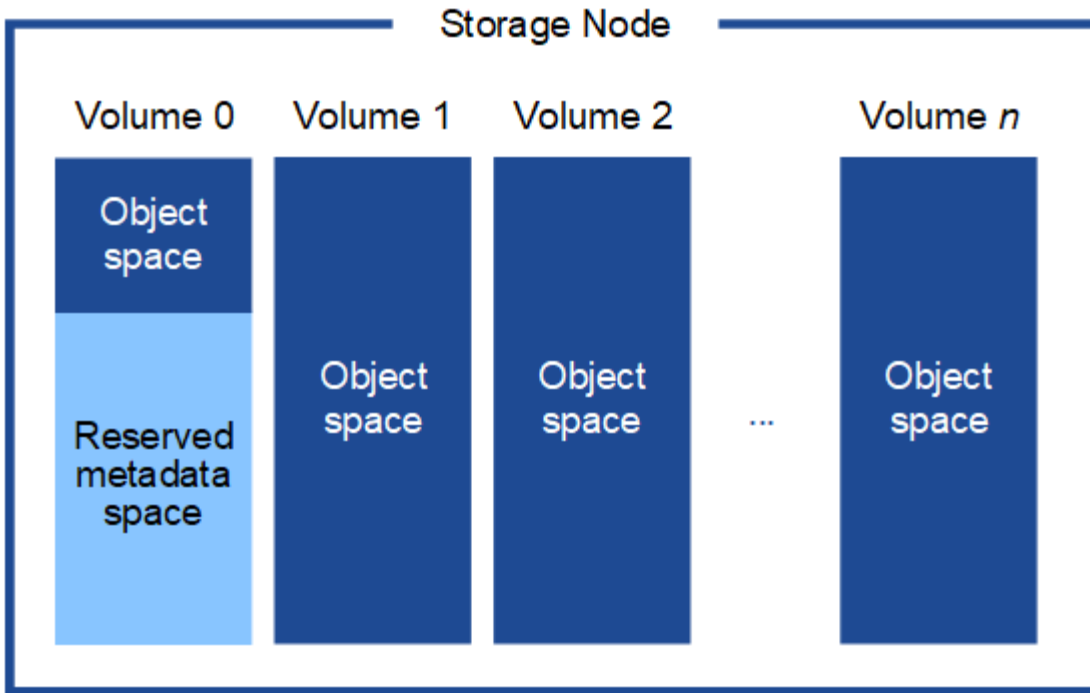
Requisitos de almacenamiento para nodos de almacenamiento

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 de 4 TB o más.



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

Como se muestra en la figura, StorageGRID reserva espacio para los metadatos de objetos 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 datos de objetos.



Para proporcionar redundancia y proteger los metadatos de los objetos contra pérdidas, StorageGRID almacena tres copias de los metadatos de todos los objetos del sistema en cada sitio. Las tres copias de metadatos de objetos se distribuyen uniformemente entre todos los nodos de almacenamiento en cada sitio.

Al instalar una cuadrícula con nodos de almacenamiento solo de metadatos, la cuadrícula también debe contener una cantidad mínima de nodos para el almacenamiento de objetos. Ver ["Tipos de nodos de almacenamiento"](#) para obtener más información sobre los nodos de almacenamiento de solo metadatos.

- Para una cuadrícula de un solo sitio, se configuran al menos dos nodos de almacenamiento para objetos y metadatos.
- Para una cuadrícula de varios sitios, se configura al menos un nodo de almacenamiento por sitio para objetos y metadatos.

Cuando asigna espacio al volumen 0 de un nuevo nodo de almacenamiento, debe asegurarse de que haya espacio adecuado para la parte de metadatos de objetos de ese nodo.

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



Si usa solo un volumen de almacenamiento para un nodo de almacenamiento y asigna 4 TB o menos al volumen, el nodo de almacenamiento podría ingresar al estado de solo lectura de almacenamiento al iniciarse y almacenar solo metadatos de objetos.



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

- Los recursos de nodo de solo metadatos basados en software deben coincidir con los recursos de los nodos de almacenamiento existentes. Por ejemplo:
 - Si el sitio StorageGRID existente utiliza dispositivos SG6000 o SG6100, los nodos de solo metadatos basados en software deben cumplir los siguientes requisitos mínimos:
 - 128 GB de RAM

- CPU de 8 núcleos
- SSD de 8 TB o almacenamiento equivalente para la base de datos Cassandra (rangedb/0)
- Si el sitio StorageGRID existente usa nodos de almacenamiento virtuales con 24 GB de RAM, CPU de 8 núcleos y 3 TB o 4 TB de almacenamiento de metadatos, los nodos solo de metadatos basados en software deben usar recursos similares (24 GB de RAM, CPU de 8 núcleos y 4 TB de almacenamiento de metadatos (rangedb/0)).

Al agregar un nuevo sitio StorageGRID , la capacidad total de metadatos del nuevo sitio debe coincidir, como mínimo, con los sitios StorageGRID existentes y los recursos del nuevo sitio deben coincidir con los nodos de almacenamiento de los sitios StorageGRID existentes.

- Si está instalando un nuevo sistema (StorageGRID 11.6 o superior) y cada nodo de almacenamiento tiene 128 GB o más de RAM, asigne 8 TB o más al volumen 0. El uso de un valor mayor para el volumen 0 puede aumentar el espacio permitido para los metadatos en cada nodo de almacenamiento.
- Al configurar diferentes nodos de almacenamiento para un sitio, utilice la misma configuración para el volumen 0 si es posible. Si un sitio contiene nodos de almacenamiento de diferentes tamaños, el nodo de almacenamiento con el volumen más pequeño (0) determinará la capacidad de metadatos de ese sitio.

Para más detalles, visite ["Administrar el almacenamiento de metadatos de objetos"](#) .

Automatizar la instalación (VMware)

Puede utilizar la herramienta VMware OVF para automatizar la implementación de nodos de la red. También puede automatizar la configuración de StorageGRID.

Automatizar la implementación de nodos de red

Utilice la herramienta VMware OVF para automatizar la implementación de nodos de red.

Antes de empezar

- Tiene acceso a un sistema Linux/Unix con Bash 3.2 o posterior.
- Tienes VMware vSphere con vCenter
- Tiene VMware OVF Tool 4.1 instalado y configurado correctamente.
- Conoces el nombre de usuario y la contraseña para acceder a VMware vSphere mediante la herramienta OVF
- Tiene los permisos suficientes para implementar máquinas virtuales desde archivos OVF y encenderlas, y permisos para crear volúmenes adicionales para adjuntarlos a las máquinas virtuales. Ver el `ovftool` documentación para más detalles.
- Conoce la URL de la infraestructura virtual (VI) para la ubicación en vSphere donde desea implementar las máquinas virtuales StorageGRID . Esta URL normalmente será una vApp o un grupo de recursos. Por ejemplo: `vi://vcenter.example.com/vi/sgrws`



Puedes utilizar VMware `ovftool` utilidad para determinar este valor (ver la `ovftool` documentación para más detalles).



Si está implementando en una vApp, las máquinas virtuales no se iniciarán automáticamente la primera vez y deberá encenderlas manualmente.

- Ha recopilado toda la información necesaria para el archivo de configuración de implementación. Ver "[Recopilar información sobre su entorno de implementación](#)" para información.
- Tiene acceso a los siguientes archivos desde el archivo de instalación de VMware para StorageGRID:

Nombre del archivo	Descripción
NetApp-SG-versión-SHA.vmdk	El archivo de disco de la máquina virtual que se utiliza como plantilla para crear máquinas virtuales de nodo de cuadrícula. Nota: Este archivo debe estar en la misma carpeta que el .ovf y .mf archivos.
vsphere-primary-admin.ovf vsphere-primary-admin.mf	El archivo de plantilla de formato de virtualización abierta(.ovf) y archivo de manifiesto(.mf) para implementar el nodo de administración principal.
vsphere-no-principal-admin.ovf vsphere-no-principal-admin.mf	El archivo de plantilla(.ovf) y archivo de manifiesto(.mf) para implementar nodos de administración no principales.
vsphere-gateway.ovf vsphere-gateway.mf	El archivo de plantilla(.ovf) y archivo de manifiesto(.mf) para implementar nodos de puerta de enlace.
vsphere-storage.ovf vsphere-storage.mf	El archivo de plantilla(.ovf) y archivo de manifiesto(.mf) para implementar nodos de almacenamiento basados en máquinas virtuales.
implementar-vsphere-ovftool.sh	El script de shell Bash utilizado para automatizar la implementación de nodos de red virtuales.
implementar-vsphere-ovftool-sample.ini	El archivo de configuración de ejemplo para usar con el deploy-vsphere-ovftool.sh guion.

Define el archivo de configuración para tu implementación

Debe especificar la información necesaria para implementar nodos de red virtuales para StorageGRID en un archivo de configuración, que es utilizado por el `deploy-vsphere-ovftool.sh` Script bash. Puede modificar un archivo de configuración de ejemplo, de modo que no tenga que crear el archivo desde cero.

Pasos

1. Hacer 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. Ingrese toda la información necesaria para implementar nodos de red virtual de VMware.

Ver [Configuración del archivo de configuración](#) para información.

4. Cuando haya ingresado y verificado toda la información necesaria, guarde y cierre el archivo.

Configuración del archivo de configuración

El `deploy-vmware-ovftool.ini` El archivo de configuración contiene las configuraciones necesarias para implementar nodos de red virtuales.

El archivo de configuración primero enumera los parámetros globales y luego enumera los parámetros específicos del nodo en secciones definidas por nombre de nodo. Cuando se utiliza el archivo:

- Los *parámetros globales* se aplican a todos los nodos de la cuadrícula.
- Los *parámetros específicos del nodo* anulan los parámetros globales.

Parámetros globales

Los parámetros globales se aplican a todos los nodos de la cuadrícula, a menos que sean anulados por configuraciones en secciones individuales. Coloque los parámetros que se aplican a varios nodos en la sección de parámetros globales y luego anule estas configuraciones según sea necesario en las secciones para 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'
```

Puedes utilizar el `--powerOffTarget` y `--overwrite` Opciones para apagar y reemplazar máquinas virtuales existentes.



Debe implementar nodos en diferentes almacenes de datos y especificar `OVFTOOL_ARGUMENTS` para cada nodo, en lugar de hacerlo globalmente.

- **FUENTE:** La ruta a la plantilla de máquina virtual `StorageGRID(.vmdk)` archivo y el `.ovf` y `.mf` archivos para nodos de cuadrícula individuales. El valor predeterminado es el directorio actual.

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- **OBJETIVO:** La URL de la infraestructura virtual VMware vSphere (vi) para la ubicación donde se implementará `StorageGRID`. Por ejemplo:

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- **GRID_NETWORK_CONFIG:** El método utilizado para adquirir direcciones IP, ya sea ESTÁTICAS o DHCP. El valor predeterminado es ESTÁTICO. Si todos o la mayoría de los nodos utilizan el mismo método para adquirir direcciones IP, puede especificar ese método aquí. Luego puede anular la configuración global especificando configuraciones diferentes para uno o más nodos individuales. Por ejemplo:

```
GRID_NETWORK_CONFIG = STATIC
```

- **GRID_NETWORK_TARGET:** El nombre de una red VMware existente que se utilizará para la red Grid. Si todos o la mayoría de los nodos usan el mismo nombre de red, puedes especificarlo aquí. Luego puede anular la configuración global especificando configuraciones diferentes para uno o más nodos individuales. Por ejemplo:

```
GRID_NETWORK_TARGET = SG Admin Network
```

- **GRID_NETWORK_MASK:** La máscara de red para la red Grid. Si todos o la mayoría de los nodos utilizan la misma máscara de red, puede especificarlo aquí. Luego puede anular la configuración global especificando configuraciones diferentes para uno o más nodos individuales. Por ejemplo:

```
GRID_NETWORK_MASK = 255.255.255.0
```

- **GRID_NETWORK_GATEWAY:** La puerta de enlace de red para la red Grid. Si todos o la mayoría de los nodos utilizan la misma puerta de enlace de red, puede especificarlo aquí. Luego puede anular la configuración global especificando configuraciones diferentes para uno o más nodos individuales. Por ejemplo:

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- **GRID_NETWORK_MTU:** Opcional. La unidad de transmisión máxima (MTU) en la red eléctrica. Si se especifica, el valor debe estar entre 1280 y 9216. Por ejemplo:

```
GRID_NETWORK_MTU = 9000
```

Si se omite, se utiliza 1400.

Si desea utilizar tramas jumbo, configure la MTU en un valor adecuado para tramas jumbo, 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 conmutador virtual en vSphere al que está conectado el nodo. De lo contrario, podrían ocurrir problemas de rendimiento de la red o pérdida de paquetes.



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

- **ADMIN_NETWORK_CONFIG:** El método utilizado para adquirir direcciones IP, ya sea DESHABILITADO, ESTÁTICO o DHCP. El valor predeterminado es DESHABILITADO. Si todos o la mayoría de los nodos utilizan el mismo método para adquirir direcciones IP, puede especificar ese método aquí. Luego puede

anular la configuración global especificando configuraciones diferentes para uno o más 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 o la mayoría de los nodos usan el mismo nombre de red, puedes especificarlo aquí. A diferencia de la red Grid, no es necesario que todos los nodos estén conectados a la misma red de administración. Luego puede anular la configuración global especificando configuraciones diferentes para uno o más nodos individuales. Por ejemplo:

```
ADMIN_NETWORK_TARGET = SG Admin Network
```

- **ADMIN_NETWORK_MASK:** La máscara de red para la red de administración. Esta configuración es necesaria si está utilizando una dirección IP estática. Si todos o la mayoría de los nodos utilizan la misma máscara de red, puede especificarlo aquí. Luego puede anular la configuración global especificando configuraciones diferentes para uno o más 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 utiliza 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 especificarlo aquí. Luego puede anular la configuración global especificando configuraciones diferentes para uno o más nodos individuales. Por ejemplo:

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- **ADMIN_NETWORK_ESL:** La lista de subredes externas (rutas) para la red de administración, especificada como una lista separada por comas de destinos de ruta CIDR. Si todos o la mayoría de los nodos utilizan la misma lista de subredes externas, puede especificarlo aquí. Luego puede anular la configuración global especificando configuraciones diferentes para uno o más 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 utiliza 1400. Si desea utilizar tramas jumbo, configure la MTU en un valor adecuado para tramas jumbo, como 9000. De lo contrario, mantenga el valor predeterminado. Si todos o la mayoría de los nodos usan la misma MTU para la red de administración, puede especificarlo aquí. Luego puede anular la configuración global especificando configuraciones diferentes para uno o más nodos individuales. Por ejemplo:


```
ADMIN_NETWORK_MTU = 8192
```

- **CLIENT_NETWORK_CONFIG:** El método utilizado para adquirir direcciones IP, ya sea DESHABILITADO, ESTÁTICO o DHCP. El valor predeterminado es DESHABILITADO. Si todos o la mayoría de los nodos utilizan el mismo método para adquirir direcciones IP, puede especificar ese método aquí. Luego puede anular la configuración global especificando configuraciones diferentes para uno o más nodos individuales. Por ejemplo:

```
CLIENT_NETWORK_CONFIG = STATIC
```

- **CLIENT_NETWORK_TARGET:** El nombre de una red VMware existente que se utilizará para la red del cliente. Esta configuración es necesaria a menos que la red del cliente esté deshabilitada. Si todos o la mayoría de los nodos usan el mismo nombre de red, puedes especificarlo aquí. A diferencia de la red Grid, no es necesario que todos los nodos estén conectados a la misma red cliente. Luego puede anular la configuración global especificando configuraciones diferentes para uno o más nodos individuales. Por ejemplo:

```
CLIENT_NETWORK_TARGET = SG Client Network
```

- **CLIENT_NETWORK_MASK:** La máscara de red para la red del cliente. Esta configuración es necesaria si está utilizando una dirección IP estática. Si todos o la mayoría de los nodos utilizan la misma máscara de red, puede especificarlo aquí. Luego puede anular la configuración global especificando configuraciones diferentes para uno o más nodos individuales. Por ejemplo:

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- **CLIENT_NETWORK_GATEWAY:** La puerta de enlace de red para la red del cliente. Esta configuración es necesaria si está utilizando una dirección IP estática. Si todos o la mayoría de los nodos utilizan la misma puerta de enlace de red, puede especificarlo aquí. Luego puede anular la configuración global especificando configuraciones diferentes para uno o más nodos individuales. Por ejemplo:

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- **CLIENT_NETWORK_MTU:** Opcional. La unidad máxima de transmisión (MTU) en la red del cliente. No especifique si CLIENT_NETWORK_CONFIG = DHCP. Si se especifica, el valor debe estar entre 1280 y 9216. Si se omite, se utiliza 1400. Si desea utilizar tramas jumbo, configure la MTU en un valor adecuado para tramas jumbo, como 9000. De lo contrario, mantenga el valor predeterminado. Si todos o la mayoría de los nodos utilizan la misma MTU para la red del cliente, puede especificarlo aquí. Luego puede anular la configuración global especificando configuraciones diferentes para uno o más nodos individuales. Por ejemplo:

```
CLIENT_NETWORK_MTU = 8192
```

- **PORT_REMAP:** Reasigna cualquier puerto utilizado por un nodo para comunicaciones internas del nodo

de la red o comunicaciones externas. La reasignación de puertos es necesaria si las políticas de red empresarial restringen uno o más puertos utilizados por StorageGRID. Para obtener la lista de puertos utilizados por StorageGRID, consulte las comunicaciones internas del nodo de la red y las comunicaciones externas en ["Pautas para establecer redes"](#).



No reasigne los puertos que planea usar para configurar los puntos finales del balanceador de carga.



Si solo se configura `PORT_REMAP`, la asignación que especifique se utilizará tanto para las comunicaciones entrantes como para las salientes. Si también se especifica `PORT_REMAP_INBOUND`, `PORT_REMAP` se aplica solo a las comunicaciones salientes.

El formato utilizado es: *network type/protocol/default port used by grid node/new port*, donde el tipo de red es `grid`, `admin` o `cliente`, y el protocolo es `tcp` o `udp`.

Por ejemplo:

```
PORT_REMAP = client/tcp/18082/443
```

Si se usa solo, esta configuración de ejemplo asigna simétricamente las comunicaciones entrantes y salientes para el nodo de la red desde el puerto 18082 al puerto 443. Si se utiliza junto con `PORT_REMAP_INBOUND`, esta configuración de ejemplo asigna las comunicaciones salientes del puerto 18082 al puerto 443.

También puedes reasignar varios puertos usando una lista separada por comas.

Por ejemplo:

```
PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80
```

- **PORT_REMAP_INBOUND:** Reasigna las comunicaciones entrantes para el puerto especificado. Si especifica `PORT_REMAP_INBOUND` pero no especifica un valor para `PORT_REMAP`, las comunicaciones salientes para el puerto no cambian.



No reasigne los puertos que planea usar para configurar los puntos finales del balanceador de carga.

El formato utilizado es: *network type/protocol/_default port used by grid node/new port*, donde el tipo de red es `grid`, `admin` o `cliente`, y el protocolo es `tcp` o `udp`.

Por ejemplo:

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

Este ejemplo toma el tráfico que se envía al puerto 443 para pasar un firewall interno y lo dirige al puerto 18082, donde el nodo de la red escucha solicitudes S3.

También puede reasignar varios puertos entrantes utilizando una lista separada por comas.

Por ejemplo:

```
PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22
```

- **TEMPORARY_PASSWORD_TYPE**: El tipo de contraseña de instalación temporal que se utilizará al acceder a la consola de VM o a la API de instalación de StorageGRID , o al usar SSH, antes de que el nodo se una a la red.



Si todos o la mayoría de los nodos utilizan el mismo tipo de contraseña de instalación temporal, especifique el tipo en la sección de parámetros globales. Luego, opcionalmente, utilice una configuración diferente para un nodo individual. Por ejemplo, si selecciona **Usar contraseña personalizada** globalmente, puede usar **CUSTOM_TEMPORARY_PASSWORD=<contraseña>** para establecer la contraseña para cada nodo.

TEMPORARY_PASSWORD_TYPE puede ser uno de los siguientes:

- **Usar nombre de nodo**: el nombre de nodo se utiliza como contraseña de instalación temporal y proporciona acceso a la consola de VM, a la API de instalación de StorageGRID y a SSH.
- **Deshabilitar contraseña**: No se utilizará ninguna contraseña de instalación temporal. Si necesita acceder a la máquina virtual para depurar problemas de instalación, consulte ["Solucionar problemas de instalación"](#) .
- **Usar contraseña personalizada**: el valor proporcionado con **CUSTOM_TEMPORARY_PASSWORD=<contraseña>** se utiliza como contraseña de instalación temporal y proporciona acceso a la consola de VM, la API de instalación de StorageGRID y SSH.



Opcionalmente, puede omitir el parámetro **TEMPORARY_PASSWORD_TYPE** y solo especificar **CUSTOM_TEMPORARY_PASSWORD=<contraseña>**.

- **CUSTOM_TEMPORARY_PASSWORD=<contraseña>** Opcional. La contraseña temporal que se utilizará durante la instalación al acceder a la consola de VM, la API de instalación de StorageGRID y SSH. Se ignora si **TEMPORARY_PASSWORD_TYPE** está configurado en **Usar nombre de nodo** o **Deshabilitar contraseña**.

Parámetros específicos del nodo

Cada nodo está en su propia sección del archivo de configuración. Cada nodo requiere las siguientes configuraciones:

- El encabezado de sección define el nombre del nodo que se mostrará en el Administrador de cuadrícula. Puede anular ese valor especificando el parámetro opcional **NODE_NAME** para el nodo.
- **TIPO_DE_NODO**: **Nodo_de_administración_de_VM**, **Nodo_de_almacenamiento_de_VM** o **Nodo_de_puerta_de_enlace_de_API_de_VM**
- **STORAGE_TYPE**: **combinado**, **datos** o **metadatos**. Este parámetro opcional para los nodos de almacenamiento tiene como valor predeterminado **combinado** (datos y metadatos) si no se especifica. Para obtener más información, consulte ["Tipos de nodos de almacenamiento"](#) .
- **GRID_NETWORK_IP**: La dirección IP del nodo en la red Grid.
- **ADMIN_NETWORK_IP**: La dirección IP del nodo en la red de administración. Obligatorio solo si el nodo está conectado a la red de administración y **ADMIN_NETWORK_CONFIG** está configurado como **STATIC**.

- **CLIENT_NETWORK_IP:** La dirección IP del nodo en la red del cliente. Obligatorio solo si el nodo está conectado a la red del cliente y CLIENT_NETWORK_CONFIG para este nodo está configurado como STATIC.
- **ADMIN_IP:** La dirección IP del nodo de administración principal en la red Grid. Utilice el valor que especifique como GRID_NETWORK_IP para el nodo de administración principal. Si omite este parámetro, el nodo intentará descubrir la IP del nodo de administración principal mediante mDNS. Para obtener más información, consulte "[Cómo los nodos de la red descubren el nodo de administración principal](#)".



El parámetro ADMIN_IP se ignora para el nodo de administración principal.

- Cualquier parámetro que no se haya establecido globalmente. Por ejemplo, si un nodo está conectado a la red de administración y no especificó los parámetros ADMIN_NETWORK globalmente, debe especificarlos para el nodo.

Nodo de administración principal

Se requieren las siguientes configuraciones adicionales para el nodo de administración principal:

- **TIPO_DE_NODO:** Nodo_de_administración_de_VM
- **ADMIN_ROLE:** Principal

Esta entrada de ejemplo es para un nodo de administración principal que está en las tres redes:

```
[DC1-ADM1]
ADMIN_ROLE = Primary
NODE_TYPE = VM_Admin_Node
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd

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 auditoría y uso de bases de datos. Puede aumentar estos ajustes utilizando el parámetro DISK. Por ejemplo:

```
DISK = INSTANCES=2, CAPACITY=300
```



Para los nodos de administración, las INSTANCIAS siempre deben ser iguales a 2.

Nodo de almacenamiento

Se requiere la siguiente configuración adicional para los nodos de almacenamiento:

- **TIPO_DE_NODO:** Nodo_de_almacenamiento_de_VM

Esta entrada de ejemplo es para un nodo de almacenamiento que está en la red y en las redes de administración, pero no en la red del cliente. Este nodo utiliza la configuración ADMIN_IP para especificar la dirección IP del nodo de administración principal en la red 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 de cliente donde la política de red empresarial del cliente establece que una aplicación cliente S3 solo puede acceder al nodo de almacenamiento mediante el puerto 80 o 443. El archivo de configuración de ejemplo utiliza PORT_REMAP para permitir que el nodo de almacenamiento envíe y reciba 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 tanto para el tráfico entrante como para el 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
```

Las siguientes configuraciones adicionales son opcionales para los 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. Puede aumentar estos ajustes con el parámetro DISK. Por ejemplo:

```
DISK = INSTANCES=16, CAPACITY=4096
```

- **STORAGE_TYPE:** De forma predeterminada, todos los nodos de almacenamiento nuevos están configurados para almacenar tanto datos de objetos como metadatos, lo que se conoce como un nodo de almacenamiento *combinado*. Puede cambiar el tipo de nodo de almacenamiento para almacenar solo datos o metadatos con el parámetro STORAGE_TYPE. Por ejemplo:

```
STORAGE_TYPE = data
```

Nodo de puerta de enlace

Se requiere la siguiente configuración adicional para los nodos de puerta de enlace:

- **TIPO_DE_NODO:** Puerta_de_Enlace_API_VM

Esta entrada de ejemplo es para un nodo de puerta de enlace de ejemplo en las tres redes. En este ejemplo, no se especificaron parámetros de red de cliente en la sección global del archivo de configuración, por lo que deben especificarse 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 administración no principal

Las siguientes configuraciones adicionales son necesarias para los nodos de administración no principales:

- **TIPO_DE_NODO:** Nodo_de_administración_de_VM
- **ADMIN_ROLE:** No principal

Esta entrada de ejemplo es para un nodo de administración no principal que no está en la red del 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 administración no principales:

- **DISCO:** De forma predeterminada, a los nodos de administración se les asignan dos discos duros adicionales de 200 GB para auditoría y uso de bases de datos. Puede aumentar estos ajustes utilizando el parámetro DISK. Por ejemplo:

```
DISK = INSTANCES=2, CAPACITY=300
```



Para los nodos de administración, las INSTANCIAS siempre deben ser iguales a 2.

Ejecutar el script Bash

Puedes utilizar el `deploy-vsphere-ovftool.sh` Script Bash y archivo de configuración `deploy-vsphere-ovftool.ini` que modificó para automatizar la implementación de nodos StorageGRID en VMware vSphere.

Antes de empezar

Ha creado un archivo de configuración `deploy-vsphere-ovftool.ini` para su entorno.

Puede utilizar la ayuda disponible con el script Bash ingresando los comandos de ayuda (`-h/--help`). Por ejemplo:

```
./deploy-vsphere-ovftool.sh -h
```

o

```
./deploy-vsphere-ovftool.sh --help
```

Pasos

1. Inicie sesión en la máquina Linux que está utilizando para ejecutar el script Bash.
2. Cambie al directorio donde extrajo el archivo de instalación.

Por ejemplo:

```
cd StorageGRID-Webscale-version/vsphere
```

3. Para implementar todos los nodos de la red, ejecute el script 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 la red no se pudo implementar debido a un error, resuelva el error y vuelva a ejecutar el script Bash solo para ese nodo.

Por ejemplo:

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd --single  
-node="DC1-S3" ./deploy-vsphere-ovftool.ini
```

La implementación se completa cuando el estado de cada nodo es "Aprobado".

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

Automatizar la configuración de StorageGRID

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

Antes de empezar

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

Nombre del archivo	Descripción
configurar-storagegrid.py	Script de Python utilizado para automatizar la configuración

Nombre del archivo	Descripción
configure-storagegrid.sample.json	Archivo de configuración de ejemplo para usar con el script
configurar-storagegrid.blank.json	Archivo de configuración en blanco para usar con el script

- Has 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`).

Puedes utilizar el `configure-storagegrid.py` Script de Python y el `configure-storagegrid.json` Archivo de configuración de cuadrícula para automatizar la configuración de su sistema StorageGRID .



También puede configurar el sistema utilizando el Administrador de Grid o la API de instalación.

Pasos

1. Inicie sesión en la máquina Linux que está utilizando para ejecutar el script de Python.
2. Cambie al directorio donde extrajo el archivo de instalación.

Por ejemplo:

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

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

3. Ejecute el script de 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 donde se está ejecutando el proceso de instalación y configuración. Debe realizar una copia de seguridad del archivo del paquete de recuperación para poder recuperar el sistema StorageGRID si uno o más nodos de la red fallan. Por ejemplo, cópielo en una ubicación de red segura y respaldada y en una ubicación de almacenamiento en la nube segura.



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

Si especificó que se deben generar contraseñas aleatorias, abra el `Passwords.txt` archivo y busque las

contraseñas necesarias para acceder a su 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.           #####
#####
```

Su sistema StorageGRID está instalado y configurado cuando se muestra un mensaje de confirmación.

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

Información relacionada

- ["Vaya al Administrador de cuadrícula"](#)
- ["Instalación API REST"](#)

Implementar nodos de red de máquinas virtuales (VMware)

Recopilar información sobre su entorno de implementación

Antes de implementar nodos de red, debe recopilar información sobre la configuración de su red y el entorno de VMware.



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

Información de VMware

Debe acceder al entorno de implementación y recopilar información sobre el entorno de VMware; las redes que se crearon para las redes Grid, Admin y Client; y los tipos de volumen de almacenamiento que planea usar para los nodos de almacenamiento.

Debe recopilar información sobre su entorno VMware, incluida la siguiente:

- 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 StorageGRID .



VMware Live vMotion hace que el tiempo del reloj de la máquina virtual salte y no es compatible con nodos de red de ningún tipo. Aunque es poco frecuente, los horarios de reloj incorrectos pueden provocar la pérdida de datos o actualizaciones de configuración.

Información de la red Grid

Debe recopilar información sobre la red VMware creada para la red StorageGRID Grid (obligatorio), que

incluye:

- El nombre de la red.
- El método utilizado para asignar direcciones IP, ya sea estática o DHCP.
 - Si utiliza direcciones IP estáticas, los detalles de red necesarios para cada nodo de la red (dirección IP, puerta de enlace, máscara de red).
 - Si está utilizando DHCP, la dirección IP del nodo de administración principal en la red Grid. Ver ["Cómo los nodos de la red descubren el nodo de administración principal"](#) Para más información.

Información de la red de administración

Para los nodos que se conectarán a la red de administración StorageGRID opcional, debe recopilar información sobre la red VMware creada para esta red, que incluye:

- El nombre de la red.
- El método utilizado para asignar direcciones IP, ya sea estática o DHCP.
 - Si utiliza direcciones IP estáticas, los detalles de red necesarios para cada nodo de la red (dirección IP, puerta de enlace, máscara de red).
 - Si está utilizando DHCP, la dirección IP del nodo de administración principal en la red Grid. Ver ["Cómo los nodos de la red descubren el nodo de administración principal"](#) Para más información.
- La lista de subredes externas (ESL) para la red de administración.

Información de la red del cliente

Para los nodos que se conectarán a la red de cliente StorageGRID opcional, debe recopilar información sobre la red VMware creada para esta red, que incluye:

- El nombre de la red.
- El método utilizado para asignar direcciones IP, ya sea estática o DHCP.
- Si utiliza direcciones IP estáticas, los detalles de red necesarios para cada nodo de la red (dirección IP, puerta de enlace, máscara de red).

Información sobre interfaces adicionales

Opcionalmente, puede agregar interfaces troncales o 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 de puerta de enlace, de modo que pueda usar interfaces VLAN para segregar el tráfico que pertenece a diferentes aplicaciones o inquilinos. O bien, es posible que desee agregar una interfaz de acceso para usar en un grupo de alta disponibilidad (HA).

Las interfaces que agregue se muestran en la página de interfaces VLAN y en la página de grupos HA en el Administrador de Grid.

- Si agrega una interfaz troncal, configure una o más interfaces VLAN para cada nueva interfaz principal. Ver ["configurar interfaces VLAN"](#) .
- Si agrega una interfaz de acceso, debe agregarla directamente a los grupos de HA. Ver ["configurar grupos de alta disponibilidad"](#) .

Volúmenes de almacenamiento para nodos de almacenamiento virtuales

Debe recopilar la siguiente información para los nodos de almacenamiento basados en máquinas virtuales:

- La cantidad y el tamaño de los volúmenes de almacenamiento (LUN de almacenamiento) que planea agregar. Consulte ["Requisitos de almacenamiento y rendimiento"](#) .

Información de configuración de la red

Debes recopilar información para configurar tu red:

- Licencia de red
- Direcciones IP del servidor de Protocolo de tiempo de red (NTP)
- Direcciones IP del servidor DNS

Cómo los nodos de la red descubren el nodo de administración principal

Los nodos de la red se comunican con el nodo de administración principal para su configuración y gestión. Cada nodo de la red debe conocer la dirección IP del nodo de administración principal en la red de la red.

Para garantizar que un nodo de la red pueda acceder al nodo de administración principal, puede realizar una de las siguientes acciones al implementar el nodo:

- Puede utilizar el parámetro ADMIN_IP para ingresar manualmente la dirección IP del nodo de administración principal.
- Puede omitir el parámetro ADMIN_IP para que el nodo de la red descubra el valor automáticamente. El descubrimiento automático es especialmente útil cuando la red Grid utiliza DHCP para asignar la dirección IP al nodo de administración principal.

El descubrimiento automático del nodo de administración principal se logra mediante un sistema de nombres de dominio de multidifusión (mDNS). Cuando el nodo de administración principal se inicia por primera vez, publica su dirección IP mediante mDNS. Otros nodos de la misma subred pueden entonces consultar la dirección IP y adquirirla automáticamente. Sin embargo, debido a que el tráfico IP de multidifusión normalmente no se puede enrutar a través de subredes, los nodos en otras subredes no pueden adquirir la dirección IP del nodo de administración principal directamente.

Si utiliza el descubrimiento automático:



- Debe incluir la configuración ADMIN_IP para al menos un nodo de la red en cualquier subred a la que el nodo de administración principal no esté conectado directamente. Luego, este nodo de la red publicará la dirección IP del nodo de administración principal para que otros nodos de la subred la descubran con mDNS.
- Asegúrese de que su infraestructura de red admita el paso de tráfico IP de multidifusión dentro de una subred.

Implementar un nodo StorageGRID como una máquina virtual

Utilice VMware vSphere Web Client para implementar cada nodo de la red como una máquina virtual. Durante la implementación, cada nodo de la red se crea y se conecta a una o más redes StorageGRID .

Si necesita implementar cualquier nodo de almacenamiento del dispositivo StorageGRID , consulte ["Implementar el nodo de almacenamiento del dispositivo"](#) .

Opcionalmente, puede reasignar los puertos del nodo o aumentar la configuración de CPU o memoria para el nodo antes de encenderlo.

Antes de empezar

- Has revisado cómo ["planificar y prepararse para la instalación"](#) , y comprende los requisitos de software, CPU y RAM, y almacenamiento y rendimiento.
- Está familiarizado con VMware vSphere Hypervisor y tiene experiencia en la implementación de máquinas virtuales en este entorno.



El `open-vm-tools` El paquete, una implementación de código abierto similar a VMware Tools, se incluye con la máquina virtual StorageGRID . No es necesario instalar VMware Tools manualmente.

- Ha descargado y extraído la versión correcta del archivo de instalación de StorageGRID para VMware.



Si está implementando el nuevo nodo como parte de una operación de expansión o recuperación, debe usar la versión de StorageGRID que se esté ejecutando actualmente en la red.

- Tiene el disco de máquina virtual StorageGRID(`.vmdk`) archivo:

```
NetApp-SG-version-SHA.vmdk
```

- Tú tienes el `.ovf` y `.mf` archivos para cada tipo de nodo de cuadrícula que esté implementando:

Nombre del 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-no-principal-admin.ovf vsphere-no-principal-admin.mf	El archivo de plantilla y el archivo de manifiesto para un nodo de administración no principal.
vsphere-storage.ovf vsphere-storage.mf	El archivo de plantilla y el archivo de manifiesto para un nodo de almacenamiento.
vsphere-gateway.ovf vsphere-gateway.mf	El archivo de plantilla y el archivo de manifiesto para un nodo de puerta de enlace.

- El `.vmdk` , `.ovf` , y `.mf` Todos los archivos están en el mismo directorio.
- Tiene un plan para minimizar los dominios de falla. Por ejemplo, no debe implementar todos los nodos de puerta de enlace en un solo host vSphere ESXi.



En una implementación de producción, no ejecute más de un nodo de almacenamiento en una sola máquina virtual. No ejecute varias máquinas virtuales en el mismo host ESXi si eso crearía un problema de dominio de falla inaceptable.

- Si está implementando un nodo como parte de una operación de expansión o recuperación, tiene la ["Instrucciones para expandir un sistema StorageGRID"](#) o el ["instrucciones de recuperación y mantenimiento"](#).
- Si está implementando un nodo StorageGRID como una máquina virtual con almacenamiento asignado desde un sistema NetApp ONTAP, ha confirmado que el volumen no tiene habilitada una política de niveles de FabricPool. Por ejemplo, si un nodo StorageGRID se ejecuta como una máquina virtual en un host VMware, asegúrese de que el volumen que respalda el almacén de datos para el nodo no tenga una política de niveles de FabricPool habilitada. Deshabilitar la organización en niveles de FabricPool para los volúmenes utilizados con nodos StorageGRID simplifica la resolución de problemas y las operaciones de almacenamiento.



Nunca use FabricPool para agrupar datos relacionados con StorageGRID en StorageGRID mismo. La organización de los datos de StorageGRID en niveles en StorageGRID aumenta la resolución de problemas y la complejidad operativa.

Acerca de esta tarea

Siga estas instrucciones para implementar inicialmente nodos de VMware, agregar un nuevo nodo de VMware en una expansión o reemplazar un nodo de VMware como parte de una operación de recuperación. Salvo lo indicado en los pasos, el procedimiento de implementación de nodos es el mismo para todos los tipos de nodos, incluidos los nodos de administración, los nodos de almacenamiento y los nodos de puerta de enlace.

Si está instalando un nuevo sistema StorageGRID :

- Puede implementar nodos en cualquier orden.
- Debe asegurarse de que cada máquina virtual pueda conectarse al nodo de administración principal a través de la red Grid.
- Debe implementar todos los nodos de la red antes de configurar la red.

Si está realizando una operación de expansión o recuperación:

- Debe asegurarse de que la nueva máquina virtual pueda conectarse a todos los demás nodos a través de la red Grid.

Si necesita reasignar alguno de los puertos del nodo, no encienda el nuevo nodo hasta que se complete la configuración de reasignación del puerto.

Pasos

1. Usando VCenter, implemente una plantilla OVF.

Si especifica una URL, apunte a una carpeta que contenga los siguientes archivos. De lo contrario, seleccione cada uno de estos archivos desde un directorio local.

```
NetApp-SG-version-SHA.vmdk  
vsphere-node.ovf  
vsphere-node.mf
```

Por ejemplo, si este es el primer nodo que está implementando, use estos archivos para implementar el nodo de administración principal para su sistema StorageGRID :

```
NetApp-SG-version-SHA.vmdk  
vsphere-primary-admin.ovf  
vsphere-primary-admin.mf
```

2. Proporcione un nombre para la máquina virtual.

La práctica estándar es utilizar el mismo nombre tanto para la máquina virtual como para el nodo de la red.

3. Coloque la máquina virtual en la vApp o grupo de recursos apropiado.

4. Si está implementando el nodo de administración principal, lea y acepte el Acuerdo de licencia de usuario final.

Según su versión de vCenter, el orden de los pasos variará para aceptar el Acuerdo de licencia de usuario final, especificar el nombre de la máquina virtual y seleccionar un almacén de datos.

5. Seleccione almacenamiento para la máquina virtual.

Si está implementando un nodo como parte de una operación de recuperación, siga las instrucciones en el [paso de recuperación de almacenamiento](#) para agregar nuevos discos virtuales, volver a conectar los discos duros virtuales desde el nodo de red fallido o ambos.

Al implementar un nodo de almacenamiento, utilice 3 o más volúmenes de almacenamiento, cada uno de los cuales debe ser 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 eliminarlos y asignar VMDK o RDM adecuados para el almacenamiento antes de encender el nodo. Los VMDK se utilizan con mayor frecuencia en entornos VMware y son más fáciles de administrar, mientras que los RDM pueden proporcionar un mejor rendimiento para cargas de trabajo que utilizan tamaños de objetos más grandes (por ejemplo, más de 100 MB).



Algunas instalaciones de StorageGRID pueden usar volúmenes de almacenamiento más grandes y más activos que las cargas de trabajo virtualizadas típicas. Es posible que necesite ajustar algunos parámetros del hipervisor, como `MaxAddressableSpaceTB` , para lograr un rendimiento óptimo. Si observa un rendimiento deficiente, comuníquese con su recurso de soporte de virtualización para determinar si su entorno podría beneficiarse de un ajuste de configuración específico de la carga de trabajo.

6. Seleccionar redes.

Determine qué redes StorageGRID utilizará el nodo seleccionando una red de destino para cada red de origen.

- Se requiere la red Grid. Debe seleccionar una red de destino en el entorno de vSphere. + La red Grid se utiliza para todo el tráfico interno de StorageGRID . Proporciona conectividad entre todos los nodos de la red, en todos los sitios y subredes. Todos los nodos de la red deben poder comunicarse con todos los demás nodos.

- Si utiliza la red de administración, seleccione una red de destino diferente en el entorno de vSphere. Si no utiliza la red de administración, seleccione el mismo destino que seleccionó para la red de cuadrícula.
- Si utiliza la red de cliente, seleccione una red de destino diferente en el entorno de vSphere. Si no utiliza la red de cliente, seleccione el mismo destino que seleccionó para la red de cuadrícula.
- Si utiliza una red de administrador o de cliente, los nodos no tienen que estar en las mismas redes de administrador o de cliente.

7. Para **Personalizar plantilla**, configure las propiedades del nodo StorageGRID requeridas.

a. Introduzca el **nombre del nodo**.



Si está recuperando un nodo de la cuadrícula, debe ingresar el nombre del nodo que está recuperando.

b. Utilice el menú desplegable **Contraseña de instalación temporal** para especificar una contraseña de instalación temporal, de modo que pueda acceder a la consola de VM o a la API de instalación de StorageGRID , o usar SSH, antes de que el nuevo nodo se una a la red.



La contraseña de instalación temporal solo se utiliza durante la instalación del nodo. Después de agregar un nodo a la red, puede acceder a él mediante el "[contraseña de la consola del nodo](#)" , que figura en el `Passwords.txt` archivo en el paquete de recuperación.

- **Usar nombre de nodo:** el valor proporcionado para el campo **Nombre de nodo** se utiliza como contraseña de instalación temporal.
- **Usar contraseña personalizada:** Se utiliza una contraseña personalizada como contraseña de instalación temporal.
- **Deshabilitar contraseña:** No se utilizará ninguna contraseña de instalación temporal. Si necesita acceder a la máquina virtual para depurar problemas de instalación, consulte "[Solucionar problemas de instalación](#)" .

c. Si seleccionó **Usar contraseña personalizada**, especifique la contraseña de instalación temporal que desea utilizar en el campo **Contraseña personalizada**.

d. En la sección **Red de cuadrícula (eth0)**, seleccione ESTÁTICA o DHCP para la **Configuración de IP de red de cuadrícula**.

- Si selecciona ESTÁTICO, ingrese la **IP de red de cuadrícula**, la **Máscara de red de cuadrícula**, la **Puerta de enlace de red de cuadrícula** y la **MTU de red de cuadrícula**.
- Si selecciona DHCP, la **IP de red de cuadrícula**, la **Máscara de red de cuadrícula** y la **Puerta de enlace de red de cuadrícula** se asignan automáticamente.

e. En el campo **IP de administrador principal**, ingrese la dirección IP del nodo de administrador principal de la red Grid.



Este paso no se aplica si el nodo que está implementando es el nodo de administración principal.

Si omite la dirección IP del nodo de administración principal, la dirección IP se descubrirá automáticamente si el nodo de administración principal, o al menos otro nodo de red con ADMIN_IP configurado, está presente en la misma subred. Sin embargo, se recomienda configurar aquí la dirección IP del nodo de administración principal.

- a. En la sección **Red de administración (eth1)**, seleccione ESTÁTICA, DHCP o DESHABILITADO para la **Configuración de IP de la red de administración**.
- Si no desea utilizar la red de administración, seleccione DESHABILITADO e ingrese **0.0.0.0** para la IP de la red de administración. Puedes dejar los demás campos en blanco.
 - Si selecciona ESTÁTICO, ingrese la **IP de red de administrador**, la **Máscara de red de administrador**, la **Puerta de enlace de red de administrador** y la **MTU de red de administrador**.
 - Si selecciona ESTÁTICO, ingrese a la **lista de subredes externas de la red de administración**. También debes configurar una puerta de enlace.
 - Si selecciona DHCP, la **IP de red de administrador**, la **Máscara de red de administrador** y la **Puerta de enlace de red de administrador** se asignan automáticamente.

- b. En la sección **Red de cliente (eth2)**, seleccione ESTÁTICA, DHCP o DESHABILITADO para la **Configuración de IP de red de cliente**.

- Si no desea utilizar la red del cliente, seleccione DESHABILITADO e ingrese **0.0.0.0** para la IP de la red del cliente. Puedes dejar los demás campos en blanco.
- Si selecciona ESTÁTICO, ingrese la **IP de red del cliente**, la **Máscara de red del cliente**, la **Puerta de enlace de red del cliente** y la **MTU de red del cliente**.
- Si selecciona DHCP, la **IP de red del cliente**, la **Máscara de red del cliente** y la **Puerta de enlace de red del cliente** se asignan automáticamente.

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 una operación de recuperación y esta no es una recuperación de nodo completo, realice estos pasos una vez completada la implementación:

- a. Haga clic derecho en la máquina virtual y seleccione **Editar configuración**.
- b. Seleccione cada disco duro virtual predeterminado que haya sido designado para almacenamiento y seleccione **Eliminar**.
- c. Dependiendo de sus circunstancias de recuperación de datos, agregue nuevos discos virtuales según sus requisitos de almacenamiento, vuelva a conectar cualquier disco duro virtual preservado del nodo de red fallido eliminado anteriormente, o ambos.

Tenga en cuenta las siguientes pautas importantes:

- Si está agregando nuevos discos, debe utilizar el mismo tipo de dispositivo de almacenamiento que estaba en uso antes de la recuperación del nodo.
- 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 eliminarlos y asignar VMDK o RDM adecuados para el almacenamiento antes de encender el nodo. Los VMDK se utilizan con mayor frecuencia en entornos VMware y son más fáciles de administrar, mientras que los RDM pueden proporcionar un mejor rendimiento para cargas de trabajo que utilizan tamaños de objetos más grandes (por ejemplo, más de 100 MB).

11. Si necesita reasignar los puertos utilizados por este nodo, siga estos pasos.

Es posible que necesite reasignar un puerto si sus políticas de red empresarial restringen el acceso a uno o más puertos utilizados por StorageGRID. Ver el "[pautas de redes](#)" para los puertos utilizados por StorageGRID.



No reasigne los puertos utilizados en los puntos finales del balanceador de carga.

- a. Seleccione la nueva VM.
- b. Desde la pestaña Configurar, seleccione **Configuración > Opciones de vApp**. La ubicación de **Opciones de vApp** depende de la versión de vCenter.
- c. En la tabla **Propiedades**, ubique PORT_REMAP_INBOUND y PORT_REMAP.
- d. Para mapear simétricamente las comunicaciones entrantes y salientes de un puerto, seleccione **PORT_REMAP**.



Si solo se configura PORT_REMAP, la asignación que especifique se aplicará tanto a las comunicaciones entrantes como a las salientes. Si también se especifica PORT_REMAP_INBOUND, PORT_REMAP se aplica solo a las comunicaciones salientes.

- i. Seleccione **Establecer valor**.
- ii. Introduzca el mapeo del puerto:

```
<network type>/<protocol>/<default port used by grid node>/<new port>
```

<network type> es grid, admin o cliente, y <protocol> es tcp o udp.

Por ejemplo, para reasignar el tráfico ssh del puerto 22 al puerto 3022, ingrese:

```
client/tcp/22/3022
```

Puede reasignar varios puertos utilizando una lista separada por comas.

Por ejemplo:

```
client/tcp/18082/443, client/tcp/18083/80
```

- i. Seleccione **Aceptar**.
- e. Para especificar el puerto utilizado para las comunicaciones entrantes al nodo, seleccione **PORT_REMAP_INBOUND**.



Si especifica PORT_REMAP_INBOUND y no especifica un valor para PORT_REMAP, las comunicaciones salientes para el puerto no cambian.

- i. Seleccione **Establecer valor**.
- ii. Introduzca el mapeo del puerto:

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port used by grid node>
```

<network type> es grid, admin o cliente, y <protocol> es tcp o udp.

Por ejemplo, para reasignar el tráfico SSH entrante que se envía al puerto 3022 para que el nodo de la red lo reciba en el puerto 22, ingrese lo siguiente:

```
client/tcp/3022/22
```

Puede reasignar varios puertos entrantes utilizando una lista separada por comas.

Por ejemplo:

```
grid/tcp/3022/22, admin/tcp/3022/22
```

i. Seleccione **OK**

12. Si desea aumentar la CPU o la memoria del nodo desde la configuración predeterminada:

- a. Haga clic derecho en la máquina virtual y seleccione **Editar configuración**.
- b. Cambie la cantidad de CPU o la cantidad de memoria según sea necesario.

Establezca la **Reserva de memoria** en el mismo tamaño que la **Memoria** asignada a la máquina virtual.

c. Seleccione **Aceptar**.

13. Encienda la máquina virtual.

Después de terminar

Si implementó este nodo como parte de un procedimiento de expansión o recuperación, vuelva a esas instrucciones para completar el procedimiento.

Configurar la red y completar la instalación (VMware)

Vaya al Administrador de cuadrícula

Utilice el Administrador de cuadrícula para definir toda la información necesaria para configurar su sistema StorageGRID .

Antes de empezar

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

Pasos

1. Abra su navegador web y navegue a:

```
https://primary_admin_node_ip
```

Alternativamente, puede acceder al Administrador de cuadrícula en el puerto 8443:

```
https://primary_admin_node_ip:8443
```

Puede utilizar la dirección IP para la IP del nodo de administración principal en la red de cuadrícula o en la red de administración, según corresponda a su configuración de red. Es posible que necesites usar la opción de seguridad/avanzada en tu navegador para navegar a un certificado que no es de confianza.

2. Administre una contraseña de instalador temporal según sea necesario:

- Si ya se ha establecido una contraseña utilizando uno de estos métodos, introdúzcala para continuar.
 - Un usuario estableció la contraseña al acceder al instalador previamente
 - La contraseña SSH/consola se importó automáticamente desde las propiedades de OVF
- Si no se ha establecido una contraseña, opcionalmente establezca una contraseña para proteger el instalador de StorageGRID .

3. Seleccione ***Instalar un sistema StorageGRID ***.

Aparece la página utilizada para configurar una cuadrícula StorageGRID .

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File

Especifique la información de la licencia de StorageGRID

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

Pasos

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

Después de la instalación, el nombre se muestra en la parte superior del menú Nodos.

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

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



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

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File NLF-959007-Internal.txt

License Serial Number

3. Seleccione **Siguiente**.

Agregar sitios

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

Pasos

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

Agregue tantos sitios adicionales como sean necesarios para su topología de cuadrícula. Puedes agregar hasta 16 sitios.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top is a blue header with 'NetApp® StorageGRID®' and a 'Help' dropdown. Below the header is a progress bar with eight steps: 1. License, 2. Sites (highlighted in blue), 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS, 7. Passwords, and 8. Summary. Below the progress bar, the 'Sites' section is active. It contains two paragraphs of text explaining single-site and multi-site deployments. Below the text are two input fields for 'Site Name 1' (containing 'Raleigh') and 'Site Name 2' (containing 'Atlanta'). To the right of the first field is a minus sign icon, and to the right of the second field are plus and minus icons, indicating that more sites can be added.

3. Haga clic en **Siguiente**.

Especificar subredes de la red Grid

Debe especificar las subredes que se utilizan en la red Grid.

Acerca de esta tarea

Las entradas de subred incluyen las subredes de la red Grid para cada sitio en su sistema StorageGRID , junto con cualquier subred a la que se deba poder acceder a través de la red Grid.

Si tiene varias subredes de cuadrícula, se requiere la puerta de enlace de red de cuadrícula. Todas las subredes de la red 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 **Subred 1**.
2. Haga clic en el signo más junto a la última entrada para agregar una entrada de red adicional. Debe especificar todas las subredes para todos los sitios en la red Grid.

- Si ya ha implementado al menos un nodo, haga clic en **Descubrir subredes de redes de cuadrícula** para completar automáticamente la Lista de subredes de redes de cuadrícula con las subredes informadas por los nodos de cuadrícula que se han registrado con el Administrador de cuadrícula.
- Debe agregar manualmente cualquier subred para NTP, DNS, LDAP u otros servidores externos a los que se acceda a través de la puerta de enlace de Grid Network.

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 **Grid Network** 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

Grid Network

You must specify the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network for each site in your StorageGRID system. Select Discover Grid Networks to automatically add subnets based on the network configuration of all registered nodes.

Note: You must manually add any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnet 1 +

3. Haga clic en **Siguiente**.

Aprobar nodos de red pendientes

Debe aprobar cada nodo de la red antes de que pueda unirse al sistema StorageGRID .

Antes de empezar

Ha implementado todos los nodos de red del dispositivo virtual y StorageGRID .



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

Pasos

1. Revise la lista de Nodos pendientes y confirme que muestra todos los nodos de la red que implementó.



Si falta un nodo de la red, confirme que se haya implementado correctamente y que tenga la IP de red de la red correcta del nodo de administración principal configurada para ADMIN_IP.

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



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve ✕ Remove		Search Q				
	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address	
☒	50:6b:4b:42:d7:00	NetApp-SGA	Storage Node	StorageGRID Appliance	172.16.5.20/21	
						◀ ▶

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

✎ Edit ↺ Reset ✕ Remove		Search Q				
	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
						◀ ▶

3. Haga clic en **Aprobar**.

4. En Configuración general, modifique la configuración de las siguientes propiedades, según sea necesario:

- **Sitio:** El nombre del sistema del sitio para este nodo de la cuadrícula.
- **Nombre:** El nombre del sistema para el nodo. El nombre predeterminado es el nombre que especificó cuando configuró el nodo.

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



Para un nodo VMware, puede cambiar el nombre aquí, pero esta acción no cambiará el nombre de la máquina virtual en vSphere.

- **Rol NTP:** El rol del Protocolo de tiempo de red (NTP) del nodo de la red. Las opciones son **Automático**, **Principal** y **Cliente**. Al seleccionar **Automático** se asigna la función principal a los nodos de administración, nodos de almacenamiento con servicios ADC, nodos de puerta de enlace y cualquier nodo de red que tenga direcciones IP no estáticas. A todos los demás nodos de la red se les

asigna el rol de Cliente.



Asegúrese de que al menos dos nodos en cada sitio puedan acceder al menos a cuatro fuentes NTP externas. Si solo un nodo en un sitio puede acceder a las fuentes NTP, se producirán problemas de sincronización si ese nodo deja de funcionar. Además, designar dos nodos por sitio como fuentes NTP primarias garantiza una sincronización precisa si un sitio está aislado del resto de la red.

- **Tipo de almacenamiento** (solo nodos de almacenamiento): especifique que un nuevo nodo de almacenamiento se use exclusivamente para datos únicamente, solo metadatos o ambos. Las opciones son **Datos y metadatos** ("combinados"), **Solo datos** y **Solo metadatos**.



Ver "[Tipos de nodos de almacenamiento](#)" para obtener información sobre los requisitos para estos tipos de nodos.

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

5. En Grid Network, 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
- **Puerta de enlace**: La puerta de enlace de la red Grid. Por ejemplo: 192.168.0.1



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



Si seleccionó DHCP para la configuración de la red Grid y cambia el valor aquí, el nuevo valor se configurará como una dirección estática en el nodo. Debe asegurarse de que la dirección IP configurada no esté dentro de un grupo de direcciones DHCP.

6. Si desea configurar la red de administración para el nodo de la red, agregue o actualice las configuraciones en la sección Red de administración según sea necesario.

Introduzca las subredes de destino de las rutas que salen 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 la red de administración y cambia el valor aquí, el nuevo valor se configurará como una dirección estática en el nodo. Debe asegurarse de que la dirección IP configurada no esté dentro de un grupo de direcciones 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 podrá configurar en este cuadro de diálogo Administrador de red. En su lugar, debes seguir estos pasos:

- a. Reinicie el dispositivo: en el Instalador del dispositivo, seleccione **Avanzado > Reiniciar**.

El reinicio puede tardar varios minutos.

- b. Seleccione **Configurar redes > Configuración de enlace** y habilite las redes adecuadas.
- c. Seleccione **Configurar redes > Configuración IP** y configure las redes habilitadas.
- d. Regrese a la página de inicio y haga clic en **Iniciar instalación**.
- e. En el Administrador de cuadrícula: si el nodo figura en la tabla Nodos aprobados, elimine el nodo.
- f. Eliminar el nodo de la tabla Nodos pendientes.
- g. Espere a que el nodo vuelva a aparecer en la lista de Nodos pendientes.
- h. Confirme que puede configurar las redes adecuadas. Ya deberían estar completados con la información proporcionada en la página de Configuración de IP del Instalador del dispositivo.

Para obtener información adicional, consulte la ["Inicio rápido para la instalación de hardware"](#) para localizar instrucciones para su electrodoméstico.

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



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

Dispositivos: Para un dispositivo StorageGRID , si la red del cliente no se configuró durante la instalación inicial mediante el instalador del dispositivo StorageGRID , no se podrá configurar en este cuadro de diálogo Administrador de Grid. En su lugar, debes seguir estos pasos:

- a. Reinicie el dispositivo: en el Instalador del dispositivo, seleccione **Avanzado > Reiniciar**.

El reinicio puede tardar varios minutos.

- b. Seleccione **Configurar redes > Configuración de enlace** y habilite las redes adecuadas.
- c. Seleccione **Configurar redes > Configuración IP** y configure las redes habilitadas.
- d. Regrese a la página de inicio y haga clic en **Iniciar instalación**.
- e. En el Administrador de cuadrícula: si el nodo figura en la tabla Nodos aprobados, elimine el nodo.
- f. Eliminar el nodo de la tabla Nodos pendientes.
- g. Espere a que el nodo vuelva a aparecer en la lista de Nodos pendientes.
- h. Confirme que puede configurar las redes adecuadas. Ya deberían estar completados con la información proporcionada en la página de Configuración de IP del Instalador del dispositivo.

Para obtener información adicional, consulte la ["Inicio rápido para la instalación de hardware"](#) para localizar instrucciones para su electrodoméstico.

8. Haga clic en **Guardar**.

La entrada del nodo de la cuadrícula se mueve a la lista de Nodos aprobados.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

Approve

Remove

Search

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
No results found.				

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

		✖ Remove		Search		
Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address	
☐ 00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21	
☐ 00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21	
☐ 00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21	
☐ 00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21	
☐ 00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21	
☐ 50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21	

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

Debes aprobar todos los nodos que quieras en la red. Sin embargo, puede regresar 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 los nodos de la cuadrícula, haga clic en **Siguiente**.

Especifique la información del servidor de Protocolo de tiempo de red

Debe especificar la información de configuración del Protocolo de tiempo de red (NTP) para el sistema StorageGRID , de modo que las operaciones realizadas en servidores separados puedan mantenerse sincronizadas.

Acerca de esta tarea

Debe especificar direcciones IPv4 para los servidores NTP.

Debe especificar servidores NTP externos. Los servidores NTP especificados deben utilizar el protocolo NTP.

Debe especificar cuatro referencias de servidor NTP de Stratum 3 o superior para evitar problemas con la diferencia horaria.



Al especificar la fuente NTP externa para una instalación de 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 hora en versiones anteriores de Windows no es lo suficientemente preciso y Microsoft no lo admite para su uso en entornos de alta precisión, como StorageGRID.

"Límite de soporte para configurar el servicio de hora de Windows para entornos de alta precisión"

Los servidores NTP externos son utilizados por los nodos a los que previamente les asignó roles NTP primarios.



Asegúrese de que al menos dos nodos en cada sitio puedan acceder al menos a cuatro fuentes NTP externas. Si solo un nodo en un sitio puede acceder a las fuentes NTP, se producirán problemas de sincronización si ese nodo deja de funcionar. Además, designar dos nodos por sitio como fuentes NTP primarias garantiza una sincronización precisa si un sitio está aislado del resto de la red.

Realice comprobaciones adicionales para VMware, como asegurarse de que el hipervisor use la misma fuente NTP que la máquina virtual y usar VMTools para deshabilitar la sincronización horaria entre el hipervisor y las máquinas virtuales StorageGRID .

Pasos

1. Especifique las direcciones IPv4 de 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 de servidor adicionales.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

Summary

Network Time Protocol

Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync.

Server 1

10.60.248.183

Server 2

10.227.204.142

Server 3

10.235.48.111

Server 4

0.0.0.0

+

3. Seleccione **Siguiente**.

Especificar la información del servidor DNS

Debe especificar la información de DNS para su sistema StorageGRID , de modo que pueda acceder a servidores externos utilizando nombres de host en lugar de direcciones IP.

Acerca de esta tarea

Especificando ["Información del servidor DNS"](#) le permite utilizar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP para notificaciones por correo electrónico y AutoSupport.

Para garantizar un funcionamiento correcto, especifique dos o tres servidores DNS. Si especifica más de tres, es posible que solo se utilicen tres debido a las limitaciones conocidas del sistema operativo en algunas plataformas. Si tiene restricciones de enrutamiento en su entorno, puede ["personalizar la lista de servidores DNS"](#) para que los nodos individuales (normalmente todos los nodos de un sitio) utilicen un conjunto diferente de hasta tres servidores DNS.

Si es posible, utilice servidores DNS a los que cada sitio pueda acceder localmente para garantizar que un sitio aislado pueda resolver los FQDN para destinos externos.

Pasos

1. Especifique la dirección IPv4 de 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 de servidor adicionales.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there's a blue header with "NetApp® StorageGRID®" and a "Help" link. Below the header is a progress bar with eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS (highlighted in blue), 7. Passwords, and 8. Summary. Below the progress bar, the "Domain Name Service" section is active. It contains a text box with instructions: "Enter the IP address for at least one Domain Name System (DNS) server, so that server hostnames can be used instead of IP addresses. Specifying at least two DNS servers is recommended. Configuring DNS enables server connectivity, email notifications, and NetApp AutoSupport." Below this, there are two input fields for DNS servers. "Server 1" has the IP address "10.224.223.130" and a red "X" icon to its right. "Server 2" has the IP address "10.224.223.136" and a red "+ X" icon to its right, indicating that more servers can be added.

La mejor práctica 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 de su sistema StorageGRID , deberá ingresar las contraseñas que se utilizarán para proteger su sistema y realizar tareas de mantenimiento.

Acerca de esta tarea

Utilice la página **Instalar contraseñas** para especificar la frase de contraseña de aprovisionamiento y la contraseña del usuario raíz de administración de la red.

- La frase de contraseña de aprovisionamiento se utiliza como clave de cifrado y no la almacena el sistema StorageGRID .
- Debe tener la contraseña de aprovisionamiento para los procedimientos de instalación, expansión y mantenimiento, incluida la descarga del paquete de recuperación. Por lo tanto, es importante que guardes la contraseña de aprovisionamiento en una ubicación segura.
- Puede cambiar la contraseña de aprovisionamiento desde el Administrador de Grid si tiene la actual.
- La contraseña del usuario raíz de administración de la red se puede cambiar mediante el Administrador de red.
- Las contraseñas de la consola de línea de comandos generadas aleatoriamente y de SSH se almacenan en el `Passwords.txt` archivo en el paquete de recuperación.

Pasos

1. En **Frase de contraseña de aprovisionamiento**, ingrese la frase de contraseña de aprovisionamiento que será necesaria para realizar cambios en la topología de la red de su sistema StorageGRID .

Guarde la contraseña de aprovisionamiento en un lugar seguro.



Si después de completarse la instalación desea cambiar la contraseña de aprovisionamiento más tarde, puede utilizar el Administrador de Grid. Seleccione **CONFIGURACIÓN > Control de acceso > Contraseñas de red**.

2. En **Confirmar contraseña de aprovisionamiento**, vuelva a ingresar la contraseña de aprovisionamiento para confirmarla.
3. En **Contraseña de usuario raíz de administración de red**, ingrese la contraseña que se utilizará para acceder al Administrador de red como usuario "root".

Guarde la contraseña en un lugar seguro.

4. En **Confirmar contraseña de usuario root**, vuelva a ingresar la contraseña de Grid Manager para confirmarla.

NetApp® StorageGRID®
Help

Install

1 License
2 Sites
3 Grid Network
4 Grid Nodes
5 NTP
6 DNS
7 Passwords
8 Summary

Passwords

Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step.

Provisioning
Passphrase

Confirm
Provisioning
Passphrase

Grid Management
Root User
Password

Confirm Root User
Password

☒ Create random command line passwords.

- Si está instalando una cuadrícula para fines de prueba de concepto o demostración, opcionalmente desmarque la casilla de verificación **Crear contraseñas de línea de comando aleatorias**.

Para las implementaciones de producción, siempre se deben utilizar contraseñas aleatorias por razones de seguridad. Borre **Crear contraseñas de línea de comando aleatorias** solo para cuadrículas de demostración si desea usar contraseñas predeterminadas para acceder a los nodos de la cuadrícula desde la línea de comando usando la cuenta "root" o "admin".



Se le solicitará que descargue el archivo del paquete de recuperación(`sgws-recovery-package-id-revision.zip`) después de hacer clic en **Instalar** en la página Resumen. Usted debe ["descargar este archivo"](#) para completar la instalación. Las contraseñas necesarias para acceder al sistema se almacenan en el `Passwords.txt` archivo, contenido en el archivo del paquete de recuperación.

- Haga clic en **Siguiente**.

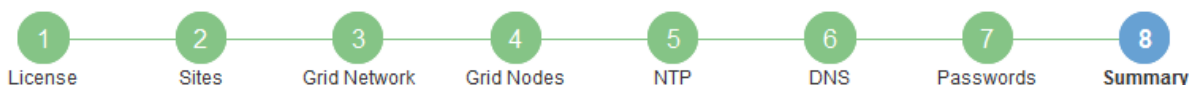
Revise su configuración y complete la instalación

Debe revisar cuidadosamente la información de configuración que ha ingresado para asegurarse de que la instalación se complete correctamente.

Pasos

- Ver la página **Resumen**.

Install



Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name	Grid1	Modify License
Passwords	Auto-generated random command line passwords	Modify Passwords

Networking

NTP	10.60.248.183 10.227.204.142 10.235.48.111	Modify NTP
DNS	10.224.223.130 10.224.223.136	Modify DNS
Grid Network	172.16.0.0/21	Modify Grid Network

Topology

Topology	Atlanta	Modify Sites	Modify Grid Nodes
	Raleigh		
	dc1-adm1	dc1-g1	dc1-s1
	dc1-s2	dc1-s3	NetApp-SGA

2. Verifique que toda la información de configuración de la red sea correcta. Utilice los enlaces Modificar en la página Resumen para volver atrás y corregir cualquier error.
3. Haga clic en **Instalar**.



Si un nodo está configurado para usar la red del cliente, la puerta de enlace predeterminada para ese nodo cambia de la red de cuadrícula a la red del cliente cuando hace clic en **Instalar**. Si pierde la conectividad, debe asegurarse de acceder al nodo de administración principal a través de una subred accesible. Ver "[Pautas para establecer redes](#)" Para más detalles.

4. Haga clic en **Descargar paquete de recuperación**.

Cuando la instalación avanza hasta el punto donde se define la topología de la red, se le solicitará que descargue el archivo del paquete de recuperación(.zip) y confirme que puede acceder correctamente al contenido de este archivo. Debe descargar el archivo del paquete de recuperación para poder recuperar el sistema StorageGRID si uno o más nodos de la red fallan. La instalación continúa en segundo plano, pero no puede completar la instalación ni acceder al sistema StorageGRID hasta que descargue y verifique este archivo.

5. Verifique que pueda extraer el contenido del .zip archivo y luego guárdelo en dos ubicaciones seguras, protegidas y separadas.



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

6. Seleccione la casilla de verificación **He descargado y verificado correctamente el archivo del paquete de recuperación** y haga clic en **Siguiente**.

Si la instalación aún está en curso, aparecerá la página de estado. Esta página indica el progreso de la instalación para cada nodo de la red.

Installation Status

If necessary, you may [Download the Recovery Package file](#) again.

Name	IT	Site	IT	Grid Network IPv4 Address	Progress	IT	Stage	IT
dc1-adm1		Site1		172.16.4.215/21			Starting services	
dc1-g1		Site1		172.16.4.216/21			Complete	
dc1-s1		Site1		172.16.4.217/21			Waiting for Dynamic IP Service peers	
dc1-s2		Site1		172.16.4.218/21			Downloading hotfix from primary Admin if needed	
dc1-s3		Site1		172.16.4.219/21			Downloading hotfix from primary Admin if needed	

Cuando se alcanza la etapa Completado para todos los nodos de la red, aparece la página de inicio de sesión del Administrador de la red.

7. Sign in en Grid Manager utilizando el usuario "root" y la contraseña que especificó durante la instalación.

Pautas posteriores a la instalación

Después de completar la implementación y configuración del nodo de la red, siga estas pautas para el direccionamiento DHCP y los cambios de configuración de red.

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

Sólo se puede configurar DHCP durante la fase de implementación. No se puede configurar DHCP durante la configuración.



Los nodos se reinician cuando la configuración de la red Grid se modifica mediante DHCP, lo que puede provocar interrupciones si un cambio de DHCP afecta a varios nodos al mismo tiempo.

- Debe utilizar los procedimientos de Cambio de IP si desea cambiar direcciones IP, máscaras de subred y puertas de enlace predeterminadas para un nodo de la red. Ver "[Configurar direcciones IP](#)".
- Si realiza cambios en la configuración de red, incluidos cambios de enrutamiento y puerta de enlace, es posible que se pierda la conectividad del cliente con el nodo de administración principal y otros nodos de la red. Dependiendo de los cambios de red aplicados, es posible que sea necesario restablecer estas conexiones.

Instalación API REST

StorageGRID proporciona la API de instalación de StorageGRID para realizar tareas de instalación.

La API utiliza la plataforma API de código abierto Swagger para proporcionar la documentación de la API. Swagger permite que tanto los desarrolladores como los no desarrolladores interactúen con la API en una interfaz de usuario que ilustra cómo la API responde a los parámetros y opciones. Esta documentación asume que está familiarizado con las tecnologías web estándar y el formato de datos JSON.



Cualquier operación de API que realice utilizando la página web de Documentación de API son operaciones en vivo. 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, cualquier parámetro de URL obligatorio u opcional y una respuesta de API esperada.

API de instalación de StorageGRID

La API de instalación de StorageGRID solo está disponible cuando configura inicialmente su sistema StorageGRID y si necesita realizar una recuperación del nodo de administración principal. Se puede acceder a la API de instalación a través de HTTPS desde Grid Manager.

Para acceder a la documentación de la API, vaya a la página web de instalación en el nodo de administración principal y seleccione **Ayuda > Documentación de la API** en la barra de menú.

La API de instalación de StorageGRID incluye las siguientes secciones:

- **config** – Operaciones relacionadas con el lanzamiento del producto y las versiones de la API. Puede enumerar la versión de lanzamiento del producto y las versiones principales de la API compatibles con esa versión.
- **grid** – Operaciones de configuración a nivel de cuadrícula. Puede obtener y actualizar la configuración de la red, incluidos los detalles de la red, las subredes de la red, las contraseñas de la red y las direcciones IP del servidor NTP y DNS.
- **nodos** – Operaciones de configuración a nivel de nodo. Puede recuperar una lista de nodos de la cuadrícula, eliminar un nodo de la cuadrícula, configurar un nodo de la cuadrícula, ver un nodo de la cuadrícula y restablecer la configuración de un nodo de la cuadrícula.
- **provision** – 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.
- **recovery-package** – Operaciones para descargar el paquete de recuperación.
- **sitios** – Operaciones de configuración a nivel de sitio. Puede crear, ver, eliminar y modificar un sitio.
- **temporary-password** – Operaciones en la contraseña temporal para proteger la mgmt-api durante la instalación.

¿A dónde ir después?

Después de completar una instalación, realice las tareas de integración y configuración necesarias. Puede realizar las tareas opcionales según sea necesario.

Tareas requeridas

- Configurar VMware vSphere Hypervisor para reinicio automático.

Debe configurar el hipervisor para reiniciar las máquinas virtuales cuando se reinicie el servidor. Sin un reinicio automático, las máquinas virtuales y los nodos de la red permanecen apagados después de que se reinicia el servidor. Para obtener más detalles, consulte la documentación de VMware vSphere Hypervisor.

- ["Crear una cuenta de inquilino"](#) para el protocolo de cliente S3 que se utilizará para almacenar objetos en su sistema StorageGRID .
- ["Acceso al sistema de control"](#) mediante la configuración de grupos y cuentas de usuario. Opcionalmente, puedes ["configurar una fuente de identidad federada"](#) (como Active Directory o OpenLDAP), para que pueda importar grupos de administración y usuarios. O bien, puedes ["crear grupos y usuarios locales"](#) .
- Integrar y probar el ["S3 API"](#) aplicaciones cliente que utilizará para cargar objetos en su sistema StorageGRID .
- ["Configurar las reglas de gestión del ciclo de vida de la información \(ILM\) y la política de ILM"](#) que desea utilizar para proteger los datos del objeto.
- Si su instalación incluye nodos de almacenamiento de dispositivos, utilice SANtricity OS para completar las siguientes tareas:
 - Conéctese a cada dispositivo StorageGRID .
 - Verificar la recepción de datos de AutoSupport .

Ver ["Configurar el hardware"](#) .

- Revisar y seguir las ["Pautas de fortalecimiento del sistema StorageGRID"](#) para eliminar riesgos de seguridad.
- ["Configurar notificaciones por correo electrónico para alertas del sistema"](#) .

Tareas opcionales

- ["Actualizar las direcciones IP de los nodos de la red"](#) si han cambiado desde que planificó su implementación y generó el paquete de recuperación.
- ["Configurar el cifrado de almacenamiento"](#), si es necesario.
- ["Configurar la compresión de almacenamiento"](#) para reducir el tamaño de los objetos almacenados, si es necesario.
- ["Configurar interfaces VLAN"](#) para aislar y particionar el tráfico de la red, si es necesario.
- ["Configurar grupos de alta disponibilidad"](#) para mejorar la disponibilidad de la conexión para los clientes Grid Manager, Tenant Manager y S3, si es necesario.
- ["Configurar los puntos finales del balanceador de carga"](#) para la conectividad del cliente S3, si es necesario.

Solucionar problemas de instalación

Si ocurre algún problema durante la instalación del sistema StorageGRID , puede acceder a los archivos de registro de instalación.

Los siguientes son los principales archivos de registro de instalación que el soporte técnico podría necesitar para resolver problemas.

- `/var/local/log/install.log` (se encuentra en todos los nodos de la red)
- `/var/local/log/gdu-server.log` (se encuentra en el nodo de administración principal)

Información relacionada

Para saber cómo acceder a los archivos de registro, consulte ["Referencia de archivos de registro"](#) .

Si necesita ayuda adicional, póngase en contacto con ["Soporte de NetApp"](#) .

La reserva de recursos de la máquina virtual requiere un ajuste

Los archivos OVF incluyen una reserva de recursos diseñada para garantizar que cada nodo de la red tenga suficiente RAM y CPU para funcionar de manera eficiente. Si crea máquinas virtuales implementando estos archivos OVF en VMware y la cantidad predefinida de recursos no está disponible, las máquinas virtuales no se iniciarán.

Acerca de esta tarea

Si está seguro de que el host de la máquina virtual tiene recursos suficientes para cada nodo de la red, ajuste manualmente los recursos asignados para cada máquina virtual y luego intente iniciar las máquinas virtuales.

Pasos

1. En el árbol de clientes de VMware vSphere Hypervisor, seleccione la máquina virtual que no está iniciada.
2. Haga clic derecho en la máquina virtual y seleccione **Editar configuración**.
3. Desde la ventana Propiedades de máquinas virtuales, seleccione la pestaña **Recursos**.
4. Ajustar los recursos asignados a la máquina virtual:
 - a. Seleccione **CPU** y luego utilice el control deslizante Reserva para ajustar los MHz reservados para esta máquina virtual.
 - b. Seleccione **Memoria** y luego utilice el control deslizante Reserva para ajustar los MB reservados para esta máquina virtual.
5. Haga clic en **Aceptar**.
6. Repita según sea necesario para otras máquinas virtuales alojadas en el mismo host de VM.

La contraseña de instalación temporal fue deshabilitada

Al implementar un nodo VMware, puede especificar opcionalmente una contraseña de instalación temporal. Debe tener esta contraseña para acceder a la consola de la VM o usar SSH antes de que el nuevo nodo se una a la red.

Si optó por deshabilitar la contraseña de instalación temporal, deberá realizar pasos adicionales para depurar problemas de instalación.

Puede realizar cualquiera de las siguientes acciones:

- Vuelva a implementar la máquina virtual, pero especifique una contraseña de instalación temporal para poder acceder a la consola o usar SSH para depurar problemas de instalación.
- Utilice vCenter para establecer la contraseña:
 - a. Apague la máquina virtual.
 - b. Vaya a **VM**, seleccione la pestaña **Configurar** y seleccione **Opciones de vApp**.
 - c. Especifique el tipo de contraseña de instalación temporal que desea establecer:
 - Seleccione **CUSTOM_TEMPORARY_PASSWORD** para establecer una contraseña temporal personalizada.
 - Seleccione **TEMPORARY_PASSWORD_TYPE** para utilizar el nombre del nodo como contraseña temporal.
 - d. Seleccione **Establecer valor**.

- e. Establecer la contraseña temporal:
 - Cambie **CUSTOM_TEMPORARY_PASSWORD** por un valor de contraseña personalizado.
 - Actualice **TEMPORARY_PASSWORD_TYPE** con el valor **Use node name**.
- f. Reinicie la máquina virtual para aplicar la nueva contraseña.

Actualizar el software StorageGRID

Actualizar el software StorageGRID

Utilice estas instrucciones para actualizar un sistema StorageGRID a una nueva versión.

Cuando realiza la actualización, se actualizan todos los nodos de su sistema StorageGRID .

Antes de empezar

Revise estos temas para conocer las nuevas características y mejoras en StorageGRID 11.9, determinar si alguna característica ha quedado obsoleta o se ha eliminado y obtener información sobre los cambios en las API de StorageGRID .

- ["Novedades de StorageGRID 11.9"](#)
- ["Funciones eliminadas o en desuso"](#)
- ["Cambios en la API de administración de la red"](#)
- ["Cambios en la API de administración de inquilinos"](#)

Novedades de StorageGRID 11.9

Esta versión de StorageGRID presenta las siguientes características y cambios funcionales.

Escalabilidad

Nodos de almacenamiento de solo datos

Para permitir un escalamiento más granular, ahora puede instalar ["Nodos de almacenamiento de solo datos"](#) . Cuando el procesamiento de metadatos no es crítico, puede optimizar su infraestructura de manera rentable. Esta flexibilidad ayuda a adaptarse a distintas cargas de trabajo y patrones de crecimiento.

Mejoras en el grupo de almacenamiento en la nube

Roles de IAM en cualquier lugar

StorageGRID ahora admite credenciales a corto plazo utilizando ["Roles de IAM en cualquier lugar en Amazon S3 para grupos de almacenamiento en la nube"](#) .

El uso de credenciales a largo plazo para acceder a los buckets S3 plantea riesgos de seguridad si dichas credenciales se ven comprometidas. Las credenciales a corto plazo tienen una vida útil limitada, lo que reduce el riesgo de acceso no autorizado.

Bloqueos de objetos S3

Ahora puedes ["Configurar un grupo de almacenamiento en la nube mediante un punto final de Amazon S3"](#) . S3 Object Lock ayuda a prevenir la eliminación accidental o maliciosa de objetos. Si organiza datos desde StorageGRID a Amazon S3, tener el bloqueo de objetos habilitado en ambos sistemas mejora la protección de datos durante todo el ciclo de vida de los datos.

Multi-tenencia

Límites de cubo

Por ["Establecer límites en los buckets S3"](#) , puedes evitar que los inquilinos monopolicen la capacidad. Además, el crecimiento descontrolado puede generar costos inesperados. Al tener límites definidos, podrás estimar mejor los gastos de almacenamiento del inquilino.

5.000 cubos por inquilino

Para mejorar la escalabilidad, StorageGRID ahora admite hasta ["5000 depósitos S3 por inquilino"](#) . Cada cuadrícula puede tener un máximo de 100.000 contenedores.

Para soportar 5000 buckets, cada nodo de almacenamiento en la red debe tener un mínimo de 64 GB de RAM.

Mejoras en el bloqueo de objetos S3

Las capacidades de configuración por inquilino proporcionan el equilibrio adecuado entre flexibilidad y seguridad de los datos. Ahora puede configurar los ajustes de retención por inquilino para:

- Permitir o no permitir el modo de cumplimiento
- Establecer un período máximo de retención

Referirse a:

- ["Administrar objetos con S3 Object Lock"](#)
- ["Cómo los administradores de red controlan la retención de objetos"](#)
- ["Crear una cuenta de inquilino"](#)

Compatibilidad con S3

suma de comprobación x-amz-checksum-sha256

- La API REST de S3 ahora proporciona soporte para el enlace: `.../s3/operations-on-objects.html[x-amz-checksum-sha256 suma de comprobación]`.
- StorageGRID ahora proporciona compatibilidad con sumas de comprobación SHA-256 para operaciones PUT, GET y HEAD. Estas sumas de comprobación mejoran la integridad de los datos.

Cambios en la compatibilidad del protocolo S3

- Se agregó soporte para Mountpoint para Amazon S3, que permite que las aplicaciones se conecten directamente a los buckets S3 como si fueran sistemas de archivos locales. Ahora puede utilizar StorageGRID con más aplicaciones y más casos de uso.
- Como parte de la incorporación de compatibilidad con Mountpoint, StorageGRID 11.9 contiene ["cambios adicionales en la compatibilidad del protocolo S3"](#) .

Mantenimiento y soporte

AutoSupport

["AutoSupport"](#) Ahora crea automáticamente casos de falla de hardware para dispositivos heredados.

Operaciones de clonación de nodos expandidas

Se ha ampliado la usabilidad de los clones de nodos para admitir nodos de almacenamiento más grandes.

Manejo mejorado de marcadores de eliminación vencidos por parte de ILM

Las reglas de tiempo de ingesta de ILM con un período de tiempo de días ahora también eliminan los marcadores de eliminación de objetos vencidos. Los marcadores de eliminación solo se eliminan cuando ha transcurrido un período de tiempo de días y el creador de eliminación actual ha expirado (no hay versiones no actuales).

Referirse a ["Cómo se eliminan los objetos versionados de S3"](#) y ["Ejemplo de cómo el ciclo de vida del bucket tiene prioridad sobre la política de ILM"](#).

Desmantelamiento de nodos mejorado

Para proporcionar una transición fluida y eficiente al hardware de próxima generación de StorageGRID, ["desmantelamiento de nodos"](#) Se ha mejorado.

Registro del sistema para puntos finales del balanceador de carga

Los registros de acceso a los puntos finales del equilibrador de carga contienen información de solución de problemas, como códigos de estado HTTP. StorageGRID ahora es compatible ["exportar estos registros a un servidor syslog externo"](#). Esta mejora permite una gestión de registros más eficiente y la integración con los sistemas de monitoreo y alerta existentes.

Mejoras adicionales para el mantenimiento y la capacidad de soporte

- Actualización de la interfaz de usuario de métricas
- Nuevas calificaciones del sistema operativo
- Compatibilidad con nuevos componentes de terceros

Seguridad

Rotación de claves de acceso SSH

Los administradores de red ahora pueden ["actualizar y rotar claves SSH"](#). La capacidad de rotar claves SSH es una práctica recomendada de seguridad y un mecanismo de defensa proactivo.

Alertas para inicios de sesión root

Cuando una entidad desconocida inicia sesión en el Administrador de Grid como raíz, ["se activa una alerta"](#). Monitorear los inicios de sesión SSH raíz es un paso proactivo hacia la protección de su infraestructura.

Mejoras de Grid Manager

Se movió la página de perfiles de codificación de borrado

La página de perfiles de codificación de borrado ahora se encuentra en **CONFIGURACIÓN > Sistema > Codificación de borrado**. Solía estar en el menú de ILM.

Mejoras en la búsqueda

El ["campo de búsqueda en el Administrador de cuadrícula"](#) Ahora incluye una mejor lógica de coincidencia, lo que le permite encontrar páginas buscando abreviaturas comunes y por los nombres de ciertas configuraciones dentro de una página. También puede buscar más tipos de elementos, como nodos, usuarios y cuentas de inquilinos.

Funciones y capacidades eliminadas o en desuso

Algunas características y capacidades fueron eliminadas o quedaron obsoletas en esta versión. Revise estos elementos para comprender si necesita actualizar las aplicaciones cliente o modificar su configuración antes de actualizar.

Definiciones

Obsoleto

Esta función **no debería** utilizarse en nuevos entornos de producción. Los entornos de producción existentes pueden seguir utilizando la función.

Fin de la vida

Última versión enviada que admite la función. En algunos casos, es posible que se elimine la documentación de la función en esta etapa.

Remoto

Primera versión que **no** admite la función.

Fin del soporte de funciones de StorageGRID

Las funciones obsoletas se eliminarán en N+2 versiones principales. Por ejemplo, si una característica queda obsoleta en la versión N (por ejemplo, 6.3), la última versión donde existirá dicha característica será N+1 (por ejemplo, 6.4). La versión N+2 (por ejemplo, 6.5) es el primer lanzamiento cuando la función no existe en el producto.

Ver el ["Página de soporte de versiones de software"](#) Para obtener información adicional.



En determinadas situaciones, NetApp podría finalizar el soporte para funciones específicas antes de lo indicado.

Característica	Obsoleto	Fin de la vida	Remoto	Enlaces a documentación anterior
Alarmas heredadas (no alertas)	11,7	11,8	11,9	"Referencia de alarmas (StorageGRID 11.8)"

Característica	Obsoleto	Fin de la vida	Remoto	Enlaces a documentación anterior
Compatibilidad con nodos de archivo	11,7	11,8	11,9	"Consideraciones para el desmantelamiento de nodos de archivo (StorageGRID 11.8)" Nota: Antes de comenzar la actualización, debes: 1. Desactivar todos los nodos de archivo. Ver "Desmantelamiento de nodos de red (sitio de documentación de StorageGRID 11.8)" . 2. Eliminar todas las referencias de nodo de archivo de los grupos de almacenamiento y las políticas de ILM. Ver "Base de conocimientos de NetApp : Guía de resolución de la actualización del software StorageGRID 11.9" .
Exportación de auditoría a través de CIFS/Samba	11,1	11,6	11,7	
Servicio CLB	11,4	11,6	11,7	
Motor de contenedores Docker	11,8	11,9	Por determinar	La compatibilidad con Docker como motor de contenedores para implementaciones de solo software está obsoleta. Docker será reemplazado por otro motor de contenedores en una versión futura. Consulte la "Lista de versiones de Docker compatibles actualmente" .
Exportación de auditoría de NFS	11,8	11,9	12,0	"Configurar el acceso del cliente de auditoría para NFS (StorageGRID 11.8)"
Compatibilidad con la API de Swift	11,7	11,9	12,0	"Utilice la API REST de Swift (StorageGRID 11.8)"
RHEL 8.8	11,9	11,9	12,0	
RHEL 9.0	11,9	11,9	12,0	
RHEL 9.2	11,9	11,9	12,0	

Característica	Obsoleto	Fin de la vida	Remoto	Enlaces a documentación anterior
Ubuntu 18,04	11,9	11,9	12,0	
Ubuntu 20,04	11,9	11,9	12,0	
Debian 11	11,9	11,9	12,0	

Consulte también:

- ["Cambios en la API de administración de la red"](#)
- ["Cambios en la API de administración de inquilinos"](#)

Cambios en la API de administración de la red

StorageGRID 11.9 utiliza la versión 4 de la API de administración de Grid. La versión 4 deja obsoleta la versión 3; sin embargo, las versiones 1, 2 y 3 aún son compatibles.



Puede seguir usando versiones obsoletas de la API de administración con StorageGRID 11.9; sin embargo, la compatibilidad con estas versiones de la API se eliminará en una futura versión de StorageGRID. Después de actualizar a StorageGRID 11.9, puede desactivar las API obsoletas mediante el uso de `PUT /grid/config/management API`.

Para obtener más información, visite ["Utilice la API de gestión de red"](#).

Revisar la configuración de cumplimiento después de habilitar el bloqueo global de objetos S3

Revise la configuración de cumplimiento de los inquilinos existentes después de habilitar la configuración global de Bloqueo de objetos S3. Cuando habilita esta configuración, las configuraciones de bloqueo de objetos S3 por inquilino dependen de la versión de StorageGRID en el momento en que se creó el inquilino.

Solicitudes de mgmt-api heredadas eliminadas

Se han eliminado estas solicitudes heredadas:

`/grid/server-types`

`/grid/ntp-roles`

Cambios en `GET /private/storage-usage` API

- Una nueva propiedad, `usageCacheDuration`, se ha agregado al cuerpo de la respuesta. Esta propiedad especifica la duración (en segundos) durante la cual la caché de búsqueda de uso permanece válida. Este valor se aplica al verificar el uso frente a la cuota de almacenamiento del inquilino y los límites de capacidad del depósito.
- El `GET /api/v4/private/storage-usage` Se ha corregido el comportamiento para que coincida con la anidación del esquema.
- Estos cambios se aplican únicamente a la API privada.

Cambios en GET `cross-grid-replication` API

La API GET `/org/containers/:name/cross-grid-replication` ya no requiere acceso `root(rootAccess)` permiso; sin embargo, debe pertenecer a un grupo de usuarios que tenga el permiso `Administrar todos los depósitos(manageAllContainers)` o `Ver todos los depósitos(viewAllContainers)` permiso.

La API PUT `/org/containers/:name/cross-grid-replication` no ha cambiado y aún requiere acceso `root(rootAccess)` permiso.

Cambios en la API de administración de inquilinos

StorageGRID 11.9 utiliza la versión 4 de la API de administración de inquilinos. La versión 4 deja obsoleta la versión 3; sin embargo, las versiones 1, 2 y 3 aún son compatibles.



Puede seguir usando versiones obsoletas de la API de administración de inquilinos con StorageGRID 11.9; sin embargo, la compatibilidad con estas versiones de la API se eliminará en una futura versión de StorageGRID. Después de actualizar a StorageGRID 11.9, puede desactivar las API obsoletas mediante el uso de PUT `/grid/config/management` API.

Para obtener más información, visite ["Comprenda la API de administración de inquilinos"](#).

Nueva API para el límite de capacidad del bucket

Puedes utilizar el `/org/containers/{bucketName}/quota-object-bytes` API con operaciones GET/PUT para obtener y establecer el límite de capacidad de almacenamiento para un depósito.

Planifique y prepárese para la actualización

Calcule el tiempo necesario para completar una actualización

Considere cuándo actualizar, en función de cuánto tiempo podría llevar la actualización. Tenga en cuenta qué operaciones puede y no puede realizar durante cada etapa de la actualización.

Acerca de esta tarea

El tiempo necesario para completar una actualización de StorageGRID depende de una variedad de factores, como la carga del cliente y el rendimiento del hardware.

La tabla resume las principales tareas de actualización y enumera el tiempo aproximado necesario para cada tarea. Los pasos después de la tabla proporcionan instrucciones que puede utilizar para estimar el tiempo de actualización de su sistema.

Tarea de actualización	Descripción	Tiempo aproximado requerido	Durante esta tarea
Ejecutar comprobaciones previas y actualizar el nodo de administración principal	Se ejecutan las comprobaciones previas de actualización y se detiene, se actualiza y se reinicia el nodo de administración principal.	De 30 minutos a 1 hora, siendo los nodos de dispositivos de servicios los que requieren la mayor parte del tiempo. Esta vez aumentarán los errores de comprobación previa no resueltos.	No puede acceder al nodo de administración principal. Es posible que se informen errores de conexión que puedes ignorar. Ejecutar las comprobaciones previas de actualización antes de iniciar la actualización le permite resolver cualquier error antes de la ventana de mantenimiento de actualización programada.
Iniciar el servicio de actualización	Se distribuye el archivo de software y se inicia el servicio de actualización.	3 minutos por nodo de la red	
Actualizar otros nodos de la red	El software de todos los demás nodos de la red se actualiza en el orden en el que usted aprueba los nodos. Cada nodo de su sistema se desactivará uno a la vez.	De 15 minutos a 1 hora por nodo, y los nodos de dispositivos son los 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. • No puede realizar otros procedimientos de mantenimiento, como revisiones, desmantelamiento o expansión. Nota: Si necesita realizar una recuperación, comuníquese con el soporte técnico.
Habilitar funciones	Las nuevas funciones de la nueva versión están habilitadas.	Menos de 5 minutos	• No cambie la configuración de la cuadrícula. • No cambie la configuración del nivel de auditoría. • No actualice la configuración de ILM. • No puede realizar otro procedimiento de mantenimiento.

Tarea de actualización	Descripción	Tiempo aproximado requerido	Durante esta tarea
Actualizar la base de datos	El proceso de actualización verifica cada nodo para verificar que no sea necesario actualizar la base de datos de Cassandra.	10 segundos por nodo o unos minutos para toda la red	La actualización de StorageGRID 11.8 a 11.9 no requiere una actualización de la base de datos Cassandra; sin embargo, el servicio Cassandra se detendrá y se reiniciará en cada nodo de almacenamiento. Para futuras versiones de funciones de StorageGRID, el paso de actualización de la base de datos de Cassandra podría demorar varios días en completarse.
Pasos finales de la actualización	Se eliminan los archivos temporales y se completa la actualización a la nueva versión.	5 minutos	Cuando se complete la tarea Pasos finales de actualización , podrá realizar todos los procedimientos de mantenimiento.

Pasos

1. Calcule el tiempo necesario para actualizar todos los nodos de la red.
 - a. Multiplique la cantidad 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. Agregue 1 hora a este tiempo para tener en cuenta el tiempo necesario para descargar el .upgrade archivo, ejecutar validaciones de verificación previa y completar los pasos finales de actualización.
2. Si tiene nodos Linux, agregue 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 sumando los resultados de los pasos 1 y 2.

Ejemplo: Tiempo estimado para actualizar a StorageGRID 11.9

Supongamos que su sistema tiene 14 nodos de red, de los cuales 8 son nodos Linux.

1. Multiplica 14 por 1 hora/nodo.
2. Agregue 1 hora para tener en cuenta la descarga, la verificación previa y los pasos finales.

El tiempo estimado para actualizar todos los nodos es de 15 horas.

3. Multiplique 8 por 15 minutos/nodo para tener en cuenta el tiempo necesario para instalar el paquete RPM o DEB en los nodos Linux.

El tiempo estimado para este paso es de 2 horas.

4. Suma los valores juntos.

Debe esperar hasta 17 horas para completar la actualización de su sistema a StorageGRID 11.9.0.



Según sea necesario, puede dividir la ventana de mantenimiento en ventanas más pequeñas aprobando subconjuntos de nodos de la red para actualizar en múltiples sesiones. Por ejemplo, es posible que prefiera actualizar los nodos del sitio A en una sesión y luego actualizar los nodos del sitio B en una sesión posterior. Si decide realizar la actualización en más de una sesión, tenga en cuenta que no podrá comenzar a usar las nuevas funciones hasta que se hayan actualizado todos los nodos.

Cómo se ve afectado su sistema durante la actualización

Conozca cómo se verá afectado su sistema StorageGRID durante la actualización.

Las actualizaciones de StorageGRID no son disruptivas

El sistema StorageGRID puede ingerir y recuperar datos de las aplicaciones cliente durante todo el proceso de actualización. Si aprueba que todos los nodos del mismo tipo se actualicen (por ejemplo, nodos de almacenamiento), los nodos se desactivan uno a la vez, por lo que no hay ningún momento en el que todos los nodos de la red o todos los nodos de la red de un determinado tipo no estén disponibles.

Para permitir la disponibilidad continua, asegúrese de que su política ILM contenga reglas que especifiquen el almacenamiento de múltiples copias de cada objeto. También debe asegurarse de que todos los clientes S3 externos estén configurados para enviar solicitudes a uno de los siguientes:

- Una dirección IP virtual de grupo de alta disponibilidad (HA)
- Un balanceador de carga de terceros de alta disponibilidad
- Múltiples nodos de puerta de enlace para cada cliente
- Múltiples nodos de almacenamiento para cada cliente

Las aplicaciones cliente podrían experimentar interrupciones a corto plazo

El sistema StorageGRID puede ingerir y recuperar datos de las aplicaciones cliente durante todo el proceso de actualización; sin embargo, las conexiones de los clientes a los nodos de puerta de enlace o nodos de almacenamiento individuales pueden interrumpirse temporalmente si la actualización necesita reiniciar los servicios en esos nodos. La conectividad se restablecerá una vez que se complete el proceso de actualización y se reanuden los servicios en los nodos individuales.

Es posible que sea necesario programar un tiempo de inactividad para aplicar una actualización si la pérdida de conectividad por un período breve no es aceptable. Puede utilizar la aprobación selectiva para programar cuándo se actualizan determinados nodos.



Puede utilizar varias puertas de enlace y grupos de alta disponibilidad (HA) para proporcionar conmutación por error automática durante el proceso de actualización. Vea las instrucciones para ["configuración de grupos de alta disponibilidad"](#).

El firmware del dispositivo se ha actualizado

Durante la actualización de StorageGRID 11.9:

- Todos los nodos del dispositivo StorageGRID se actualizan automáticamente a la versión 3.9 del firmware del instalador del dispositivo StorageGRID.
- Los dispositivos SG6060 y SGF6024 se actualizan automáticamente a la versión de firmware BIOS 3B08.EX y a la versión de firmware BMC 4.00.07.

- Los dispositivos SG100 y SG1000 se actualizan automáticamente a la versión de firmware BIOS 3B13.EC y a la versión de firmware BMC 4.74.07.
- Los dispositivos SGF6112, SG6160, SG110 y SG1100 se actualizan automáticamente a la versión de firmware 3.16.07 de BMC .

Las políticas de ILM se manejan de manera diferente según su estado

- La política activa seguirá siendo la misma después de la actualización.
- Al actualizar, solo se conservan las últimas 10 políticas históricas.
- Si hay una política propuesta, se eliminará durante la actualización.

Es posible que se activen alertas

Se pueden activar alertas cuando los servicios se inician y se detienen y cuando el sistema StorageGRID está funcionando como un entorno de versión mixta (algunos nodos de la red ejecutan una versión anterior, mientras que otros se han actualizado a una versión posterior). Es posible que se activen otras alertas después de completarse la actualización.

Por ejemplo, es posible que vea la alerta **No se puede comunicar con el nodo** cuando se detienen los servicios, o es posible que vea la alerta **Error de comunicación de Cassandra** cuando algunos nodos se han actualizado a StorageGRID 11.9 pero otros nodos aún ejecutan StorageGRID 11.8. En general, estas alertas desaparecerán cuando se complete la actualización.

La alerta **Ubicación ILM inalcanzable** podría activarse cuando los nodos de almacenamiento se detienen durante la actualización a StorageGRID 11.9. Esta alerta podría persistir durante 1 día después de que se complete la actualización.

Una vez completada la actualización, puede revisar las alertas relacionadas 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 se puede generar una gran cantidad de notificaciones SNMP cuando los nodos de la red se detienen y reinician durante la actualización. Para evitar notificaciones excesivas, desmarque la casilla de verificación **Habilitar notificaciones del agente SNMP (CONFIGURACIÓN > Monitoreo > Agente SNMP)** para deshabilitar las notificaciones SNMP antes de comenzar la actualización. Luego, vuelva a habilitar las notificaciones una vez completada la actualización.

Los cambios de configuración están restringidos



Esta lista se aplica específicamente a las actualizaciones de StorageGRID 11.8 a StorageGRID 11.9. Si está actualizando a otra versión de StorageGRID , consulte la lista de cambios restringidos en las instrucciones de actualización para esa versión.

Hasta que se complete la tarea **Habilitar nueva función**:

- No realice ningún cambio en la configuración de la cuadrícula.
- No habilite ni deshabilite ninguna función nueva.
- No actualice la configuración de ILM. De lo contrario, podría experimentar un comportamiento ILM inconsistente e inesperado.
- No aplique una revisión ni recupere un nodo de la cuadrícula.



Comuníquese con el soporte técnico si necesita recuperar un nodo durante la actualización.

- No debe administrar grupos de alta disponibilidad, interfaces VLAN ni puntos finales del equilibrador de carga mientras actualiza a StorageGRID 11.9.
- No elimine ningún grupo de alta disponibilidad hasta que se complete la actualización a StorageGRID 11.9. Las direcciones IP virtuales en otros grupos de HA podrían volverse inaccesibles.

Hasta que se complete la tarea **Pasos finales de actualización**:

- No realice un procedimiento de expansión.
- No realice un procedimiento de desmantelamiento.

No puedes ver los detalles de los depósitos ni administrarlos desde el Administrador de inquilinos

Durante la actualización a StorageGRID 11.9 (es decir, mientras el sistema funciona como un entorno de versión mixta), no puede ver los detalles de los depósitos ni administrarlos mediante el Administrador de inquilinos. Uno de los siguientes errores aparece en la página Depósitos del Administrador de inquilinos:

- No puedes usar esta API mientras estás actualizando a 11.9.
- No puedes ver los detalles de las versiones del depósito en el Administrador de inquilinos mientras actualizas a 11.9.

Este error se resolverá una vez que se complete la actualización a 11.9.

Solución alternativa

Mientras la actualización 11.9 está en progreso, use las siguientes herramientas para ver los detalles de los depósitos o administrarlos, en lugar de usar el Administrador de inquilinos:

- Para realizar operaciones S3 estándar en un bucket, utilice el ["API REST de S3"](#) o el ["API de gestión de inquilinos"](#).
- Para realizar operaciones personalizadas de StorageGRID en un depósito (por ejemplo, ver y modificar la consistencia del depósito, habilitar o deshabilitar actualizaciones del último tiempo de acceso o configurar la integración de búsqueda), utilice la API de administración de inquilinos.

Verifique la versión instalada de StorageGRID

Antes de comenzar la actualización, verifique que la versión anterior de StorageGRID esté instalada con la última revisión disponible aplicada.

Acerca de esta tarea

Antes de actualizar a StorageGRID 11.9, su red debe tener instalado StorageGRID 11.8. Si actualmente está utilizando una versión anterior de StorageGRID, debe instalar todos los archivos de actualización anteriores junto con sus últimas revisiones (muy recomendado) hasta que la versión actual de su red sea StorageGRID 11.8.x.y.

Una posible ruta de actualización se muestra en el [ejemplo](#).



NetApp recomienda encarecidamente que aplique la última revisión para cada versión de StorageGRID antes de actualizar a la siguiente versión y que también aplique la última revisión para cada nueva versión que instale. En algunos casos, es necesario aplicar una revisión para evitar el riesgo de pérdida de datos. Ver ["Descargas de NetApp : StorageGRID"](#) y las notas de la versión de cada revisión para obtener más información.

Pasos

1. Sign in en Grid Manager usando un ["navegador web compatible"](#) .
2. Desde la parte superior del Administrador de cuadrícula, seleccione **Ayuda > Acerca de**.
3. Verifique que la **Versión** sea 11.8.x.y.

En el número de versión StorageGRID 11.8.x.y:

- La **versión principal** tiene un valor x de 0 (11.8.0).
 - Una **hotfix**, si se ha aplicado, tiene un valor y (por ejemplo, 11.8.0.1).
4. Si **Versión** no es 11.8.x.y, vaya a ["Descargas de NetApp : StorageGRID"](#) para descargar los archivos de cada versión anterior, incluida la última revisión para cada versión.
 5. Obtén las instrucciones de actualización para cada versión que hayas descargado. Luego, realice el procedimiento de actualización de software para esa versión y aplique la última revisión para esa versión (muy recomendado).

Ver el ["Procedimiento de revisión de StorageGRID"](#) .

Ejemplo: Actualizar a StorageGRID 11.9 desde la versión 11.6

El siguiente ejemplo muestra los pasos para actualizar de la versión 11.6 de StorageGRID a la versión 11.8 como preparación para una actualización de StorageGRID 11.9.

Descargue e instale el software en la siguiente secuencia para preparar su sistema para la actualización:

1. Actualice a la versión principal de StorageGRID 11.6.0.
2. Aplique la última revisión StorageGRID 11.6.0.y.
3. Actualice a la versión principal de StorageGRID 11.7.0.
4. Aplique la última revisión StorageGRID 11.7.0.y.
5. Actualice a la versión principal de StorageGRID 11.8.0.
6. Aplique la última revisión StorageGRID 11.8.0.y.

Obtenga los materiales necesarios para una actualización de software

Antes de comenzar la actualización del software, obtenga todos los materiales necesarios.

Artículo	Notas
Servicio de computadora portátil	La computadora portátil de servicio debe tener: • Puerto de red • Cliente SSH (por ejemplo, PuTTY)
"Navegador web compatible"	La compatibilidad del navegador generalmente cambia para cada versión de StorageGRID . Asegúrese de que su navegador sea compatible con la nueva versión de StorageGRID .
Frase de contraseña de aprovisionamiento	La frase de contraseña se crea y se documenta cuando se instala por primera vez el sistema StorageGRID . La frase de contraseña de aprovisionamiento no aparece en la <code>Passwords.txt</code> archivo.
Archivo RPM o DEB de Linux	Si hay nodos implementados en hosts Linux, debe "Descargue e instale el paquete RPM o DEB en todos los hosts" antes de comenzar la actualización. Asegúrese de que su sistema operativo cumpla con los requisitos mínimos de versión de kernel de StorageGRID: • "Instalar StorageGRID en hosts de Red Hat Enterprise Linux" • "Instalar StorageGRID en hosts Ubuntu o Debian"
Documentación de StorageGRID	• "Notas de la versión" para StorageGRID 11.9 (se requiere iniciar sesión). Asegúrese de leerlos detenidamente antes de comenzar la actualización. • "Guía de resolución de actualización del software StorageGRID" para la versión principal a la que está actualizando (se requiere iniciar sesión) • Otro "Documentación de StorageGRID" , según sea necesario.

Verifique el estado del sistema

Antes de actualizar un sistema StorageGRID , verifique que el sistema esté listo para admitir la actualización. Asegúrese de que el sistema esté funcionando normalmente y que todos los nodos de la red estén operativos.

Pasos

1. Sign in en Grid Manager usando un ["navegador web compatible"](#) .
2. Verifique y resuelva cualquier alerta activa.
3. Confirme que no haya tareas de cuadrícula conflictivas activas o pendientes.
 - a. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
 - b. Seleccione **site > primary Admin Node > CMN > Grid Tasks > Configuración**.

Las tareas de evaluación de la gestión del ciclo de vida de la información (ILME) son las únicas tareas de la red que pueden ejecutarse simultáneamente con la actualización del software.

- c. Si hay otras tareas de la red activas o pendientes, espere a que finalicen o liberen su bloqueo.



Comuníquese con el soporte técnico si una tarea no finaliza o no libera su bloqueo.

- Referirse a "[Comunicaciones internas de los nodos de la red](#)" y "[Comunicaciones externas](#)" para garantizar que todos los puertos necesarios para StorageGRID 11.9 estén abiertos antes de realizar la actualización.



No se requieren puertos adicionales al actualizar a StorageGRID 11.9.

El siguiente puerto requerido se agregó en StorageGRID 11.7. Asegúrese de que esté disponible antes de actualizar a StorageGRID 11.9.

Puerto	Descripción
18086	Puerto TCP utilizado para solicitudes S3 del balanceador de carga StorageGRID a LDR y al nuevo servicio LDR. Antes de actualizar, confirme que este puerto esté abierto desde todos los nodos de la red a todos los nodos de almacenamiento. El bloqueo de este puerto provocará interrupciones del servicio S3 después de la actualización a StorageGRID 11.9.



Si ha abierto algún puerto de firewall personalizado, se le notificará durante la comprobación previa a la actualización. Debe ponerse en contacto con el soporte técnico antes de continuar con la actualización.

Actualizar software

Inicio rápido de actualización

Antes de comenzar la actualización, revise el flujo de trabajo general. La página de actualización de StorageGRID lo guía a través de cada paso de la actualización.

1

Preparar hosts Linux

Si hay nodos StorageGRID implementados en hosts Linux, "[instalar el paquete RPM o DEB en cada host](#)" antes de comenzar la actualización.

2

Subir archivos de actualización y revisión

Desde el nodo de administración principal, acceda a la página Actualización de StorageGRID y cargue el archivo de actualización y el archivo de revisión, si es necesario.

3

Descargar paquete de recuperación

Descargue el paquete de recuperación actual antes de comenzar la actualización.

4

Ejecutar comprobaciones previas de actualización

Las comprobaciones previas a la actualización le ayudan a detectar problemas para que pueda resolverlos antes de comenzar la actualización real.

5

Iniciar actualización

Cuando se inicia la actualización, las comprobaciones previas se ejecutan nuevamente y el nodo de administración principal se actualiza automáticamente. No se puede acceder al Administrador de cuadrícula mientras se actualiza el nodo de administración principal. Los registros de auditoría tampoco estarán disponibles. Esta actualización puede tardar hasta 30 minutos.

6

Descargar paquete de recuperación

Una vez actualizado el nodo de administración principal, descargue un nuevo paquete de recuperación.

7

Aprobar nodos

Puede aprobar nodos de cuadrícula individuales, grupos de nodos de cuadrícula o todos los nodos de cuadrícula.



No apruebe la actualización de un nodo de la red a menos que esté seguro de que el nodo está listo para detenerse y reiniciarse.

8

Reanudar operaciones

Cuando se hayan actualizado todos los nodos de la red, se habilitarán nuevas funciones y se podrán reanudar las operaciones. Debe esperar para realizar un procedimiento de desmantelamiento o expansión hasta que se hayan completado la tarea de fondo **Actualizar base de datos** y la tarea **Pasos finales de actualización**.

Información relacionada

["Calcule el tiempo necesario para completar una actualización"](#)

Linux: Descargue e instale el paquete RPM o DEB en todos los hosts

Si hay nodos StorageGRID implementados en hosts Linux, descargue e instale un paquete RPM o DEB adicional en cada uno de estos hosts antes de comenzar la actualización.

Descargar archivos de actualización, Linux y revisiones

Cuando realiza una actualización de StorageGRID desde Grid Manager, se le solicita que descargue el archivo de actualización y cualquier revisión necesaria como primer paso. Sin embargo, si necesita descargar archivos para actualizar los hosts Linux, puede ahorrar tiempo descargando todos los archivos necesarios con anticipación.

Pasos

1. Ir a ["Descargas de NetApp : StorageGRID"](#) .

2. Seleccione el botón para descargar la última versión o seleccione otra versión del menú desplegable y seleccione **Ir**.

Las versiones del software StorageGRID tienen este formato: 11.x.y. Las revisiones de StorageGRID tienen este formato: 11.x.y.z.

3. Sign in con el nombre de usuario y la contraseña de su cuenta de NetApp .
4. Si aparece un aviso de Precaución/Lectura obligatoria, tome nota del número de revisión y seleccione la casilla de verificación.
5. Lea el Acuerdo de licencia de usuario final (EULA), seleccione la casilla de verificación y luego seleccione **Aceptar y continuar**.

Aparecerá la página de descargas de la versión que usted seleccionó. La página contiene tres columnas.

6. Desde la segunda columna (**Actualizar StorageGRID**), descargue dos archivos:
 - El archivo de actualización para la última versión (este es el archivo en la sección denominada **VMware, SG1000 o SG100 Primary Admin Node**). Si bien este archivo no es necesario hasta que realice la actualización, descargarlo ahora le ahorrará tiempo.
 - Un archivo RPM o DEB en cualquiera de los dos .tgz o .zip formato. Seleccione el .zip archivo si está ejecutando Windows en la computadora portátil de servicio.
 - Red Hat Enterprise Linux
`StorageGRID-Webscale-version-RPM-uniqueID.zip`
`StorageGRID-Webscale-version-RPM-uniqueID.tgz`
 - Ubuntu o Debian
`StorageGRID-Webscale-version-DEB-uniqueID.zip`
`StorageGRID-Webscale-version-DEB-uniqueID.tgz`
7. Si necesita aceptar un aviso de Precaución/Lectura obligatoria debido a una revisión obligatoria, descargue la revisión:
 - a. Regresar a "[Descargas de NetApp : StorageGRID](#)".
 - b. Seleccione el número de revisión en el menú desplegable.
 - c. Acepte nuevamente el aviso de precaución y el EULA.
 - d. Descargue y guarde la revisión y su README.

Se le pedirá que cargue el archivo de revisión en la página de actualización de StorageGRID cuando inicie la actualización.

Instalar archivo en todos los hosts Linux

Realice estos pasos antes de actualizar el software StorageGRID .

Pasos

1. Extraiga los paquetes RPM o DEB del archivo de instalación.
2. Instale los paquetes RPM o DEB en todos los hosts Linux.

Consulte los pasos para instalar los servicios de host de StorageGRID en las instrucciones de instalación:

- "[Red Hat Enterprise Linux: Instalar servicios de host de StorageGRID](#)"

- ["Ubuntu o Debian: Instalar los servicios de host de StorageGRID"](#)

Los nuevos paquetes se instalan como paquetes adicionales.

Eliminar archivos de instalación de versiones anteriores

Para liberar espacio en los hosts Linux, puede eliminar los archivos de instalación de versiones anteriores de StorageGRID que ya no necesita.

Pasos

1. Elimine los archivos de instalación antiguos de StorageGRID .

Sombrero rojo

1. Capturar la lista de paquetes de StorageGRID instalados: `dnf list | grep -i storagegrid`.

Ejemplo:

```
[root@rhel-example ~]# dnf list | grep -i storagegrid
StorageGRID-Webscale-Images-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Images-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Images-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Images-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
StorageGRID-Webscale-Service-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Service-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Service-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Service-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
[root@rhel-example ~]#
```

2. Eliminar paquetes StorageGRID anteriores: `dnf remove images-package service-package`



No elimine los archivos de instalación de la versión de StorageGRID que está ejecutando actualmente ni de las versiones de StorageGRID a las que planea actualizar.

Puede ignorar con seguridad las advertencias que aparecen. Se refieren a archivos que se han reemplazado al instalar paquetes StorageGRID más nuevos.

Ejemplo:

```
[root@rhel-example ~]# dnf remove StorageGRID-Webscale-Images-11-6-
0.x86_64 StorageGRID-Webscale-Service-11-6-0.x86_64
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can
use subscription-manager to register.

Dependencies resolved.
=====
```

```

=====
Package                Architecture      Version      Repository
Size
=====
=====
Removing:
StorageGRID-Webscale-Images-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 2.7 G
StorageGRID-Webscale-Service-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 7.5 M

Transaction Summary
=====
=====
Remove 2 Packages

Freed space: 2.8 G
Is this ok [y/N]: y
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing: 1/1
  Running scriptlet: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64 1/2
  Erasing: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64 1/2
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv6.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv4.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui64.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui48.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/__init__.
pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/sets.pyc:
remove failed: No such file or directory

```

```
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/ip/rfc1924.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/ip/nmap.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/ip/iana.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/ip/glob.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/ip/__init__.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/fbsocket.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/eui/ieee.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/eui/__init__.pyc:  
remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/core.pyc: remove  
failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/subnet_spl  
itter.pyc: remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/__init__.p  
yc: remove failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/compat.pyc: remove  
failed: No such file or directory  
warning: file /usr/lib64/python2.7/site-  
packages/netapp/storagegrid/vendor/latest/netaddr/__init__.pyc:  
remove failed: No such file or directory
```

```
Erasing: StorageGRID-Webscale-Images-11-6-0-11.6.0-  
20220210.0232.8d56cfe.x86_64 2/2
```

```
Verifying: StorageGRID-Webscale-Images-11-6-0-11.6.0-  
20220210.0232.8d56cfe.x86_64 1/2
```

```
Verifying: StorageGRID-Webscale-Service-11-6-0-11.6.0-  
20220210.0232.8d56cfe.x86_64 2/2
```



```
Installed products updated.
```

```
Removed:
```

```
StorageGRID-Webscale-Images-11-6-0-11.6.0-  
20220210.0232.8d56cfe.x86_64  
StorageGRID-Webscale-Service-11-6-0-11.6.0-  
20220210.0232.8d56cfe.x86_64
```

```
Complete!
```

```
[root@rhel-example ~]#
```

Ubuntu y Debian

1. Capturar la lista de paquetes de StorageGRID instalados: `dpkg -l | grep storagegrid`

Ejemplo:

```
root@debian-example:~# dpkg -l | grep storagegrid  
ii storagegrid-webscale-images-11-6-0 11.6.0-20220210.0232.8d56cfe  
amd64 StorageGRID Webscale docker images for 11.6.0  
ii storagegrid-webscale-images-11-7-0 11.7.0-  
20230424.2238.1a2cf8c.dev-signed amd64 StorageGRID Webscale docker  
images for 11.7.0  
ii storagegrid-webscale-images-11-8-0 11.8.0-20240131.0139.e3e0c87  
amd64 StorageGRID Webscale docker images for 11.8.0  
ii storagegrid-webscale-images-11-9-0 11.9.0-20240826.1753.4aeeb70  
amd64 StorageGRID Webscale docker images for 11.9.0  
ii storagegrid-webscale-service-11-6-0 11.6.0-20220210.0232.8d56cfe  
amd64 StorageGRID Webscale host services for 11.6.0  
ii storagegrid-webscale-service-11-7-0 11.7.0-20230424.2238.1a2cf8c  
amd64 StorageGRID Webscale host services for 11.7.0  
ii storagegrid-webscale-service-11-8-0 11.8.0-20240131.0139.e3e0c87  
amd64 StorageGRID Webscale host services for 11.8.0  
ii storagegrid-webscale-service-11-9-0 11.9.0-20240826.1753.4aeeb70  
amd64 StorageGRID Webscale host services for 11.9.0  
root@debian-example:~#
```

2. Eliminar paquetes StorageGRID anteriores: `dpkg -r images-package service-package`



No elimine los archivos de instalación de la versión de StorageGRID que está ejecutando actualmente ni de las versiones de StorageGRID a las que planea actualizar.

Ejemplo:

```
root@debian-example:~# dpkg -r storagegrid-webscale-service-11-6-0
storagegrid-webscale-images-11-6-0
(Reading database ... 38190 files and directories currently
installed.)
Removing storagegrid-webscale-service-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
locale: Cannot set LC_CTYPE to default locale: No such file or
directory
locale: Cannot set LC_MESSAGES to default locale: No such file or
directory
locale: Cannot set LC_ALL to default locale: No such file or
directory
dpkg: warning: while removing storagegrid-webscale-service-11-6-0,
directory '/usr/lib/python2.7/dist-
packages/netapp/storagegrid/vendor/latest' not empty so not removed
Removing storagegrid-webscale-images-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
root@debian-example:~#
```

1. Eliminar imágenes de contenedores StorageGRID .

Docker

1. Capturar la lista de imágenes de contenedores instaladas: `docker images`

Ejemplo:

```
[root@docker-example ~]# docker images
```

REPOSITORY	TAG	IMAGE ID	CREATED
storagegrid-11.9.0	Admin_Node	610f2595bcb4	2 days ago
2.77GB			
storagegrid-11.9.0	Storage_Node	7f73d33eb880	2 days ago
2.65GB			
storagegrid-11.9.0	API_Gateway	2f0bb79526e9	2 days ago
1.82GB			
storagegrid-11.8.0	Storage_Node	7125480de71b	7 months ago
2.54GB			
storagegrid-11.8.0	Admin_Node	404e9f1bd173	7 months ago
2.63GB			
storagegrid-11.8.0	Archive_Node	c3294a29697c	7 months ago
2.39GB			
storagegrid-11.8.0	API_Gateway	1f88f24b9098	7 months ago
1.74GB			
storagegrid-11.7.0	Storage_Node	1655350eff6f	16 months ago
2.51GB			
storagegrid-11.7.0	Admin_Node	872258dd0dc8	16 months ago
2.48GB			
storagegrid-11.7.0	Archive_Node	121e7c8b6d3b	16 months ago
2.41GB			
storagegrid-11.7.0	API_Gateway	5b7a26e382de	16 months ago
1.77GB			
storagegrid-11.6.0	Admin_Node	ee39f71a73e1	2 years ago
2.38GB			
storagegrid-11.6.0	Storage_Node	f5ef895dcad0	2 years ago
2.08GB			
storagegrid-11.6.0	Archive_Node	5782de552db0	2 years ago
1.95GB			
storagegrid-11.6.0	API_Gateway	cb480ed37eea	2 years ago
1.35GB			

```
[root@docker-example ~]#
```

2. Eliminar las imágenes de contenedor de versiones anteriores de StorageGRID : `docker rmi image id`



No elimine las imágenes de contenedor de la versión de StorageGRID que está ejecutando actualmente ni de las versiones de StorageGRID a las que planea actualizar.

Ejemplo:

```
[root@docker-example ~]# docker rmi cb480ed37eea
Untagged: storagegrid-11.6.0:API_Gateway
Deleted:
sha256:cb480ed37eea0ae9cf3522de1dadfbff0075010d89c1c0a2337a3178051ddf02
Deleted:
sha256:5f269aabf15c32c1fe6f36329c304b6c6ecb563d973794b9b59e8e5ab8cccafa
Deleted:
sha256:47c2b2c295a77b312b8db69db58a02d8e09e929e121352bec713fa12dae66bde
[root@docker-example ~]#
```

Podman

1. Capturar la lista de imágenes de contenedores instaladas: `podman images`

Ejemplo:

```
[root@podman-example ~]# podman images
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
localhost/storagegrid-11.8.0	Storage_Node	7125480de71b	7 months ago	2.57 GB
localhost/storagegrid-11.8.0	Admin_Node	404e9f1bd173	7 months ago	2.67 GB
localhost/storagegrid-11.8.0	Archive_Node	c3294a29697c	7 months ago	2.42 GB
localhost/storagegrid-11.8.0	API_Gateway	1f88f24b9098	7 months ago	1.77 GB
localhost/storagegrid-11.7.0	Storage_Node	1655350eff6f	16 months ago	2.54 GB
localhost/storagegrid-11.7.0	Admin_Node	872258dd0dc8	16 months ago	2.51 GB
localhost/storagegrid-11.7.0	Archive_Node	121e7c8b6d3b	16 months ago	2.44 GB
localhost/storagegrid-11.7.0	API_Gateway	5b7a26e382de	16 months ago	1.8 GB
localhost/storagegrid-11.6.0	Admin_Node	ee39f71a73e1	2 years ago	2.42 GB
localhost/storagegrid-11.6.0	Storage_Node	f5ef895dcad0	2 years ago	2.11 GB
localhost/storagegrid-11.6.0	Archive_Node	5782de552db0	2 years ago	1.98 GB
localhost/storagegrid-11.6.0	API_Gateway	cb480ed37eea	2 years ago	1.38 GB

```
[root@podman-example ~]#
```

2. Eliminar las imágenes de contenedor de versiones anteriores de StorageGRID : `podman rmi image id`



No elimine las imágenes de contenedor de la versión de StorageGRID que está ejecutando actualmente ni de las versiones de StorageGRID a las que planea actualizar.

Ejemplo:

```
[root@podman-example ~]# podman rmi f5ef895dcad0
Untagged: localhost/storagegrid-11.6.0:Storage_Node
Deleted:
f5ef895dcad0d78d0fd21a07dd132d7c7f65f45d80ee7205a4d615494e44cbb7
[root@podman-example ~]#
```

Realizar la actualización

Puede actualizar a StorageGRID 11.9 y aplicar la última revisión para esa versión al mismo tiempo. La página de actualización de StorageGRID proporciona la ruta de actualización recomendada y enlaces directos a las páginas de descarga correctas.

Antes de empezar

Ha revisado todas las consideraciones y completado todos los pasos de planificación y preparación.

Acceda a la página de actualización de StorageGRID

Como primer paso, acceda a la página Actualización de StorageGRID en el Administrador de Grid.

Pasos

1. Sign in en Grid Manager usando un ["navegador web compatible"](#) .
2. Seleccione **MANTENIMIENTO > Sistema > Actualización de software**.
3. Desde el mosaico de actualización de StorageGRID , seleccione **Actualizar**.

Seleccionar archivos

La ruta de actualización en la página Actualización de StorageGRID indica qué versiones principales (por ejemplo, 11.9.0) y revisiones (por ejemplo, 11.9.0.1) debe instalar para llegar a la última versión de StorageGRID . Debe instalar las versiones y revisiones recomendadas en el orden que se muestra.



Si no se muestra ninguna ruta de actualización, es posible que su navegador no pueda acceder al sitio de soporte de NetApp o que la casilla de verificación **Buscar actualizaciones de software** en la página AutoSupport (**SUPPORT > Herramientas > * AutoSupport* > Configuración**) esté deshabilitada.

Pasos

1. Para el paso **Seleccionar archivos**, revise la ruta de actualización.
2. En la sección Descargar archivos, seleccione cada enlace **Descargar** para descargar los archivos necesarios del sitio de soporte de NetApp .

Si no se muestra ninguna ruta de actualización, vaya a la ["Descargas de NetApp : StorageGRID"](#) para determinar si hay una nueva versión o revisión disponible y descargar los archivos que necesita.



Si necesita descargar e instalar un paquete RPM o DEB en todos los hosts de Linux, es posible que ya tenga los archivos de actualización y revisión de StorageGRID enumerados en la ruta de actualización.

3. Seleccione **Explorar** para cargar el archivo de actualización de versión a StorageGRID:
`NetApp_StorageGRID_11.9.0_Software_uniqueID.upgrade`

Cuando finaliza el proceso de carga y validación, aparece una marca de verificación verde junto al nombre del archivo.

4. Si descargó un archivo de revisión, seleccione **Explorar** para cargar ese archivo. La revisión se aplicará automáticamente como parte de la actualización de la versión.
5. Seleccione **Continuar**.

Ejecutar comprobaciones previas

La ejecución de comprobaciones previas le permite detectar y resolver cualquier problema de actualización antes de comenzar a actualizar su red.

Pasos

1. Para el paso **Ejecutar comprobaciones previas**, comience ingresando la contraseña de aprovisionamiento para su red.
2. Seleccione **Descargar paquete de recuperación**.

Debe descargar la copia actual del archivo del paquete de recuperación antes de actualizar el nodo de administración principal. El archivo del paquete de recuperación le permite restaurar el sistema si ocurre una falla.

3. Cuando se descargue el archivo, confirme que puede acceder al contenido, incluido el `Passwords.txt` archivo.
4. Copiar el archivo descargado(.zip) a dos lugares seguros, protegidos y separados.



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

5. Seleccione **Ejecutar comprobaciones previas** y espere a que se completen las comprobaciones previas.
6. Revise los detalles de cada verificación previa informada y resuelva cualquier error informado. Ver el "[Guía de resolución de actualización del software StorageGRID](#)" para la versión StorageGRID 11.9.

Debe resolver todos los *errores* de comprobación previa antes de poder actualizar su sistema. Sin embargo, no es necesario abordar las *advertencias* de precheck antes de actualizar.



Si ha abierto algún puerto de firewall personalizado, se le notificará durante la validación previa. Debe ponerse en contacto con el soporte técnico antes de continuar con la actualización.

7. Si realizó algún cambio de configuración para resolver los problemas informados, seleccione **Ejecutar comprobaciones previas** nuevamente para obtener resultados actualizados.

Si se han resuelto todos los errores, se le solicitará que inicie la actualización.

Iniciar actualización y actualizar el nodo de administración principal

Cuando se inicia la actualización, se ejecutan nuevamente las comprobaciones previas de actualización y el nodo de administración principal se actualiza automáticamente. Esta parte de la actualización puede tardar hasta 30 minutos.



No podrá acceder a ninguna otra página de Grid Manager mientras se esté actualizando el nodo de administración principal. Los registros de auditoría tampoco estarán disponibles.

Pasos

1. Seleccione **Iniciar actualización**.

Aparecerá una advertencia para recordarle que perderá temporalmente el acceso al Administrador de cuadrícula.

2. Seleccione **Aceptar** para reconocer la advertencia e iniciar la actualización.
3. Espere a que se realicen las comprobaciones previas de actualización y a que se actualice el nodo de administración principal.



Si se informa algún error de verificación previa, resuélvalo y seleccione **Iniciar actualización** nuevamente.

Si la red tiene otro nodo de administración que está en línea y listo, puede usarlo para monitorear el estado del nodo de administración principal. Tan pronto como se actualice el nodo de administración principal, podrá aprobar los demás nodos de la red.

4. Según sea necesario, seleccione **Continuar** para acceder al paso **Actualizar otros nodos**.

Actualizar otros nodos

Debe actualizar todos los nodos de la red, pero puede realizar múltiples sesiones de actualización y personalizar la secuencia de actualización. Por ejemplo, es posible que prefiera actualizar los nodos del sitio A en una sesión y luego actualizar los nodos del sitio B en una sesión posterior. Si decide realizar la actualización en más de una sesión, tenga en cuenta que no podrá comenzar a usar las nuevas funciones hasta que se hayan actualizado todos los nodos.

Si el orden en que se actualizan los nodos es importante, apruebe los nodos o grupos de nodos uno a la vez y espere hasta que se complete la actualización en cada nodo antes de aprobar el siguiente nodo o grupo de nodos.



Cuando la actualización comienza en un nodo de la red, los servicios en ese nodo se detienen. Posteriormente se reinicia el nodo de la red. Para evitar interrupciones del servicio para las aplicaciones cliente que se comunican con el nodo, no apruebe la actualización de un nodo a menos que esté seguro de que el nodo está listo para detenerse y reiniciarse. Según sea necesario, programe una ventana de mantenimiento o notifique a los clientes.

Pasos

1. Para el paso **Actualizar otros nodos**, revise el Resumen, que proporciona la hora de inicio de la actualización en su totalidad y el estado de cada tarea de actualización principal.
 - **Iniciar servicio de actualización** es la primera tarea de actualización. Durante esta tarea, el archivo de software se distribuye a los nodos de la red y se inicia el servicio de actualización en cada nodo.
 - Cuando se completa la tarea **Iniciar servicio de actualización**, se inicia la tarea **Actualizar otros nodos de la red** y se le solicita que descargue una nueva copia del paquete de recuperación.
2. Cuando se le solicite, ingrese su contraseña de aprovisionamiento y descargue una nueva copia del paquete de recuperación.



Debe descargar una nueva copia del archivo del paquete de recuperación después de actualizar el nodo de administración principal. El archivo del paquete de recuperación le permite restaurar el sistema si ocurre una falla.

3. Revise las tablas de estado para cada tipo de nodo. Hay tablas para nodos de administración no principales, nodos de puerta de enlace y nodos de almacenamiento.

Un nodo de la cuadrícula puede estar en una de estas etapas cuando aparecen las tablas por primera vez:

- Desempaquetando la actualización

- Descargando
- Esperando ser aprobado

4. Cuando esté listo para seleccionar nodos de la red para actualizar (o si necesita desaprobados nodos seleccionados), utilice estas instrucciones:

Tarea	Instrucción
Busque nodos específicos para aprobar, como todos los nodos en un sitio en particular	Introduzca la cadena de búsqueda en el campo Buscar
Seleccionar todos los nodos para actualizar	Seleccione Aprobar todos los nodos
Seleccionar todos los nodos del mismo tipo para actualizar (por ejemplo, todos los nodos de almacenamiento)	Seleccione el botón Aprobar todo para el tipo de nodo Si aprueba más de un nodo del mismo tipo, los nodos se actualizarán uno a la vez.
Seleccione un nodo individual para la actualización	Seleccione el botón Aprobar para el nodo
Posponer la actualización en todos los nodos seleccionados	Seleccione Desaprobar todos los nodos
Posponer la actualización en todos los nodos seleccionados del mismo tipo	Seleccione el botón Desaprobar todo para el tipo de nodo
Posponer la actualización en un nodo individual	Seleccione el botón Desaprobar para el nodo

5. Espere a que los nodos aprobados pasen por estas etapas de actualización:

- Aprobado y en espera de ser actualizado
- Servicios de parada



No puedes eliminar un nodo cuando su etapa llega a **Deteniendo servicios**. El botón **Desaprobar** está deshabilitado.

- Contenedor de parada
- Limpieza de imágenes de Docker
- Actualización de los paquetes del sistema operativo base



Cuando un nodo del dispositivo llega a esta etapa, se actualiza el software del instalador del dispositivo StorageGRID en el dispositivo. Este proceso automatizado garantiza que la versión del instalador del dispositivo StorageGRID permanezca sincronizada con la versión del software StorageGRID .

- Reiniciando



Algunos modelos de dispositivos podrían reiniciarse varias veces para actualizar el firmware y el BIOS.

- Realizar pasos después de reiniciar
- Servicios de inicio
- Hecho

6. Repita el [paso de aprobación](#) tantas veces como sea necesario hasta que se hayan actualizado todos los nodos de la red.

Actualización completa

Cuando todos los nodos de la red hayan completado las etapas de actualización, la tarea **Actualizar otros nodos de la red** se mostrará como Completada. Las tareas de actualización restantes se realizan automáticamente en segundo plano.

Pasos

1. Una vez que se complete la tarea **Habilitar funciones** (lo que ocurre rápidamente), puede comenzar a usar la ["nuevas funciones"](#) en la versión mejorada de StorageGRID .
2. Durante la tarea **Actualizar base de datos**, el proceso de actualización verifica cada nodo para verificar que no sea necesario actualizar la base de datos de Cassandra.



La actualización de StorageGRID 11.8 a 11.9 no requiere una actualización de la base de datos Cassandra; sin embargo, el servicio Cassandra se detendrá y se reiniciará en cada nodo de almacenamiento. Para futuras versiones de funciones de StorageGRID , el paso de actualización de la base de datos de Cassandra podría demorar varios días en completarse.

3. Cuando se haya completado la tarea **Actualizar base de datos**, espere unos minutos hasta que se completen los **Pasos finales de actualización**.
4. Cuando se hayan completado los **Pasos finales de actualización**, la actualización estará lista. El primer paso, **Seleccionar archivos**, se vuelve a mostrar con un banner de éxito verde.
5. Verifique que las operaciones de la red hayan vuelto a la normalidad:
 - a. Verifique que los servicios estén funcionando con normalidad y que no haya alertas inesperadas.
 - b. Confirme que las conexiones del cliente al sistema StorageGRID estén funcionando como se espera.

Solucionar problemas de actualización

Si algo sale mal al realizar una actualización, es posible que pueda resolver el problema usted mismo. Si no puede resolver un problema, reúna toda la información que pueda y luego comuníquese con el soporte técnico.

La actualización no se completa

Las siguientes secciones describen cómo recuperarse de situaciones en las que la actualización ha fallado parcialmente.

Errores de comprobación previa de la actualización

Para detectar y resolver problemas, puede ejecutar manualmente las comprobaciones previas a la actualización antes de comenzar la actualización real. La mayoría de los errores de verificación previa brindan

información sobre cómo resolver el problema.

Fallos de aprovisionamiento

Si el proceso de aprovisionamiento automático falla, comuníquese con el soporte técnico.

El nodo de la red se bloquea o no se inicia

Si un nodo de la red falla durante el proceso de actualización o no puede iniciarse exitosamente una vez finalizada la actualización, comuníquese con el soporte técnico para investigar y corregir cualquier problema subyacente.

Se interrumpe la ingesta o recuperación de datos

Si la ingesta o recuperación de datos se interrumpe inesperadamente cuando no está actualizando un nodo de la red, comuníquese con el soporte técnico.

Errores de actualización de la base de datos

Si la actualización de la base de datos falla con un error, vuelva a intentar la actualización. Si vuelve a fallar, contacte con el soporte técnico.

Información relacionada

["Comprobación del estado del sistema antes de actualizar el software"](#)

Problemas de interfaz de usuario

Es posible que experimente problemas con el Administrador de red o el Administrador de inquilinos durante o después de la actualización.

Grid Manager muestra varios mensajes de error durante la actualización

Si actualiza su navegador o navega a otra página de Grid Manager mientras se actualiza el nodo de administración principal, es posible que vea varios mensajes "503: Servicio no disponible" y "Problema para conectarse al servidor". Puede ignorar estos mensajes con seguridad: dejarán de aparecer tan pronto como se actualice el nodo.

Si estos mensajes aparecen durante más de una hora después de iniciar la actualización, es posible que haya ocurrido algo que impidió que se actualizara el nodo de administración principal. Si no puede resolver el problema por su cuenta, comuníquese con el soporte técnico.

La interfaz web no responde como se esperaba

Es posible que el administrador de red o el administrador de inquilinos no respondan como se espera después de actualizar el software StorageGRID .

Si experimenta problemas con la interfaz web:

- Asegúrese de estar utilizando un ["navegador web compatible"](#) .



La compatibilidad del navegador generalmente cambia para cada versión de StorageGRID .

- Limpia el caché de tu navegador web.

Al borrar la memoria caché se eliminan los recursos obsoletos utilizados por la versión anterior del

software StorageGRID y se permite que la interfaz de usuario vuelva a funcionar correctamente. Para obtener instrucciones, consulte la documentación de su navegador web.

Mensajes de error de "Comprobación de disponibilidad de imágenes de Docker"

Al intentar iniciar el proceso de actualización, es posible que reciba un mensaje de error que indique "Los siguientes problemas fueron identificados por el conjunto de validación de verificación de disponibilidad de imágenes de Docker". Todos los problemas deben resolverse antes de poder completar la actualización.

Comuníquese 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. Archivo de información de la versión de actualización {file_path} No coincidió con el formato esperado.	El paquete de actualización está dañado.	Vuelva a cargar el paquete de actualización e inténtelo nuevamente. Si el problema persiste, contacte con el soporte técnico.
Archivo de información de la versión de actualización {file_path} No fue encontrado. No se puede determinar la versión de actualización.	El paquete de actualización está dañado.	Vuelva a cargar el paquete de actualización e inténtelo nuevamente. Si el problema persiste, contacte con el soporte técnico.
No se puede determinar la versión de lanzamiento instalada actualmente en {node_name} .	Un archivo crítico en el nodo está dañado.	Póngase en contacto con el soporte técnico.
Error de conexión al intentar listar versiones en {node_name}	El nodo está fuera de línea o la conexión fue interrumpida.	Verifique que todos los nodos estén en línea y sean accesibles desde el nodo de administración principal, e inténtelo nuevamente.
El host del nodo {node_name} no tiene StorageGRID {upgrade_version} imagen cargada. Las imágenes y los servicios deben estar instalados en el host antes de que pueda continuar la actualización.	Los paquetes RPM o DEB para la actualización no se han instalado en el host donde se ejecuta el nodo, o las imágenes aún están en proceso de importación. Nota: Este error solo se aplica a los nodos que se ejecutan como contenedores en Linux.	Verifique que los paquetes RPM o DEB se hayan instalado en todos los hosts Linux donde se ejecutan los nodos. Asegúrese de que la versión sea correcta tanto para el servicio como para el archivo de imágenes. Espere unos minutos y vuelva a intentarlo. Ver "Linux: Instalar paquete RPM o DEB en todos los hosts" .
Error al comprobar el nodo {node_name}	Se produjo un error inesperado.	Espere unos minutos y vuelva a intentarlo.

Mensaje	Causa	Solución
Error no detectado al ejecutar comprobaciones previas. {error_string}	Se produjo un error inesperado.	Espere unos minutos y vuelva a intentarlo.

Aplicar la revisión de StorageGRID

Procedimiento de revisión de StorageGRID

Es posible que necesite aplicar una revisión a su sistema StorageGRID si se detectan y resuelven problemas con el software entre versiones de funciones.

Las revisiones de StorageGRID contienen cambios de software que están disponibles fuera de una versión de parche o función. Los mismos cambios se incluirán en una versión futura. Además, cada versión de revisión contiene un resumen de todas las revisiones anteriores dentro de la versión de función o parche.

Consideraciones para aplicar un hotfix

No se puede aplicar una revisión de StorageGRID cuando se está ejecutando otro procedimiento de mantenimiento. Por ejemplo, no se puede aplicar una revisión mientras se ejecuta un procedimiento de desmantelamiento, expansión o recuperación.



Si se pausa un procedimiento de desmantelamiento de un nodo o sitio, puede aplicar una revisión de forma segura. Además, es posible que pueda aplicar una revisión durante las etapas finales de un procedimiento de actualización de StorageGRID. Consulte las instrucciones para actualizar el software StorageGRID para obtener más detalles.

Después de cargar la revisión en el Administrador de cuadrícula, esta se aplica automáticamente al nodo de administración principal. Luego, puede aprobar la aplicación de la revisión al resto de los nodos en su 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. Debes resolver cualquier problema que haya causado las fallas y luego volver a intentar todo el proceso. Los nodos en los que se haya aplicado con éxito previamente la revisión se omitirán en las aplicaciones posteriores. Puede volver a intentar de forma segura el proceso de revisión tantas veces como sea necesario hasta que se hayan actualizado todos los nodos. La revisión debe instalarse correctamente en todos los nodos de la red para que la aplicación se complete.

Si bien los nodos de la red se actualizan con la nueva versión de revisión, los cambios reales en una revisión podrían afectar solo a servicios específicos en tipos específicos de nodos. Por ejemplo, una revisión podría afectar únicamente al servicio LDR en los nodos de almacenamiento.

Cómo se aplican las revisiones para la recuperación y expansión

Después de aplicar una revisión a su red, el nodo de administración principal instala automáticamente la misma versión de revisión en cualquier nodo restaurado mediante operaciones de recuperación o agregado en una expansión.

Sin embargo, si necesita recuperar el nodo de administración principal, debe instalar manualmente la versión correcta de StorageGRID y luego aplicar la revisión. La versión final de StorageGRID del nodo de administración principal debe coincidir con la versión de los demás nodos de la red.

El siguiente ejemplo ilustra cómo aplicar una revisión al recuperar el nodo de administración principal:

1. Supongamos que la red está ejecutando una versión StorageGRID 11.A.B con la última revisión. La "versión de cuadrícula" es 11.D.B.y.
2. El nodo de administración principal falla.
3. Vuelve a implementar el nodo de administración principal mediante StorageGRID 11.A.B y realiza el procedimiento de recuperación.



Según sea necesario para que coincida con la versión de la red, puede utilizar una versión menor al implementar el nodo; no es necesario implementar primero la versión principal.

4. A continuación, aplique la revisión 11.A.B.y al nodo de administración principal.

Para obtener más información, consulte ["Configurar el nodo de administración principal de reemplazo"](#) .

Cómo se ve afectado su sistema cuando aplica una revisión

Debe comprender cómo se verá afectado su sistema StorageGRID cuando aplique una revisión.

Las revisiones de StorageGRID no son disruptivas

El sistema StorageGRID puede ingerir y recuperar datos de las aplicaciones cliente durante todo el proceso de revisión. Si aprueba que se realicen revisiones en todos los nodos del mismo tipo (por ejemplo, nodos de almacenamiento), los nodos se desactivan uno a la vez, por lo que no hay ningún momento en el que todos los nodos de la red o todos los nodos de la red de un determinado tipo no estén disponibles.

Para permitir la disponibilidad continua, asegúrese de que su política ILM contenga reglas que especifiquen el almacenamiento de múltiples copias de cada objeto. También debe asegurarse de que todos los clientes S3 externos estén configurados para enviar solicitudes a uno de los siguientes:

- Una dirección IP virtual de grupo de alta disponibilidad (HA)
- Un balanceador de carga de terceros de alta disponibilidad
- Múltiples nodos de puerta de enlace para cada cliente
- Múltiples nodos de almacenamiento para cada cliente

Las aplicaciones cliente podrían experimentar interrupciones a corto plazo

El sistema StorageGRID puede ingerir y recuperar datos de las aplicaciones cliente durante todo el proceso de revisión; sin embargo, las conexiones de los clientes a los nodos de puerta de enlace o nodos de almacenamiento individuales pueden interrumpirse temporalmente si la revisión necesita reiniciar los servicios en esos nodos. La conectividad se restablecerá una vez que se complete el proceso de revisión y se reanuden los servicios en los nodos individuales.

Es posible que sea necesario programar un tiempo de inactividad para aplicar una revisión si la pérdida de conectividad durante un período breve no es aceptable. Puede utilizar la aprobación selectiva para programar cuándo se actualizan determinados nodos.



Puede utilizar varias puertas de enlace y grupos de alta disponibilidad (HA) para proporcionar conmutación por error automática durante el proceso de revisión. Vea las instrucciones para ["configuración de grupos de alta disponibilidad"](#) .

Es posible que se activen alertas y notificaciones SNMP

Es posible que se activen alertas y notificaciones SNMP cuando se reinician los servicios y cuando el sistema StorageGRID está funcionando como un entorno de versión mixta (algunos nodos de la red ejecutan una versión anterior, mientras que otros se han actualizado a una versión posterior). En general, estas alertas y notificaciones desaparecerán cuando se complete la revisión.

Los cambios de configuración están restringidos

Al aplicar una revisión a StorageGRID:

- No realice ningún cambio en la configuración de la red (por ejemplo, especificar subredes de la red de red o aprobar nodos de red 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 un hotfix, debes obtener todos los materiales necesarios.

Artículo	Notas
Archivo de revisión de StorageGRID	Debes descargar el archivo de revisión de StorageGRID .
• Puerto de red • "Navegador web compatible" • Cliente SSH (por ejemplo, PuTTY)	
Paquete de recuperación(.zip) archivo	Antes de aplicar una revisión," Descargue el archivo del paquete de recuperación más reciente " en caso de que ocurra algún problema durante la revisión. Luego, después de aplicar la revisión, descargue una nueva copia del archivo del paquete de recuperación y guárdelo en un lugar seguro. El archivo del paquete de recuperación actualizado le permite restaurar el sistema si ocurre una falla.
Archivo Passwords.txt	Opcional y se utiliza solo si está aplicando una revisión manualmente mediante el cliente SSH. El Passwords.txt El archivo es parte del paquete de recuperación .zip archivo.
Frase de contraseña de aprovisionamiento	La frase de contraseña se crea y se documenta cuando se instala por primera vez el sistema StorageGRID . La frase de contraseña de aprovisionamiento no aparece en la Passwords.txt archivo.
Documentación relacionada	readme.txt`archivo para la revisión. Este archivo está incluido en la página de descarga de revisiones. Asegúrese de revisar el `readme Limpie con cuidado antes de aplicar la revisión.

Descargar archivo de revisión

Debe descargar el archivo de revisión antes de poder aplicar la revisión.

Pasos

1. Ir a ["Descargas de NetApp : StorageGRID"](#) .
2. Seleccione la flecha hacia abajo debajo de **Software disponible** para ver una lista de revisiones que están 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 acabas de ["recuperó el nodo de administración principal"](#) y necesita aplicar una revisión, seleccione la misma versión de revisión que está instalada en los otros nodos de la red.

- a. Seleccione la versión de revisión que desea descargar y seleccione **Ir**.
- b. Sign in con el nombre de usuario y la contraseña de su cuenta de NetApp .
- c. Lea y acepte el Acuerdo de licencia de usuario final.

Aparecerá la página de descarga de la versión que usted seleccionó.

- d. Descargar la revisión `readme.txt` archivo para ver un resumen de los cambios incluidos en la revisión.

4. Seleccione el botón de descarga para la revisión y guarde el archivo.



No cambie el nombre de este archivo.



Si está utilizando un dispositivo macOS, el archivo de revisión podría guardarse automáticamente como un `.txt` archivo. Si es así, debes cambiar el nombre del archivo sin el `.txt` extensión.

5. Seleccione una ubicación para la descarga y seleccione **Guardar**.

Verifique el estado del sistema antes de aplicar la revisión

Debe verificar que el sistema esté listo para aceptar la revisión.

1. Sign in en Grid Manager usando un ["navegador web compatible"](#) .
2. Si es posible, asegúrese de que el sistema esté funcionando normalmente y que todos los nodos de la red estén conectados a la red.

Los nodos conectados tienen marcas de verificación verdes  en la página Nodos.

3. Verifique y resuelva cualquier alerta actual, si es posible.
4. Asegúrese de que no haya otros procedimientos de mantenimiento en curso, como una actualización, recuperación, expansión o desmantelamiento.

Debe esperar a que se complete cualquier procedimiento de mantenimiento activo antes de aplicar una revisión.

No se puede aplicar una revisión de StorageGRID cuando se está ejecutando otro procedimiento de mantenimiento. Por ejemplo, no se puede aplicar una revisión mientras se ejecuta un procedimiento de desmantelamiento, expansión o recuperación.



Si un nodo o sitio ["El procedimiento de desmantelamiento está en pausa"](#) , puedes aplicar una revisión de forma segura. Además, es posible que pueda aplicar una revisión durante las etapas finales de un procedimiento de actualización de StorageGRID . Vea las instrucciones para ["actualización del software StorageGRID"](#) .

Aplicar revisión

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

Antes de empezar

- Usted ha revisado el ["Consideraciones para aplicar una revisión"](#) .
- Tienes la contraseña de aprovisionamiento.
- Tienes acceso Root o permiso de Mantenimiento.

Acerca de esta tarea

- Puede retrasar la aplicación de una revisión a un nodo, pero el proceso de revisión no estará completo hasta que la aplique a todos los nodos.
- No puede realizar una actualización del software StorageGRID ni del sistema operativo SANtricity hasta que haya completado el proceso de revisión.

Pasos

1. Sign in en Grid Manager usando un ["navegador web compatible"](#) .
2. Seleccione **MANTENIMIENTO > Sistema > Actualización de software**.

Aparece la página de Actualización de software.

Software update

You can upgrade StorageGRID software, apply a hotfix, or upgrade the SANtricity OS software on StorageGRID storage appliances. NetApp recommends you apply the latest hotfix before and after each software upgrade. Some hotfixes are required to prevent data loss.

StorageGRID upgrade

Upgrade to the next StorageGRID version and apply the latest hotfix for that version.

Upgrade →

StorageGRID hotfix

Apply a hotfix to your current StorageGRID software version.

Apply hotfix →

SANtricity OS update

Update the SANtricity OS software on your StorageGRID storage appliances.

Update →

3. Seleccione **Aplicar revisión**.

Aparece la página de revisión de StorageGRID .

StorageGRID Hotfix

Before starting the hotfix process, you must confirm that there are no active alerts and that all grid nodes are online and available.

When the primary Admin Node is updated, services are stopped and restarted. Connectivity might be interrupted until the services are back online.

Hotfix file

Hotfix file ?

Browse

Passphrase

Provisioning Passphrase ?

Start

4. Seleccione el archivo de revisión que descargó del sitio de soporte de NetApp .

- Seleccione **Explorar**.
- Localice y seleccione el archivo.

`hotfix-install-version`

- Seleccione **Abrir**.

El archivo está cargado. Una vez finalizada la carga, el nombre del archivo se muestra en el campo Detalles.



No cambie el nombre del archivo porque es parte del proceso de verificación.

5. Introduzca la contraseña de aprovisionamiento en el cuadro de texto.

El botón **Inicio** se habilita.

6. Seleccione **Inicio**.

Aparece una advertencia indicando que la conexión de su navegador podría perderse temporalmente mientras se reinician los servicios en el 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 revisión.



Si se informa algún error, resuélvalo, vuelva a cargar el archivo de revisión y seleccione **Iniciar** nuevamente.

b. Aparece la tabla de progreso de instalación de la revisión.

Esta tabla muestra todos los nodos de su red y la etapa actual de la instalación de la revisión para cada nodo. Los nodos de la tabla están agrupados por tipo (nodos de administración, nodos de puerta de enlace y nodos de almacenamiento).

c. La barra de progreso llega al final y luego el nodo de administración principal se muestra como "Completado".

Hotfix Installation Progress

						Approve All	Remove All
Admin Nodes - 1 out of 1 completed							
						Search	
Site	Name	Progress	Stage			Details	Action
Vancouver	VTC-ADM1-101-191		Complete				

8. Opcionalmente, ordene las listas de nodos en cada agrupación en orden ascendente o descendente por **Sitio**, **Nombre**, **Progreso**, **Etapa** o **Detalles**. O ingrese un término en el cuadro **Buscar** para buscar nodos específicos.

9. Aprobar los nodos de la red que están listos para ser actualizados. Los nodos aprobados del mismo tipo se actualizan uno a la vez.



No apruebe la revisión de un nodo a menos que esté seguro de que el nodo está listo para actualizarse. Cuando se aplica la revisión a un nodo de la red, es posible que se reinicien algunos servicios de ese nodo. Estas operaciones podrían provocar interrupciones del servicio para 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** dentro de cada agrupación para agregar todos los nodos del mismo tipo a la cola de revisiones. Si ha ingresado 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** en la parte superior de la página aprueba todos los nodos enumerados en la página, mientras que el botón **Aprobar todo** en la parte superior de una agrupación de tablas solo aprueba todos los nodos de ese grupo. Si el orden en que se actualizan los nodos es importante, apruebe los nodos o grupos de nodos uno a la vez y espere hasta que se complete la actualización en cada nodo antes de aprobar el siguiente nodo o 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, comuníquese con el soporte técnico.

- Seleccione **Eliminar** o **Eliminar todo** para eliminar un nodo o todos los nodos de la cola de revisiones.

Cuando la etapa avanza más allá de "En cola", el botón **Eliminar** se oculta y ya no se puede eliminar el nodo del proceso de revisión.

▲
Storage Nodes - 1 out of 9 completed

Approve All

Remove All

Search

Q

Site	Name	Progress	Stage	Details	Action
Raleigh	RAL-S1-101-196		Queued		Remove
Raleigh	RAL-S2-101-197		Complete		
Raleigh	RAL-S3-101-198		Queued		Remove
Sunnyvale	SVL-S1-101-199		Queued		Remove
Sunnyvale	SVL-S2-101-93		Waiting for you to approve		Approve
Sunnyvale	SVL-S3-101-94		Waiting for you to approve		Approve
Vancouver	VTC-S1-101-193		Waiting for you to approve		Approve
Vancouver	VTC-S2-101-194		Waiting for you to approve		Approve
Vancouver	VTC-S3-101-195		Waiting for you to approve		Approve

10. Espere mientras se aplica la revisión a cada nodo de la red aprobado.

Cuando la revisión se haya instalado correctamente en todos los nodos, se cerrará la tabla Progreso de

instalación de la revisión. Un banner verde muestra la fecha y la hora en que se completó la revisión.

11. Si no se pudo aplicar la revisión a ningún nodo, revise el error de cada nodo, resuelva el problema y repita estos pasos.

El procedimiento no estará completo hasta que la revisión se haya aplicado exitosamente a todos los nodos. Puede volver a intentar de forma segura el proceso de revisión tantas veces como sea necesario hasta que se complete.

Configurar y administrar un sistema StorageGRID

Administrar StorageGRID

Administrar StorageGRID

Utilice estas instrucciones para configurar y administrar un sistema StorageGRID .

Acerca de estas instrucciones

Las tareas principales para configurar y administrar StorageGRID le permiten:

- Utilice el Administrador de cuadrícula para configurar grupos y usuarios
- Cree cuentas de inquilino para permitir que las aplicaciones cliente de S3 almacenen y recuperen objetos
- Configurar y administrar redes StorageGRID
- Configurar AutoSupport
- Administrar la configuración del nodo

Antes de empezar

- Tiene una comprensión general del sistema StorageGRID .
- Tienes conocimientos bastante detallados de shells de comandos de Linux, redes y configuración y configuración de hardware de servidor.

Comience a usar Grid Manager

Requisitos del navegador web

Debe utilizar un navegador web compatible.

Navegador web	Versión mínima compatible
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

Debes configurar la ventana del navegador a un ancho recomendado.

Ancho del navegador	Píxeles
Mínimo	1024
Óptimo	1280

Sign in en el Administrador de cuadrícula

Puede acceder a la página de inicio de sesión de Grid Manager ingresando el nombre de dominio completo (FQDN) o la dirección IP de un nodo de administración en la barra de direcciones de un navegador web compatible.

Cada sistema StorageGRID incluye un nodo de administración principal y cualquier cantidad de nodos de administración no principales. Puede iniciar sesión en Grid Manager en cualquier nodo de administración para administrar el sistema StorageGRID. Sin embargo, algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

Conectarse al grupo HA

Si los nodos de administración están incluidos en un grupo de alta disponibilidad (HA), se conectan utilizando la dirección IP virtual del grupo de HA o un nombre de dominio completo que se asigna a la dirección IP virtual. El nodo de administración principal debe seleccionarse como la interfaz principal del grupo, de modo que cuando acceda al Administrador de cuadrícula, lo haga en el nodo de administración principal, a menos que este no esté disponible. Ver ["Administrar grupos de alta disponibilidad"](#).

Usar SSO

Los pasos para iniciar sesión son ligeramente diferentes si ["Se ha configurado el inicio de sesión único \(SSO\)"](#).

Sign in en Grid Manager en el primer nodo de administración

Antes de empezar

- Tienes tus credenciales de inicio de sesión.
- Estás usando un ["navegador web compatible"](#).
- Las cookies están habilitadas en su navegador web.
- Pertenece a un grupo de usuarios que tiene al menos un permiso.
- Tienes la URL para el Administrador de Grid:

```
https://FQDN_or_Admin_Node_IP/
```

Puede utilizar el nombre de dominio completo, la dirección IP de un nodo de administración o la dirección IP virtual de un grupo de alta disponibilidad de nodos de administración.

Para acceder al Administrador de cuadrícula en un puerto distinto del puerto predeterminado para HTTPS (443), incluya el número de puerto en la URL:

```
https://FQDN_or_Admin_Node_IP:port/
```



SSO no está disponible en el puerto restringido de Grid Manager. Debes utilizar el puerto 443.

Pasos

1. Abra un navegador web compatible.
2. En la barra de direcciones del navegador, ingrese la URL del Administrador de cuadrícula.

3. Si aparece una alerta de seguridad, instale el certificado utilizando el asistente de instalación del navegador. Ver "[Administrar certificados de seguridad](#)".
4. Sign in en el Administrador de cuadrícula.

La pantalla de inicio de sesión que aparece depende de si se ha configurado el inicio de sesión único (SSO) para StorageGRID.

No usar SSO

- a. Introduzca su nombre de usuario y contraseña para el Administrador de Grid.
- b. Seleccione **Iniciar sesión**.



The screenshot shows the login interface for NetApp StorageGRID Grid Manager. At the top, the logo "NetApp StorageGRID®" is displayed, followed by the title "Grid Manager" in a large font. Below the title, there are two input fields: "Username" and "Password". The "Username" field is currently empty with a cursor at the start. Below the "Password" field is a blue "Sign in" button. At the bottom of the form, there are three links: "Tenant sign in", "NetApp support", and "NetApp.com".

Usando SSO

- Si StorageGRID utiliza SSO y esta es la primera vez que accede a la URL en este navegador:
 - i. Seleccionar * Sign in*. Puedes dejar el 0 en el campo Cuenta.



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. Ingrese sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización. Por ejemplo:

Sign in with your organizational account

Sign in

- Si StorageGRID usa SSO y usted ha accedido previamente al Administrador de Grid o a una cuenta de inquilino:
 - i. Ingrese **0** (el ID de la cuenta del Administrador de Grid) o seleccione **Administrador de Grid** si aparece en la lista de cuentas recientes.

The image shows a web interface for NetApp StorageGRID. At the top, there is a logo consisting of a square icon followed by the text "NetApp StorageGRID®". Below the logo is the heading "Sign in". Underneath the heading, there is a section labeled "Recent" with a dropdown menu showing "Grid Manager". Below that is a section labeled "Account" with a text input field containing the number "0". At the bottom of the form is a blue button with the text "Sign in". Below the button, there is a link that says "NetApp support | NetApp.com".

NetApp StorageGRID®

Sign in

Recent

Grid Manager ▼

Account

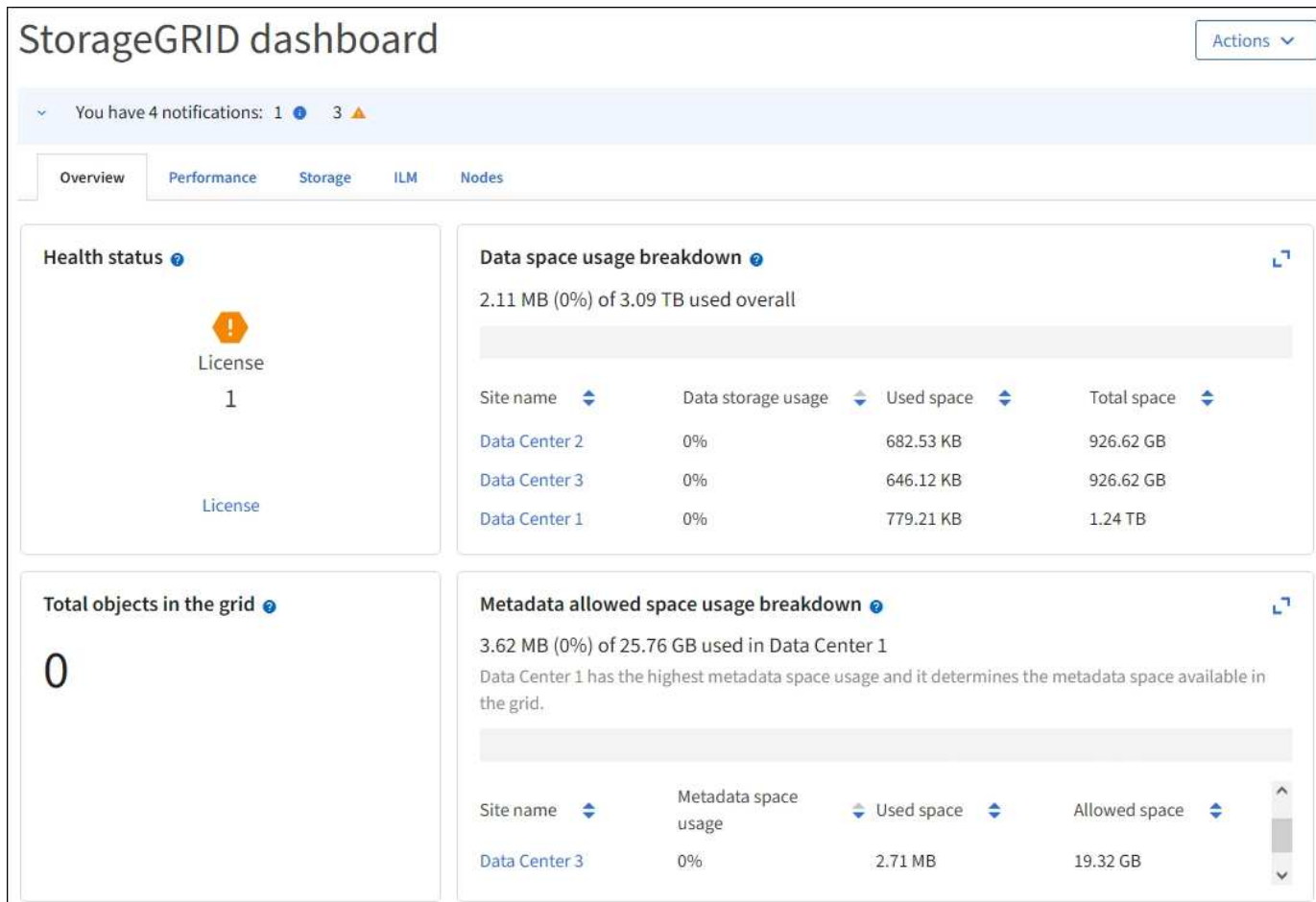
0

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. Seleccionar * Sign in*.
- iii. Sign in 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 del Grid Manager, que incluye el panel de control. Para saber qué información se proporciona, consulte ["Ver y administrar el panel de control"](#).



Iniciar sesión en otro nodo de administración

Siga estos pasos para iniciar sesión en otro nodo de administración.

No usar SSO

Pasos

1. En la barra de direcciones del navegador, ingrese el nombre de dominio completo o la dirección IP del otro nodo de administración. Incluya el número de puerto según sea necesario.
2. Introduzca su nombre de usuario y contraseña para el Administrador de Grid.
3. Seleccione **Iniciar sesión**.

Usando SSO

Si StorageGRID usa SSO y ha iniciado sesión en un nodo de administración, puede acceder a otros nodos de administración sin tener que iniciar sesión nuevamente.

Pasos

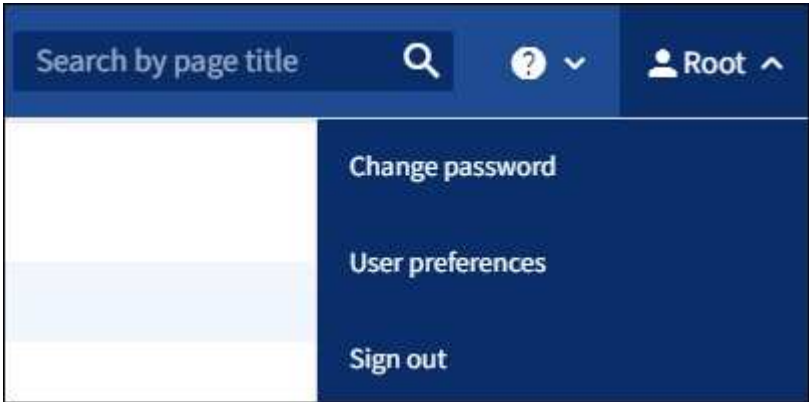
1. Ingrese el nombre de dominio completo o la dirección IP del otro nodo de administración en la barra de direcciones del navegador.
2. Si su sesión SSO ha expirado, ingrese sus credenciales nuevamente.

Cerrar sesión en Grid Manager

Cuando termine de trabajar con Grid Manager, deberá cerrar la sesión para asegurarse de que usuarios no autorizados no puedan acceder al sistema StorageGRID . Es posible que cerrar su navegador no cierre su 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	Has cerrado la sesión del nodo de administración. Se muestra la página de inicio de sesión de Grid Manager. Nota: Si inició sesión en más de un nodo de administración, deberá cerrar sesión en cada nodo.
SSO habilitado	Has cerrado la sesión de todos los nodos de administración a los que estabas accediendo. Se muestra la página de inicio de sesión de StorageGRID . Grid Manager aparece como predeterminado en el menú desplegable Cuentas recientes y el campo ID de cuenta muestra 0. Nota: Si SSO está habilitado y también ha iniciado sesión en el Administrador de inquilinos, también debe "cerrar sesión en la cuenta del inquilino" a "cerrar sesión de SSO" .

Cambiar tu contraseña

Si es un usuario local del Grid Manager, puede cambiar su propia contraseña.

Antes de empezar

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

Acerca de esta tarea

Si inicia sesión en StorageGRID como un usuario federado o si el inicio de sesión único (SSO) está habilitado, no podrá cambiar su contraseña en Grid Manager. En su lugar, debe cambiar su contraseña en la fuente de identidad externa, por ejemplo, Active Directory o OpenLDAP.

Pasos

1. Desde el encabezado del Administrador de cuadrícula, seleccione **su nombre** > **Cambiar contraseña**.
2. Introduzca su contraseña actual.
3. Escriba una nueva contraseña.

Su contraseña debe contener al menos 8 y no más de 32 caracteres. Las contraseñas distinguen entre mayúsculas y minúsculas.

4. Ingrese nuevamente la nueva contraseña.
5. Seleccione **Guardar**.

Ver la información de la licencia de StorageGRID

Puede ver la información de la licencia de su sistema StorageGRID , como la capacidad máxima de almacenamiento de su red, siempre que sea necesario.

Antes de empezar

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

Acerca de esta tarea

Si hay un problema con la licencia de software para este sistema StorageGRID , la tarjeta de estado de salud en el panel incluye un ícono de estado de licencia y un enlace **Licencia**. El número indica el número de problemas relacionados con la licencia.



Pasos

1. Acceda a la página de Licencia realizando una de las siguientes acciones:
 - Seleccione **MANTENIMIENTO** > **Sistema** > **Licencia**.
 - Desde la tarjeta de estado de salud en el panel de control, seleccione el ícono de estado de licencia o el enlace **Licencia**.

Este enlace solo aparece si hay un problema con la licencia.

2. Ver los detalles de solo lectura de la licencia actual:

- ID del sistema StorageGRID , que es el número de identificación único para esta instalación de StorageGRID
- Número de serie de la licencia
- Tipo de licencia, ya sea **Perpetua** o **Suscripción**
- Capacidad de almacenamiento licenciada de la red
- Capacidad de almacenamiento admitida
- Fecha de finalización de la licencia. **N/A** aparece para una licencia perpetua.
- Fecha de finalización del soporte

Esta fecha se lee del archivo de licencia actual y podría estar desactualizada si extendió o renovó el contrato de servicio de soporte después de obtener el archivo de licencia. Para actualizar este valor, consulte "[Actualizar la información de la licencia de StorageGRID](#)". También puede ver la fecha de finalización real del contrato utilizando Active IQ.

- Contenido del archivo de texto de la licencia

Actualizar la información de la licencia de StorageGRID

Debe actualizar la información de la licencia de su sistema StorageGRID cada vez que cambien los términos de su licencia. Por ejemplo, debe actualizar la información de la licencia si compra capacidad de almacenamiento adicional para su red.

Antes de empezar

- Tiene un nuevo archivo de licencia para aplicar a su sistema StorageGRID .
- Tienes "[permisos de acceso específicos](#)".
- Tienes la contraseña de aprovisionamiento.

Pasos

1. Seleccione **MANTENIMIENTO > Sistema > Licencia**.
2. En la sección Actualizar licencia, seleccione **Explorar**.
3. Localice y seleccione el nuevo archivo de licencia(.txt).

El nuevo archivo de licencia se valida y se muestra.

4. Introduzca la contraseña de aprovisionamiento.
5. Seleccione **Guardar**.

Utilice la API

Utilice la API de gestión de red

Puede realizar tareas de administración del sistema utilizando la API REST de administración de cuadrícula en lugar de la interfaz de usuario de Grid Manager. Por ejemplo, es posible que desee utilizar la API para automatizar operaciones o crear múltiples entidades, como usuarios, más rápidamente.

Recursos de alto nivel

La API de administración de red proporciona los siguientes recursos de nivel superior:

- `/grid`: El acceso está restringido a los usuarios de Grid Manager y se basa en los permisos de grupo configurados.
- `/org`: El acceso está restringido a los usuarios que pertenecen a un grupo LDAP local o federado para una cuenta de inquilino. Para obtener más información, consulte ["Utilice una cuenta de inquilino"](#).
- `/private`: El acceso 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 puntos finales privados de StorageGRID también ignoran la versión API de la solicitud.

Emitir solicitudes de API

La API de administración de red utiliza la plataforma API de código abierto 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 completos y documentación para cada operación de API.

Antes de empezar

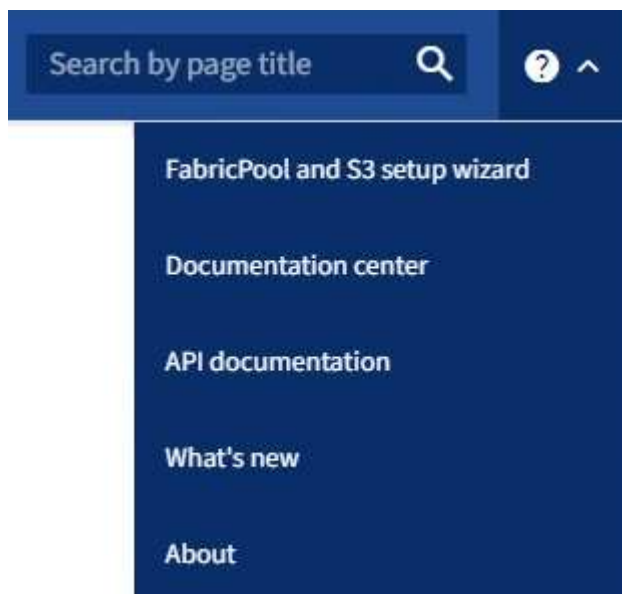
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).



Cualquier operación de API que realice utilizando la página web de Documentación de API son operaciones en vivo. Tenga cuidado de no crear, actualizar o eliminar datos de configuración u otros datos por error.

Pasos

1. Desde el encabezado de Grid Manager, seleccione el ícono de ayuda y seleccione **Documentación de API**.



2. Para realizar una operación con la API privada, seleccione **Ir a la documentación de la API privada** en la

página API de administración de StorageGRID .

Las API privadas están sujetas a cambios sin previo aviso. Los puntos finales privados de StorageGRID también ignoran la versión API de la solicitud.

3. Seleccione la operación deseada.

Cuando expande 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 URL del punto final, una lista de parámetros obligatorios u opcionales, un ejemplo del cuerpo de la solicitud (cuando sea necesario) y las posibles respuestas.

The screenshot displays the 'groups' API endpoint in the StorageGRID API Explorer. The interface is titled 'groups Operations on groups'. The selected method is 'GET' for the endpoint '/grid/groups', which is described as 'Lists Grid Administrator Groups'. A 'Try it out' button is visible in the top right corner of the parameters section.

Parameters

Name	Description
type string (query)	filter by group type Available values : local, federated --
limit integer (query)	maximum number of results Default value : 25 25
marker string (query)	marker-style pagination offset (value is Group's URN) marker - marker-style pagination offset (value
includeMarker boolean (query)	if set, the marker element is also returned --
order string (query)	pagination order (desc requires marker) Available values : asc, desc --

Responses

Response content type:

Code	Description
200	successfully retrieved Example Value Model <pre>{ "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers",</pre>

5. Determinar si la solicitud requiere parámetros adicionales, como un ID de grupo o usuario. Luego, obtenga estos valores. Es posible que primero debas emitir una solicitud API diferente para obtener la información que necesitas.
6. Determina si necesitas modificar el cuerpo de la solicitud de ejemplo. Si es así, puede seleccionar **Modelo** para conocer los requisitos de cada campo.
7. Seleccione **Probarlo**.
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 fue exitosa.

Operaciones de la API de gestión de red

La API de administración de red organiza las operaciones disponibles en las siguientes secciones.



Esta lista solo incluye operaciones disponibles en la API pública.

- **cuentas:** Operaciones para administrar cuentas de inquilinos de almacenamiento, incluida la creación de nuevas cuentas y la recuperación del uso de almacenamiento para una cuenta determinada.
- **alert-history:** Operaciones sobre alertas resueltas.
- **alert-receivers:** Operaciones sobre receptores de notificaciones de alerta (correo electrónico).
- **alert-rules:** Operaciones sobre reglas de alerta.
- **alert-silences:** Operaciones sobre silencios de alerta.
- **alertas:** Operaciones sobre alertas.
- **audit:** Operaciones para listar y actualizar la configuración de auditoría.
- **auth:** Operaciones para realizar la autenticación de la sesión del usuario.

La API de administración de red admite el esquema de autenticación de token de portador. 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/authenticate`). Si el usuario se autentica correctamente, se devuelve un token de seguridad. Este token debe proporcionarse en el encabezado de las solicitudes de API posteriores ("Autorización: Bearer *token*"). El token caduca después de 16 horas.



Si el inicio de sesión único está habilitado para el sistema StorageGRID, debe realizar diferentes pasos para autenticarse. Consulte "Autenticación en la API si el inicio de sesión único está habilitado".

Consulte "Protección contra la falsificación de solicitudes entre sitios" para obtener información sobre cómo mejorar la seguridad de la autenticación.

- **client-certificates:** Operaciones para configurar certificados de cliente para que se pueda acceder a StorageGRID de forma segura mediante herramientas de monitoreo externas.
- **config:** Operaciones relacionadas con el lanzamiento del producto y las versiones de la API de administración de cuadrícula. Puede enumerar la versión de lanzamiento del producto y las versiones principales de la API de administración de cuadrícula compatibles con esa versión, y puede deshabilitar las versiones obsoletas de la API.

- **funciones-desactivadas:** Operaciones para ver funciones que podrían haber sido desactivadas.
- **dns-servers:** Operaciones para listar y cambiar servidores DNS externos configurados.
- **drive-details:** Operaciones en unidades para modelos de dispositivos de almacenamiento específicos.
- **endpoint-domain-names:** Operaciones para enumerar y cambiar los nombres de dominio de los puntos finales de S3.
- **erasure-coding:** Operaciones sobre perfiles de codificación de borrado.
- **expansión:** Operaciones de expansión (nivel de procedimiento).
- **expansion-nodes:** Operaciones de expansión (nivel de nodo).
- **sitios-de-expansión:** Operaciones de expansión (a nivel de sitio).
- **grid-networks:** Operaciones para listar y cambiar la lista de redes de cuadrícula.
- **grid-passwords:** Operaciones para la gestión de contraseñas de la red.
- **grupos:** Operaciones para administrar grupos de administradores de grid locales y para recuperar grupos de administradores de grid federados desde un servidor LDAP externo.
- **identity-source:** Operaciones para configurar una fuente de identidad externa y sincronizar manualmente la información de usuarios y grupos federados.
- **ilm:** Operaciones sobre la gestión del ciclo de vida de la información (ILM).
- **in-progress-procedures:** recupera los procedimientos de mantenimiento que están actualmente en curso.
- **licencia:** Operaciones para recuperar y actualizar la licencia de StorageGRID .
- **logs:** Operaciones para recopilar y descargar archivos de registro.v
- **métricas:** Operaciones sobre métricas de StorageGRID , incluidas consultas de métricas instantáneas en un único punto en el tiempo y consultas de métricas de rango durante un período de tiempo. La API de administración de red utiliza la herramienta de monitoreo de sistemas Prometheus como fuente de datos de back-end. Para obtener información sobre cómo construir consultas de Prometheus, consulte el sitio web de Prometheus.



Métricas que incluyen *private* en sus nombres están destinados únicamente para uso interno. Estas métricas están sujetas a cambios entre versiones de StorageGRID sin previo aviso.

- **node-details:** Operaciones sobre los detalles del nodo.
- **node-health:** Operaciones sobre el estado de salud del nodo.
- **node-storage-state:** Operaciones sobre el estado de almacenamiento del nodo.
- **ntp-servers:** Operaciones para listar o actualizar servidores externos de Protocolo de tiempo de red (NTP).
- **objetos:** Operaciones sobre objetos y metadatos de objetos.
- **recuperación:** Operaciones para el procedimiento de recuperación.
- **recovery-package:** Operaciones para descargar el paquete de recuperación.
- **regiones:** Operaciones para ver y crear regiones.
- **s3-object-lock:** Operaciones en la configuración global de bloqueo de objetos S3.
- **server-certificate:** Operaciones para ver y actualizar los certificados del servidor de Grid Manager.
- **snmp:** Operaciones en la configuración SNMP actual.

- **storage-watermarks:** Marcas de agua del nodo de almacenamiento.
- **traffic-classes:** Operaciones para políticas de clasificación de tráfico.
- **untrusted-client-network:** Operaciones en la configuración de red de cliente no confiable.
- **usuarios:** Operaciones para ver y administrar usuarios de Grid Manager.

Control de versiones de la API de gestión de red

La API de administración de red utiliza versiones para admitir actualizaciones sin interrupciones.

Por ejemplo, esta URL de solicitud especifica la versión 4 de la API.

`https://hostname_or_ip_address/api/v4/authorize`

La versión principal de la API se actualiza cuando se realizan cambios que *no son compatibles* con versiones anteriores. La versión menor de la API se actualiza cuando se realizan cambios que *son compatibles* con versiones anteriores. Los cambios compatibles incluyen la adición de nuevos puntos finales o nuevas propiedades.

El siguiente ejemplo ilustra cómo se actualiza la versión de la API según el tipo de cambios realizados.

Tipo de cambio en la API	Versión antigua	Nueva versión
Compatible con versiones anteriores	2,1	2,2
No compatible con versiones anteriores	2,1	3,0

Cuando instala el software StorageGRID por primera vez, solo se habilita la versión más reciente de la API. Sin embargo, cuando actualiza a una nueva versión de funciones de StorageGRID, continúa teniendo acceso a la versión anterior de API durante al menos una versión de funciones de StorageGRID .



Puede configurar las versiones compatibles. Consulte la sección **config** de la documentación de la API de Swagger para obtener más información. "[API de gestión de red](#)" Para más información. Debe desactivar el soporte para la versión anterior después de actualizar todos los clientes API para usar la versión más nueva.

Las solicitudes obsoletas se marcan como obsoletas de las siguientes maneras:

- El encabezado de respuesta es "Obsoleto: verdadero".
- El cuerpo de la respuesta JSON incluye "deprecated": true
- Se agrega una advertencia obsoleta a nms.log. Por ejemplo:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determinar qué versiones de API son compatibles con la versión actual

Utilice el `GET /versions` Solicitud de API para devolver una lista de las principales versiones de API compatibles. Esta solicitud se encuentra en la sección **config** de la documentación de la API de Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Especificar una versión de API para una solicitud

Puede especificar la versión de la API utilizando un parámetro de ruta(`/api/v4`) o un encabezado(`Api-Version: 4`). Si proporciona ambos valores, el valor del encabezado anula el valor de la ruta.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protección contra la falsificación de solicitudes entre sitios (CSRF)

Puede ayudar a protegerse contra ataques de falsificación de solicitud entre sitios (CSRF) contra StorageGRID mediante el uso de tokens CSRF para mejorar la autenticación que utiliza cookies. El administrador de red y el administrador de inquilinos habilitan automáticamente esta función de seguridad; otros clientes de API pueden elegir si habilitarla cuando inician sesión.

Un atacante que puede activar una solicitud a un sitio diferente (por ejemplo, con un formulario HTTP POST) puede provocar que ciertas solicitudes se realicen utilizando las cookies del usuario que inició sesión.

StorageGRID ayuda a proteger contra ataques CSRF mediante el uso de tokens CSRF. Cuando está habilitada, el contenido de una cookie específica debe coincidir con el contenido de un encabezado específico o de un parámetro de cuerpo POST específico.

Para habilitar la función, configure el `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 cierto, una `GridCsrfToken` La cookie se establece con un valor aleatorio para los inicios de sesión en Grid Manager y `AccountCsrfToken` La cookie se establece con un valor aleatorio para los inicios 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 uno de los siguientes:

- El `X-Csrf-Token` encabezado, con el valor del encabezado establecido en el valor de la cookie del token CSRF.
- Para los puntos finales que aceptan un cuerpo codificado por formulario: A `csrfToken` parámetro del cuerpo de la solicitud codificado en formulario.

Consulte la documentación de la API en línea para obtener ejemplos y detalles adicionales.



Las solicitudes que tienen una cookie de token CSRF configurada también aplicarán el encabezado "Content-Type: application/json" para cualquier solicitud que espere un cuerpo de solicitud JSON como protección adicional contra ataques CSRF.

Utilice la API si el inicio de sesión único está habilitado

Utilice la API si el inicio de sesión único está habilitado (Active Directory)

Si tienes "[Inicio de sesión único \(SSO\) configurado y habilitado](#)" y utiliza Active Directory como proveedor de SSO, debe emitir una serie de solicitudes de API para obtener un token de autenticación que sea válido para la API de administración de Grid o la API de administración de inquilinos.

Sign in en la API si el inicio de sesión único está habilitado

Estas instrucciones se aplican si utiliza Active Directory como proveedor de identidad SSO.

Antes de empezar

- Conoce el nombre de usuario y la contraseña de SSO de un usuario federado que pertenece a un grupo de usuarios de StorageGRID .
- Si desea acceder a la API de administración de inquilinos, debe conocer el ID de la cuenta del inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar uno de los siguientes ejemplos:

- El `storagegrid-ssoauth.py` Script de Python, que se encuentra en el directorio de archivos de

instalación de StorageGRID(. /rpms para Red Hat Enterprise Linux, ./debs para Ubuntu o Debian, y ./vsphere para VMware).

- Un ejemplo de flujo de trabajo de solicitudes curl.

El flujo de trabajo curl puede expirar si lo realiza demasiado lento. Es posible que veas el error: A valid SubjectConfirmation was not found on this Response .



El flujo de trabajo curl de ejemplo no protege la contraseña para que otros usuarios no la vean.

Si tiene un problema de codificación de URL, es posible que vea el error: Unsupported SAML version .

Pasos

1. Seleccione uno de los siguientes métodos para obtener un token de autenticación:
 - Utilice el storagegrid-ssoauth.py Script de Python. Vaya al paso 2.
 - Utilice solicitudes curl. Vaya al paso 3.
2. Si desea utilizar el storagegrid-ssoauth.py script, pasa el script al intérprete de Python y ejecuta el script.

Cuando se le solicite, ingrese valores para los siguientes argumentos:

- El método SSO. Introduzca ADFS o adfs.
- El nombre de usuario de SSO
- El dominio donde está instalado StorageGRID
- La dirección de StorageGRID
- El ID de la cuenta del inquilino, si desea acceder a la API de administración 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 puedes usar el token para otras solicitudes, de manera similar a como usarías la API si no se estuviera utilizando SSO.

3. Si desea utilizar solicitudes curl, utilice 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 administración de red, utilice 0 como TENANTACCOUNTID.

- b. Para recibir una URL de autenticación firmada, emita una solicitud POST a /api/v3/authorize-saml y elimine la codificación JSON adicional de la respuesta.

Este ejemplo muestra una solicitud POST para una URL de autenticación firmada para TENANTACCOUNTID. Los resultados se transmitirán a `python -m json.tool` para eliminar 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 para este ejemplo incluye una URL firmada que está codificada como 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. Guardar el 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 del cliente de AD FS.

Una opción es solicitar el formulario de inicio de sesión utilizando 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 la solicitud del cliente:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRT0MwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Guarde el ID de la solicitud del cliente de la respuesta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Envía tus credenciales a la acción del 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=$SAMPLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS devuelve una redirección 302, con información adicional en los encabezados.



Si la autenticación multifactor (MFA) está habilitada para su sistema SSO, la publicación 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=fZHRT0MwFIZfhb...UJikvo77sXPw%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. Guardar el MSISAuth cookie de la respuesta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

- h. Envía una solicitud GET a la ubicación especificada con las cookies del POST 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 la sesión de AD FS para su uso posterior al cerrar sesión, y el cuerpo de la respuesta contiene 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
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LTNmMDgtNDRkZC04Yzg5LTQ3ND
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. Guardar el SAMLResponse del campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

- j. Usando lo guardado SAMLResponse , crear un StorageGRID/api/saml-response solicitud para

generar un token de autenticación de StorageGRID .

Para RelayState , use el ID de la cuenta del inquilino o use 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"
```

Ya puedes utilizar MYTOKEN para otras solicitudes, de forma similar a como usarías la API si no se estuviera utilizando SSO.

Cerrar sesión en la API si el inicio de sesión único está habilitado

Si se ha habilitado el inicio de sesión único (SSO), debe emitir una serie de solicitudes de API para cerrar sesión en la API de administración de red o en la API de administración de inquilinos. Estas instrucciones se aplican si está utilizando Active Directory como proveedor de identidad SSO

Acerca de esta tarea

Si es necesario, puede cerrar sesión en la API de StorageGRID cerrando la sesión desde la página de cierre de sesión única de su organización. O bien, puede activar el cierre de sesión único (SLO) desde StorageGRID, lo que requiere un token portador de StorageGRID válido.

Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase `cookie "sso=true" a la API de SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Se devuelve una URL de cierre de sesión:

```
{
  "apiVersion": "3.0",
  "data":
  "https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
  "responseTime": "2018-11-20T22:20:30.839Z",
  "status": "success"
}
```

2. Guardar 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 nuevamente a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Se devuelve la respuesta 302. La ubicación de redireccionamiento no es aplicable al cierre de sesión exclusivo de 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. Eliminar el token portador de StorageGRID .

La eliminación del token portador de StorageGRID funciona de la misma manera que sin SSO. Si no se proporciona la cookie "sso=true", el usuario cierra la sesión de StorageGRID sin afectar el estado de SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

A 204 No Content La respuesta indica que el usuario ahora ha cerrado la sesión.

```
HTTP/1.1 204 No Content
```

Utilice la API si el inicio de sesión único está habilitado (Azure)

Si tienes ["Inicio de sesión único \(SSO\) configurado y habilitado"](#) y usa Azure como proveedor de SSO, puede usar dos scripts de ejemplo para obtener un token de autenticación que sea válido para la API de administración de red o la API de administración de inquilinos.

Sign in en la API si el inicio de sesión único de Azure está habilitado

Estas instrucciones se aplican si utiliza Azure como proveedor de identidad de SSO

Antes de empezar

- Conoce la dirección de correo electrónico y la contraseña de SSO de un usuario federado que pertenece a un grupo de usuarios de StorageGRID .
- Si desea acceder a la API de administración de inquilinos, debe conocer el ID de la cuenta del inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar los siguientes scripts de ejemplo:

- El `storagegrid-ssoauth-azure.py` secuencia de comandos de Python
- El `storagegrid-ssoauth-azure.js` Script de Node.js

Ambos scripts se encuentran en el directorio de archivos de instalación de StorageGRID(`./rpms` para Red Hat Enterprise Linux, `./debs` para Ubuntu o Debian, y `./vsphere` para VMware).

Para escribir su propia integración de API con Azure, consulte la `storagegrid-ssoauth-azure.py` guion. El script de Python realiza dos solicitudes a StorageGRID directamente (primero para obtener SAMLRequest y luego 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 de SSO se pueden ejecutar mediante una serie de solicitudes de API, pero hacerlo no es sencillo. El módulo Node.js Puppeteer se utiliza para rastrear la interfaz SSO de Azure.

Si tiene un problema de codificación de URL, es posible que vea el error: `Unsupported SAML version .`

Pasos

1. Instale las dependencias necesarias, de la siguiente manera:

- a. Instalar Node.js (ver "<https://nodejs.org/en/download/>").
- b. Instale los módulos Node.js necesarios (puppeteer y jsdom):

```
npm install -g <module>
```

2. Pase el script de Python al intérprete de Python para ejecutarlo.

Luego, el script de Python llamará al script Node.js correspondiente para realizar las interacciones de SSO de Azure.

3. Cuando se le solicite, ingrese valores para los siguientes argumentos (o páselos mediante parámetros):
 - La dirección de correo electrónico SSO utilizada para iniciar sesión en Azure
 - La dirección de StorageGRID
 - El ID de la cuenta del inquilino, si desea acceder a la API de administración de inquilinos
4. Cuando se le solicite, ingrese la contraseña y prepárese para proporcionar una autorización MFA a Azure si se le 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'}
```



El script asume que la MFA se realiza mediante Microsoft Authenticator. Es posible que necesites modificar el script para admitir otras formas de MFA (como ingresar un código recibido en un mensaje de texto).

El token de autorización de StorageGRID se proporciona en la salida. Ahora puedes usar el token para otras solicitudes, de manera similar a como usarías la API si no se estuviera utilizando SSO.

Utilice la API si el inicio de sesión único está habilitado (PingFederate)

Si tienes "[Inicio de sesión único \(SSO\) configurado y habilitado](#)" y utiliza PingFederate como proveedor de SSO, debe emitir una serie de solicitudes de API para obtener un token de autenticación que sea válido para la API de administración de red o la API de administración de inquilinos.

Sign in en la API si el inicio de sesión único está habilitado

Estas instrucciones se aplican si utiliza PingFederate como proveedor de identidad SSO

Antes de empezar

- Conoce el nombre de usuario y la contraseña de SSO de un usuario federado que pertenece a un grupo de usuarios de StorageGRID .
- Si desea acceder a la API de administración de inquilinos, debe conocer el ID de la cuenta del inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puede utilizar uno de los siguientes ejemplos:

- El `storagegrid-ssoauth.py` Script de Python, que se encuentra en el directorio de archivos de instalación de StorageGRID (`./rpms` para Red Hat Enterprise Linux, `./debs` para Ubuntu o Debian, y `./vsphere` para VMware).
- Un ejemplo de flujo de trabajo de solicitudes curl.

El flujo de trabajo curl puede expirar si lo realiza demasiado lento. Es posible que veas el error: `A valid SubjectConfirmation was not found on this Response`.



El flujo de trabajo curl de ejemplo no protege la contraseña para que otros usuarios no la vean.

Si tiene un problema de codificación de URL, es posible que vea el error: `Unsupported SAML version`.

Pasos

1. Seleccione uno de los siguientes métodos para obtener un token de autenticación:
 - Utilice el `storagegrid-ssoauth.py` Script de Python. Vaya al paso 2.
 - Utilice solicitudes curl. Vaya al paso 3.
2. Si desea utilizar el `storagegrid-ssoauth.py` script, pasa el script al intérprete de Python y ejecuta el script.

Cuando se le solicite, ingrese valores para los siguientes argumentos:

- El método SSO. Puede ingresar cualquier variación de "pingfederate" (PINGFEDERATE, pingfederate, etc.).
- El nombre de usuario de SSO
- El dominio donde está instalado StorageGRID . Este campo no se utiliza para PingFederate. Puede dejarlo en blanco o ingresar cualquier valor.
- La dirección de StorageGRID
- El ID de la cuenta del inquilino, si desea acceder a la API de administración 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 puedes usar el token para otras solicitudes, de manera similar a como usarías la API si no se estuviera utilizando SSO.

3. Si desea utilizar solicitudes curl, utilice 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 administración de red, utilice 0 como TENANTACCOUNTID.

- b. Para recibir una URL de autenticación firmada, emita una solicitud POST a /api/v3/authorize-saml y elimine la codificación JSON adicional de la respuesta.

Este ejemplo muestra una solicitud POST para una URL de autenticación firmada para TENANTACCOUNTID. Los resultados se pasarán a python -m json.tool para eliminar 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 para este ejemplo incluye una URL firmada que está codificada como 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. Guardar el SAMLRequest de la respuesta para su uso en comandos posteriores.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

- d. Exportar la respuesta y la cookie, y hacer eco de la respuesta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```



```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Exporta el valor 'pf.adapterId' y repite la respuesta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Exporta el valor 'href' (elimina la barra diagonal final /) y repite la respuesta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Exportar el valor de 'acción':

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Enviar cookies junto con las credenciales:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMPLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Guardar el SAMLResponse del campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Usando lo guardado SAMLResponse , crear un StorageGRID/api/saml-response solicitud para generar un token de autenticación de StorageGRID .

Para RelayState , use el ID de la cuenta del inquilino o use 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"
```

Ya puedes utilizar MYTOKEN para otras solicitudes, de forma similar a como usarías la API si no se estuviera utilizando SSO.

Cerrar sesión en la API si el inicio de sesión único está habilitado

Si se ha habilitado el inicio de sesión único (SSO), debe emitir una serie de solicitudes de API para cerrar sesión en la API de administración de red o en la API de administración de inquilinos. Estas instrucciones se aplican si utiliza PingFederate como proveedor de identidad SSO

Acerca de esta tarea

Si es necesario, puede cerrar sesión en la API de StorageGRID cerrando la sesión desde la página de cierre de sesión única de su organización. O bien, puede activar el cierre de sesión único (SLO) desde StorageGRID, lo que requiere un token portador de StorageGRID válido.

Pasos

1. Para generar una solicitud de cierre de sesión firmada, pase `cookie "sso=true" a la API de SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Se devuelve una URL de cierre de sesión:

```
{
  "apiVersion": "3.0",
  "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
  "responseTime": "2021-10-12T22:20:30.839Z",
  "status": "success"
}
```

2. Guardar 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 nuevamente a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Se devuelve la respuesta 302. La ubicación de redireccionamiento no es aplicable al cierre de sesión exclusivo de 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. Eliminar el token portador de StorageGRID .

La eliminación del token portador de StorageGRID funciona de la misma manera que sin SSO. Si no se proporciona la cookie "sso=true", el usuario cierra la sesión de StorageGRID sin afectar el estado de SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

A 204 No Content La respuesta indica que el usuario ahora ha cerrado la sesión.

```
HTTP/1.1 204 No Content
```

Desactivar funciones con la API

Puede utilizar la API de administración de red para desactivar por completo ciertas funciones en el sistema StorageGRID . Cuando una función está desactivada, 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 evitar el acceso a ciertas funciones en el sistema StorageGRID . Desactivar una función es la única forma de evitar que el usuario root o los usuarios que pertenecen a grupos de administradores con permiso de **acceso root** puedan usar esa función.

Para comprender cómo esta funcionalidad podría ser útil, considere el siguiente escenario:

La empresa A es un proveedor de servicios que alquila 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 quiere asegurarse de que sus propios empleados nunca puedan acceder a ninguna cuenta de inquilino después de que la cuenta se haya implementado.

La empresa A puede lograr este objetivo mediante el sistema de desactivación de funciones en la API de administración de la red. Al desactivar por completo la función **Cambiar contraseña de root del inquilino** en el Administrador de Grid (tanto la UI como la API), la Compañía A garantiza que los usuarios administradores, incluido el usuario root y los usuarios que pertenecen a grupos con permiso de **Acceso root**, no puedan cambiar la contraseña de ningún usuario root de la cuenta de inquilino.

Pasos

1. Acceda a la documentación de Swagger para la API de administración de cuadrícula. Ver "[Utilice la API de gestión de red](#)".
2. Localice el punto final Desactivar funciones.
3. Para desactivar una función, como Cambiar la contraseña raíz del inquilino, envíe un cuerpo a la API como este:

```
{ "grid": { "changeTenantRootPassword": true } }
```

Cuando se completa la solicitud, la función Cambiar la contraseña raíz del inquilino se deshabilita. El permiso de administración **Cambiar contraseña de root del inquilino** ya no aparece en la interfaz de usuario, y cualquier solicitud de API que intente cambiar la contraseña de root de un inquilino fallará con "403 Prohibido".

Reactivar funciones desactivadas

De forma predeterminada, puede utilizar la API de administración de cuadrícula para reactivar una función que se ha desactivado. Sin embargo, si desea evitar que las funciones desactivadas se vuelvan a activar, puede desactivar la función **activateFeatures**.



La función **activateFeatures** no se puede reactivar. Si decide desactivar esta función, tenga en cuenta que perderá permanentemente la capacidad de reactivar cualquier otra función desactivada. Debe ponerse en contacto con el soporte técnico para restaurar cualquier funcionalidad perdida.

Pasos

1. Acceda a la documentación de Swagger para la API de administración de cuadrícula.

2. Localice el punto final Desactivar funciones.
3. Para reactivar todas las funciones, envíe un cuerpo a la API como este:

```
{ "grid": null }
```

Cuando se completa esta solicitud, se reactivan todas las funciones, incluida la función Cambiar la contraseña raíz del inquilino. El permiso de administración **Cambiar contraseña de root del inquilino** ahora aparece en la interfaz de usuario, y cualquier solicitud de API que intente cambiar la contraseña de root de un inquilino tendrá éxito, asumiendo que el usuario tiene el permiso de administración **Acceso de root** o **Cambiar contraseña de root del inquilino**.



El ejemplo anterior hace que *todas* las funciones desactivadas se reactiven. Si se han desactivado otras funciones que deben permanecer desactivadas, deberá especificarlas explícitamente en la solicitud PUT. Por ejemplo, para reactivar la función Cambiar contraseña de root del inquilino y continuar desactivando el permiso de administración de storageAdmin, envíe esta solicitud PUT:

```
{ "grid": {"storageAdmin": true} }
```

Controlar el acceso a StorageGRID

Controlar el acceso a StorageGRID

Usted controla quién puede acceder a StorageGRID y qué tareas pueden realizar los usuarios creando o importando grupos y usuarios y asignando permisos a cada grupo. Opcionalmente, puede habilitar el inicio de sesión único (SSO), crear certificados de cliente y cambiar las contraseñas de la red.

Controlar el acceso al Administrador de Grid

Usted determina quién puede acceder al Administrador de Grid y a la API de Administración de Grid importando grupos y usuarios desde un servicio de federación de identidad o configurando grupos y usuarios locales.

Usando ["federación de identidades"](#) facilita la configuración ["grupos"](#) y ["usuarios"](#) es más rápido y permite a los usuarios iniciar sesión en StorageGRID usando credenciales familiares. Puede configurar la federación de identidad si utiliza Active Directory, OpenLDAP u Oracle Directory Server.



Comuníquese con el soporte técnico si desea utilizar otro servicio LDAP v3.

Usted determina qué tareas puede realizar cada usuario asignándoles diferentes ["permisos"](#) a cada grupo. Por ejemplo, es posible que desee que los usuarios de un grupo puedan administrar las reglas de ILM y que los usuarios de otro grupo puedan realizar tareas de mantenimiento. Un usuario debe pertenecer al menos a un grupo para acceder al sistema.

Opcionalmente, puede configurar un grupo para que sea de solo lectura. Los usuarios de un grupo de solo lectura solo pueden ver configuraciones y funciones. No pueden realizar ningún cambio ni realizar ninguna operación en el Administrador de Grid ni en la API de administración de Grid.

Habilitar el inicio de sesión único

El sistema StorageGRID admite el inicio de sesión único (SSO) mediante el estándar Security Assertion

Markup Language 2.0 (SAML 2.0). Después de usted "[configurar y habilitar SSO](#)" Todos los usuarios deben estar autenticados por un proveedor de identidad externo antes de poder acceder al Administrador de Grid, al Administrador de Inquilinos, a la API de Administración de Grid o a la API de Administración de Inquilinos. Los usuarios locales no pueden iniciar sesión en StorageGRID.

Cambiar la contraseña de aprovisionamiento

La frase de contraseña de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, y para descargar el paquete de recuperación de StorageGRID . La frase de contraseña también es necesaria para descargar copias de seguridad de la información de topología de la red y de las claves de cifrado para el sistema StorageGRID . Puede "[cambiar la contraseña](#)" según sea necesario.

Cambiar las contraseñas de la consola del nodo

Cada nodo de su red tiene una contraseña de consola de nodo única, que necesita para iniciar sesión en el nodo como "admin" mediante SSH, o como usuario root en una conexión de consola física/VM. Según sea necesario, puede "[cambiar la contraseña de la consola del nodo](#)" para cada nodo.

Cambiar la contraseña de aprovisionamiento

Utilice este procedimiento para cambiar la frase de contraseña de aprovisionamiento de StorageGRID . La frase de contraseña es necesaria para los procedimientos de recuperación, expansión y mantenimiento. La frase de contraseña también es necesaria para descargar copias de seguridad del paquete de recuperación que incluyen la información de topología de la red, las contraseñas de la consola del nodo de la red y las claves de cifrado para el sistema StorageGRID .

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)" .
- Tiene permisos de acceso de mantenimiento o root.
- Tienes la contraseña de aprovisionamiento actual.

Acerca de esta tarea

La frase de contraseña de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, y para "[descargando el paquete de recuperación](#)" . La frase de contraseña de aprovisionamiento no aparece en la `Passwords.txt` archivo. Asegúrese de documentar la contraseña de aprovisionamiento y guardarla en un lugar seguro.

Pasos

1. Seleccione **CONFIGURACIÓN > Control de acceso> Contraseñas de red**.
2. En **Cambiar contraseña de aprovisionamiento**, seleccione **Realizar un cambio**
3. Introduzca su contraseña de aprovisionamiento actual.
4. Introduzca la nueva contraseña. La frase de contraseña debe contener al menos 8 y no más de 32 caracteres. Las frases de contraseña distinguen entre mayúsculas y minúsculas.
5. Guarde la nueva contraseña de aprovisionamiento en una ubicación segura. Es necesario para procedimientos de instalación, expansión y mantenimiento.
6. Vuelva a ingresar la nueva contraseña y seleccione **Guardar**.

El sistema muestra un banner de éxito verde cuando se completa el cambio de contraseña de aprovisionamiento.



Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

7. Seleccione **Paquete de recuperación**.

8. Ingrese la nueva contraseña 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 del paquete de recuperación le permite restaurar el sistema si ocurre una falla.

Cambiar las contraseñas de la consola del nodo

Cada nodo de su red tiene una contraseña de consola de nodo única, que necesita para iniciar sesión en el nodo. Utilice estos pasos para cambiar la contraseña única de la consola de cada nodo de su red.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#).
- Tú tienes el [Permiso de mantenimiento o acceso root](#).
- Tienes la contraseña 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 como usuario root en una conexión de consola física/VM. El proceso de cambio de contraseña de la consola del nodo crea nuevas contraseñas para cada nodo de su red y almacena las contraseñas en un archivo actualizado. `Passwords.txt` archivo en el paquete de recuperación. Las contraseñas aparecen en la columna Contraseña del archivo `Passwords.txt`.



Hay contraseñas de acceso SSH independientes para las claves SSH utilizadas para la comunicación entre nodos. Las contraseñas de acceso SSH no se modifican con este procedimiento.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN > Control de acceso > Contraseñas de red**.
2. En **Cambiar contraseñas de la consola del nodo**, seleccione **Realizar un cambio**.

Introduzca la contraseña de aprovisionamiento

Pasos

1. Introduzca la contraseña de aprovisionamiento para su red.
2. Seleccione **Continuar**.

Descargar el paquete de recuperación actual

Antes de cambiar las contraseñas de la consola del nodo, descargue el paquete de recuperación actual. Puede utilizar las contraseñas de este archivo si el proceso de cambio de contraseña falla para algún nodo.

Pasos

1. Seleccione **Descargar paquete de recuperación**.
2. Copiar el archivo del paquete de recuperación(.zip) a dos lugares seguros, protegidos y separados.



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

3. Seleccione **Continuar**.
4. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí** si está listo para comenzar a cambiar las contraseñas de la consola del nodo.

No puedes cancelar este proceso una vez iniciado.

Cambiar las contraseñas de la consola del nodo

Cuando se inicia el proceso de contraseña de la consola del nodo, se genera un nuevo paquete de recuperación que incluye las nuevas contraseñas. Luego, 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 se complete la descarga:
 - a. Abrir 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. Copiar el nuevo archivo del paquete de recuperación(.zip) a dos lugares seguros, protegidos y separados.



No sobrescriba el paquete de recuperación antiguo.

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

4. Seleccione la casilla de verificación para indicar que ha descargado el nuevo paquete de recuperación y verificado el contenido.
5. Seleccione **Cambiar contraseñas de la consola del nodo** y espere a que todos los nodos se actualicen con las nuevas contraseñas. Esto podría tardar unos minutos.

Si se cambian las contraseñas de todos los nodos, aparece un banner de éxito verde. Vaya al siguiente paso.

Si se produce un error durante el proceso de actualización, aparecerá un mensaje con la lista de nodos que no pudieron cambiar sus contraseñas. El sistema volverá a intentar automáticamente el proceso en cualquier nodo cuya contraseña no se haya podido cambiar. Si el proceso finaliza con algunos nodos que aún no tienen la contraseña cambiada, aparece el botón **Reintentar**.

Si la actualización de contraseña falló para uno o más nodos:

- a. Revise los mensajes de error enumerados en la tabla.
- b. Resolver los problemas.
- c. Seleccione **Reintentar**.



Al volver a intentarlo solo se cambian las contraseñas de la consola de nodo en los nodos que fallaron durante intentos anteriores de cambio de contraseña.

6. Después de cambiar las contraseñas de la consola de nodo para todos los nodos, elimine el archivo [primer paquete de recuperación que descargaste](#) .
7. Opcionalmente, utilice el enlace **Paquete de recuperación** para descargar una copia adicional del nuevo paquete de recuperación.

Cambiar las contraseñas de acceso SSH para los nodos de administración

Al cambiar las contraseñas de acceso SSH para los nodos de administración también se actualizan los conjuntos únicos de claves SSH internas para cada nodo de la red. El nodo de administración principal utiliza estas claves SSH para acceder a los nodos mediante una autenticación segura y sin contraseña.

Utilice una clave SSH para iniciar sesión en un nodo como `admin` o al usuario `root` en una máquina virtual o conexión de consola física.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de mantenimiento o acceso root"](#) .
- Tienes la contraseña de aprovisionamiento actual.

Acerca de esta tarea

Las nuevas contraseñas de acceso para los nodos de administración y las nuevas claves internas para cada nodo se almacenan en el `Passwords.txt` archivo en el paquete de recuperación. Las claves se enumeran en la columna Contraseña de ese archivo.

Hay contraseñas de acceso SSH independientes para las claves SSH utilizadas para la comunicación entre nodos. Estos no se modifican con este procedimiento.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN > Control de acceso > Contraseñas de red**.
2. En **Cambiar claves SSH**, seleccione **Realizar un cambio**.

Descargar el paquete de recuperación actual

Antes de cambiar las claves de acceso SSH, descargue el paquete de recuperación actual. Puede utilizar las claves de este archivo si el proceso de cambio de clave falla para algún nodo.

Pasos

1. Introduzca la contraseña de aprovisionamiento para su red.
2. Seleccione **Descargar paquete de recuperación**.

3. Copiar el archivo del paquete de recuperación(.zip) a dos lugares seguros, protegidos y separados.



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

4. Seleccione **Continuar**.
5. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí** si está listo para comenzar a cambiar las claves de acceso SSH.



No puedes cancelar este proceso una vez iniciado.

Cambiar las claves de acceso SSH

Cuando se inicia el proceso de cambio de claves de acceso SSH, se genera un nuevo paquete de recuperación que incluye las nuevas claves. Luego, las claves se actualizan en cada nodo.

Pasos

1. Espere a que se genere el nuevo paquete de recuperación, lo que puede tardar unos minutos.
2. Cuando el botón Descargar nuevo paquete de recuperación esté habilitado, seleccione **Descargar nuevo paquete de recuperación** y guarde el archivo del nuevo paquete de recuperación(.zip) a dos lugares seguros, protegidos y separados.
3. Cuando se complete la descarga:
 - a. Abrir el .zip archivo.
 - b. Confirme que puede acceder al contenido, incluido el Passwords.txt archivo, que contiene las nuevas claves de acceso SSH.
 - c. Copiar el nuevo archivo del paquete de recuperación(.zip) a dos lugares seguros, protegidos y separados.



No sobrescriba el paquete de recuperación antiguo.

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

4. Espere a que las claves se actualicen en cada nodo, lo que puede demorar unos minutos.

Si se cambian las claves de todos los nodos, aparece un banner de éxito verde.

Si se produce un error durante el proceso de actualización, un mensaje de banner enumera la cantidad de nodos cuyas claves no se pudieron cambiar. El sistema volverá a intentar automáticamente el proceso en cualquier nodo cuya clave no haya sido cambiada. Si el proceso finaliza con algunos nodos que aún no tienen una clave modificada, aparece el botón **Reintentar**.

Si la actualización de la clave falló para uno o más nodos:

- a. Revise los mensajes de error enumerados en la tabla.
- b. Resolver los problemas.
- c. Seleccione **Reintentar**.

Al volver a intentarlo solo se cambian las claves de acceso SSH en los nodos que fallaron durante intentos de cambio de clave anteriores.

- Después de cambiar las claves de acceso SSH para todos los nodos, elimine el archivo [primer paquete de recuperación que descargaste](#) .
- Opcionalmente, seleccione **MANTENIMIENTO > Sistema > Paquete de recuperación** para descargar una copia adicional del nuevo paquete de recuperación.

Utilizar 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 usando credenciales familiares.

Configurar la federación de identidades para Grid Manager

Puede configurar la federación de identidad en Grid Manager si desea que los grupos de administradores y los usuarios se administren en otro sistema, como Active Directory, Azure Active Directory (Azure AD), OpenLDAP u Oracle Directory Server.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Está utilizando Active Directory, Azure AD, OpenLDAP u Oracle Directory Server como proveedor de identidad.



Si desea utilizar un servicio LDAP v3 que no figura en la lista, comuníquese con el soporte técnico.

- Si planea utilizar OpenLDAP, debe configurar el servidor OpenLDAP. Ver [Directrices para configurar un servidor OpenLDAP](#) .
- Si planea habilitar el inicio de sesión único (SSO), ha revisado la ["Requisitos y consideraciones para el inicio de sesión único"](#) .
- Si planea utilizar Seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidad utiliza TLS 1.2 o 1.3. Ver ["Cifrados compatibles para conexiones TLS salientes"](#) .

Acerca de esta tarea

Puede configurar una fuente de identidad para Grid Manager si desea importar grupos desde 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, según los permisos de administración asignados al grupo.
- Grupos de usuarios inquilinos para inquilinos que no utilizan su propia fuente de identidad. Los usuarios de los grupos de inquilinos pueden iniciar sesión en el Administrador de inquilinos y realizar tareas, según los permisos asignados al grupo en el Administrador de inquilinos. Ver ["Crear una cuenta de inquilino"](#) y ["Utilice una cuenta de inquilino"](#) Para más detalles.

Entrar a la configuración

Pasos

1. Seleccione **CONFIGURACIÓN > Control de acceso > Federación de identidades**.
2. Seleccione **Habilitar federación de identidad**.
3. En la sección Tipo de servicio LDAP, seleccione el tipo de servicio LDAP que desea configurar.

Ldap service type

Select the type of LDAP service you want to configure.

Active Directory

Azure

OpenLDAP

Other

Seleccione **Otro** para configurar valores para un servidor LDAP que utiliza Oracle Directory Server.

4. Si seleccionó **Otro**, complete los campos en la sección Atributos LDAP. De lo contrario, vaya al siguiente paso.
 - **Nombre único de usuario:** el 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 está configurando Oracle Directory Server, ingrese `uid`.
 - **UUID de usuario:** el 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 está configurando Oracle Directory Server, ingrese `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:** el 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 está configurando Oracle Directory Server, ingrese `cn`.
 - **UUID de grupo:** el 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 está configurando Oracle Directory Server, ingrese `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 servicios LDAP, ingrese la información de conexión de red y servidor LDAP requerida en la sección Configurar servidor LDAP.
 - **Nombre de host:** 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, puedes utilizar cualquier puerto siempre que tu firewall esté configurado correctamente.

- **Nombre de usuario:** La ruta completa del nombre distinguido (DN) del 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 acceder a los siguientes atributos:

- `sAMAccountName` o `uid`
- `objectGUID`, `entryUUID`, o `nsuniqueid`
- `cn`
- `memberOf` o `isMemberOf`
- **Directorio Activo:** `objectSid`, `primaryGroupID`, `userAccountControl`, y `userPrincipalName`
- **Azur:** `accountEnabled` y `userPrincipalName`

- **Contraseña:** La contraseña asociada al nombre de usuario.



Si cambia la contraseña en el futuro, deberá actualizarla en esta página.

- **DN base de grupo:** la ruta completa del nombre distinguido (DN) de un subárbol LDAP en el que desea buscar grupos. En el ejemplo de Active Directory (abajo), todos los grupos cuyo nombre distintivo es relativo al DN base (`DC=storagegrid,DC=example,DC=com`) se pueden usar como grupos federados.



Los valores de **Nombre único del grupo** deben ser únicos dentro del **DN base del grupo** al que pertenecen.

- **DN base de usuario:** la ruta completa del nombre distinguido (DN) de un subárbol LDAP en el 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 vinculado** (opcional): el patrón de nombre de usuario predeterminado que StorageGRID debe usar si el patrón no se puede determinar automáticamente.

Se recomienda proporcionar **Formato de nombre de usuario de enlace** porque puede permitir que los usuarios inicien sesión si StorageGRID no puede vincularse 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 distinguido:** `CN=[USERNAME],CN=Users,DC=example,DC=com`

Incluya **[NOMBRE DE USUARIO]** exactamente como está escrito.

6. En la sección Seguridad de la capa de transporte (TLS), seleccione una configuración de seguridad.

- **Usar STARTTLS:** utilice STARTTLS para proteger 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.

- **Usar LDAPS:** La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debe seleccionar esta opción para Azure.
- **No utilizar TLS:** El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Azure.



No se admite el uso de la opción **No usar TLS** si su servidor de Active Directory aplica la firma LDAP. Debe utilizar STARTTLS o LDAPS.

7. Si seleccionó STARTTLS o LDAPS, elija el certificado utilizado para proteger la conexión.

- **Usar certificado CA del sistema operativo:** utilice el certificado CA de Grid predeterminado instalado en el sistema operativo para proteger las conexiones.
- **Usar certificado CA personalizado:** utilice un certificado de seguridad personalizado.

Si selecciona esta configuración, 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 ingresar todos los valores, debe probar la conexión antes de poder guardar la configuración. StorageGRID verifica la configuración de conexión para el servidor LDAP y el formato de nombre de usuario vinculado, si proporcionó uno.

Pasos

1. Seleccione **Probar conexión**.
2. Si no proporcionó un formato de nombre de usuario vinculado:
 - Aparecerá el mensaje "Conexión de prueba exitosa" si la configuración de conexión es válida. Seleccione **Guardar** para guardar la configuración.
 - Aparece el mensaje "No se pudo establecer la conexión de prueba" si la configuración de conexión no es válida. Seleccione **Cerrar**. Luego, resuelva cualquier problema y pruebe la conexión nuevamente.
3. Si proporcionó un formato de nombre de usuario vinculado, ingrese el nombre de usuario y la contraseña de un usuario federado válido.

Por ejemplo, ingrese su propio nombre de usuario y contraseña. No incluya ningún carácter especial en el nombre de usuario, como @ o /.

Test Connection

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

[Cancel](#) [Test Connection](#)

- Aparecerá el mensaje "Conexión de prueba exitosa" si la configuración de conexión es válida. Seleccione **Guardar** para guardar la configuración.
- Aparece un mensaje de error si la configuración de conexión, el formato de nombre de usuario vinculado o el nombre de usuario y la contraseña de prueba no son válidos. Resuelva cualquier problema y pruebe la conexión nuevamente.

Forzar la sincronización con la fuente de identidad

El sistema StorageGRID sincroniza periódicamente los grupos y usuarios federados desde la fuente de identidad. Puede forzar el inicio de la sincronización si desea habilitar o restringir los permisos de usuario lo más rápido posible.

Pasos

1. Vaya a la página de federación de identidad.
2. Seleccione **Servidor de sincronización** en la parte superior de la página.

El proceso de sincronización puede tardar algún tiempo dependiendo de su entorno.



La alerta **Error de sincronización de federación de identidad** se activa si hay un problema al sincronizar grupos y usuarios federados desde la fuente de identidad.

Deshabilitar la federación de identidades

Puede deshabilitar temporal o permanentemente la federación de identidad para grupos y usuarios. Cuando la federación de identidad está deshabilitada, no hay comunicación entre StorageGRID y la fuente de identidad. Sin embargo, cualquier configuración que haya realizado se conservará, lo que le permitirá volver a habilitar fácilmente la federación de identidad en el futuro.

Acerca de esta tarea

Antes de deshabilitar la federación de identidad, debe tener en cuenta lo siguiente:

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que actualmente hayan iniciado sesión conservarán el acceso al sistema StorageGRID hasta que su sesión expire, pero no podrán iniciar sesión una vez que expire su sesión.

- No se producirá sincronización entre el sistema StorageGRID y la fuente de identidad, y no se generarán alertas para las cuentas que no se hayan sincronizado.
- La casilla de verificación **Habilitar federación de identidad** está deshabilitada si el inicio de sesión único (SSO) está configurado en **Habilitado** o **Modo Sandbox**. El estado de SSO en la página de inicio de sesión único debe ser **Deshabilitado** antes de poder deshabilitar la federación de identidad. Ver ["Deshabilitar el inicio de sesión único"](#).

Pasos

1. Vaya a la página de federación de identidad.
2. Desmarque la casilla de verificación **Habilitar federación de identidad**.

Directrices para configurar un servidor OpenLDAP

Si desea utilizar un servidor OpenLDAP para la federación de identidad, debe configurar ajustes específicos en el servidor OpenLDAP.



Para las fuentes de identidad que no sean ActiveDirectory o Azure, StorageGRID no bloqueará automáticamente el acceso a S3 a los usuarios que estén deshabilitados externamente. Para bloquear el acceso a S3, elimine todas las claves S3 del usuario o elimine el usuario de todos los grupos.

Superposiciones de miembros y refinaciones

Las superposiciones memberof y refint deben estar habilitadas. Para obtener más información, consulte las instrucciones para el mantenimiento inverso de la membresía del grupo en <http://www.openldap.org/doc/admin24/index.html> ["Documentación de OpenLDAP: Guía del administrador de la versión 2.4"].

Indexación

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 el nombre de usuario estén indexados para un rendimiento óptimo.

Consulte la información sobre el mantenimiento de la membresía del grupo inverso en <http://www.openldap.org/doc/admin24/index.html> ["Documentación de OpenLDAP: Guía del administrador de la versión 2.4"].

Administrar grupos de administradores

Puede crear grupos de administradores para administrar los permisos de seguridad de uno o más usuarios administradores. Los usuarios deben pertenecer a un grupo para tener acceso al sistema StorageGRID.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Si planea importar un grupo federado, ha configurado la federación de identidad y el grupo federado ya existe en la fuente de identidad configurada.

Crear un grupo de administradores

Los grupos de administradores le permiten determinar qué usuarios pueden acceder a qué funciones y operaciones en el Administrador de Grid y la API de administración de Grid.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN > Control de acceso > Grupos de administradores**.
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 usuarios locales.
- Cree un grupo federado para importar usuarios desde la fuente de identidad.

Grupo local

Pasos

1. Seleccione **Grupo local**.
2. Introduzca un nombre para mostrar para el grupo, que podrá actualizar más tarde según sea necesario. Por ejemplo, "Usuarios de mantenimiento" o "Administradores de ILM".
3. Introduzca un nombre único para el grupo, que no podrá actualizar más tarde.
4. Seleccione **Continuar**.

Grupo federado

Pasos

1. Seleccione **Grupo federado**.
2. Ingrese el nombre del grupo que desea importar, exactamente como aparece en la fuente de identidad configurada.
 - Para Active Directory y Azure, utilice sAMAccountName.
 - Para OpenLDAP, utilice el CN (nombre común).
 - Para otro LDAP, utilice el nombre único apropiado para el servidor LDAP.
3. Seleccione **Continuar**.

Administrar permisos de grupo

Pasos

1. Para **Modo de acceso**, seleccione si los usuarios del grupo pueden cambiar configuraciones y realizar operaciones en el Administrador de cuadrícula y la API de administración de cuadrícula o si solo pueden ver configuraciones y funciones.
 - **Lectura y escritura** (predeterminado): los usuarios pueden cambiar la configuración y realizar las operaciones permitidas por sus permisos de administración.
 - **Solo lectura**: los usuarios solo pueden ver configuraciones y funciones. No pueden realizar ningún cambio ni realizar ninguna operación en el Administrador de Grid ni en la API de administración de Grid. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.



Si un usuario pertenece a varios grupos y alguno de ellos está configurado como **Solo lectura**, el usuario tendrá acceso de solo lectura a todas las configuraciones y funciones seleccionadas.

2. Seleccione uno o más "[permisos del grupo de administradores](#)".

Debe asignar al menos un permiso a cada grupo; de lo contrario, los usuarios que pertenecen 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**.

Agregar usuarios (solo grupos locales)

Pasos

1. Opcionalmente, seleccione uno o más usuarios locales para este grupo.

Si aún no ha creado usuarios locales, puede guardar el grupo sin agregar usuarios. Puede agregar este grupo al usuario en la página Usuarios. Ver "[Administrar usuarios](#)" Para más detalles.

2. Seleccione **Crear grupo y Finalizar**.

Ver y editar grupos de administradores

Puede ver detalles de grupos existentes, modificar un grupo o duplicar un grupo.

- Para ver información básica de todos los grupos, revise la tabla en 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 de acciones	Página de 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.

Tarea	Menú de acciones	Página de detalles
Editar nombre para mostrar (solo grupos locales)	a. Seleccione la casilla de verificación del grupo. b. Seleccione Acciones > Editar nombre del 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 .
Editar el modo de acceso o los permisos	a. Seleccione la casilla de verificación del grupo. b. Seleccione Acciones > Ver detalles del grupo . c. Opcionalmente, cambie el modo de acceso del grupo. d. Opcionalmente, seleccione o desmarque " permisos del grupo de administradores ". e. Seleccione Guardar cambios .	a. Seleccione el nombre del grupo para mostrar los detalles. b. Opcionalmente, cambie el modo de acceso del grupo. c. Opcionalmente, seleccione o desmarque " permisos del grupo de administradores ". d. Seleccione Guardar cambios .

Duplicar un grupo

Pasos

1. Seleccione la casilla de verificación del grupo.
2. Seleccione **Acciones > Duplicar grupo**.
3. Complete el asistente para duplicar grupo.

Eliminar un grupo

Puede eliminar un grupo de administradores cuando desee eliminar el grupo del sistema y eliminar todos los permisos asociados con el grupo. Al eliminar un grupo de administradores se eliminan todos los usuarios del grupo, pero no se eliminan los usuarios mismos.

Pasos

1. Desde la página Grupos, seleccione la casilla de verificación de cada grupo que desee eliminar.
2. Seleccione **Acciones > Eliminar grupo**.
3. Seleccione **Eliminar grupos**.

Permisos del grupo de administradores

Al crear grupos de usuarios administradores, selecciona uno o más permisos para controlar el acceso a funciones específicas del Administrador de cuadrícula. Luego puede asignar cada usuario a uno o más de estos grupos de administración para determinar qué tareas puede realizar ese usuario.

Debe asignar al menos un permiso a cada grupo; de lo contrario, los usuarios que pertenecen a ese grupo no

podrán iniciar sesión en Grid Manager ni en la API de administración de Grid.

De forma predeterminada, cualquier usuario que pertenezca a un grupo que tenga al menos un permiso puede realizar las siguientes tareas:

- Sign in en el Administrador de cuadrícula
- Ver el panel de control
- Ver las páginas de Nodos
- Ver alertas actuales y resueltas
- Cambiar su propia contraseña (sólo usuarios locales)
- Ver cierta información proporcionada en las páginas de Configuración y Mantenimiento

Interacción entre permisos y modo de acceso

Para todos los permisos, la configuración **Modo de acceso** del grupo determina si los usuarios pueden cambiar configuraciones y realizar operaciones o si solo pueden ver las configuraciones y funciones relacionadas. Si un usuario pertenece a varios grupos y alguno de ellos está configurado como **Solo lectura**, el usuario tendrá acceso de solo lectura a todas las configuraciones y funciones seleccionadas.

Las siguientes secciones describen los permisos que puede asignar al crear o editar un grupo de administradores. Cualquier funcionalidad no mencionada explícitamente requiere el permiso de **acceso root**.

Acceso root

Este permiso proporciona acceso a todas las funciones de administración de la red.

Cambiar la contraseña raíz del inquilino

Este permiso proporciona acceso a la opción **Cambiar contraseña root** en la página Inquilinos, lo que le permite controlar quién puede cambiar la contraseña del usuario root local del inquilino. Este permiso también se utiliza para migrar claves S3 cuando la función de importación de claves S3 está habilitada. Los usuarios que no tienen este permiso no pueden ver la opción **Cambiar contraseña root**.



Para otorgar acceso a la página Inquilinos, que contiene la opción **Cambiar contraseña root**, asigne también el permiso **Cuentas de inquilinos**.

Configuración de la página de topología de cuadrícula

Este permiso proporciona acceso a las pestañas de Configuración en la página **SOPORTE > Herramientas > Topología de cuadrícula**.



La página de topología de cuadrícula ha quedado obsoleta y se eliminará en una versión futura.

ILM

Este permiso proporciona acceso a las siguientes opciones del menú **ILM**:

- Normas
- Políticas
- Etiquetas de política

- Pools de almacenamiento
- Grados de almacenamiento
- Regiones
- Búsqueda de metadatos de objetos



Los usuarios deben tener los permisos **Otra configuración de red** y **Configuración de página de topología de red** para administrar los niveles de almacenamiento.

Mantenimiento

Los usuarios deben tener el permiso de Mantenimiento para utilizar estas opciones:

- **CONFIGURACIÓN > Control de acceso:**
 - Contraseñas de la red
- **CONFIGURACIÓN > Red:**
 - Nombres de dominio de punto final S3
- **MANTENIMIENTO > Tareas:**
 - Desmantelamiento
 - Expansión
 - Comprobación de existencia de objetos
 - Recuperación
- **MANTENIMIENTO > Sistema:**
 - Paquete de recuperación
 - Actualización de software
- **SOPORTE > Herramientas:**
 - Registros

Los usuarios que no tienen el permiso de Mantenimiento pueden ver, pero no editar, estas páginas:

- **MANTENIMIENTO > Red:**
 - servidores DNS
 - Red de cuadrícula
 - servidores NTP
- **MANTENIMIENTO > Sistema:**
 - Licencia
- **CONFIGURACIÓN > Red:**
 - Nombres de dominio de punto final S3
- **CONFIGURACIÓN > Seguridad:**
 - Certificados
- **CONFIGURACIÓN > Monitoreo:**
 - Servidor de auditoría y syslog

Administrar alertas

Este permiso proporciona acceso a opciones para administrar alertas. Los usuarios deben tener este permiso para administrar silencios, notificaciones de alerta y reglas de alerta.

Consulta de métricas

Este permiso proporciona acceso a:

- **SOPORTE > Herramientas > Página Métricas**
- Consultas de métricas de Prometheus personalizadas mediante la sección **Métricas** de la API de administración de cuadrícula
- Tarjetas del panel de control de Grid Manager que contienen métricas

Búsqueda de metadatos de objetos

Este permiso proporciona acceso a la página **ILM > Búsqueda de metadatos de objetos**.

Otra configuración de red

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 la página de topología de cuadrícula**.

- **ILM:**
 - Grados de almacenamiento
- **CONFIGURACIÓN > Sistema:**
- **SOPORTE > Otro:**
 - Costo del enlace

Administrador de dispositivos de almacenamiento

Este permiso proporciona:

- Acceso al E-Series SANtricity System Manager en dispositivos de almacenamiento a través del Grid Manager.
- La capacidad de realizar tareas de resolución de problemas y mantenimiento en la pestaña Administrar unidades para dispositivos que admiten estas operaciones.

Cuentas de inquilinos

Este permiso proporciona la capacidad de:

- Acceda a la página Inquilinos, donde puede crear, editar y eliminar cuentas de inquilinos
- Ver las políticas de clasificación de tráfico existentes
- Ver las tarjetas del panel de Grid Manager que contienen detalles de los inquilinos

Administrar usuarios

Puede ver usuarios locales y federados. También puede crear usuarios locales y asignarlos a grupos de administradores locales para determinar a qué funciones de Grid Manager pueden acceder estos usuarios.

Antes de empezar

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

Crear un usuario local

Puede crear uno o más usuarios locales y asignar cada usuario a uno o más grupos locales. Los permisos del grupo controlan a qué funciones de Grid Manager y Grid Management API puede acceder el usuario.

Sólo puedes crear usuarios locales. Utilice la fuente de identidad externa para administrar usuarios y grupos federados.

El administrador de cuadrícula incluye un usuario local predefinido, llamado "root". No puedes eliminar el usuario root.



Si el inicio de sesión único (SSO) está habilitado, los usuarios locales no pueden iniciar sesión en StorageGRID.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN > Control de acceso > Usuarios administradores**.
2. Seleccione **Crear usuario**.

Ingrese las credenciales de usuario

Pasos

1. Introduzca el nombre completo del usuario, un nombre de usuario único y una contraseña.
2. Opcionalmente, seleccione **Sí** si este usuario no debe tener acceso al Administrador de Grid o a la API de administración de Grid.
3. Seleccione **Continuar**.

Asignar a grupos

Pasos

1. Opcionalmente, asigne el usuario a uno o más grupos para determinar los permisos del usuario.

Si aún no ha creado grupos, puede guardar el usuario sin seleccionar grupos. Puede agregar este usuario a un grupo en la página Grupos.

Si un usuario pertenece a varios grupos, los permisos son acumulativos. Ver ["Administrar grupos de administradores"](#) Para más detalles.

2. Seleccione **Crear usuario** y seleccione **Finalizar**.

Ver y editar usuarios locales

Puede ver detalles de los usuarios locales y federados existentes. Puede modificar un usuario local para cambiar su nombre completo, contraseña o membresía de grupo. También puede impedir temporalmente que un usuario acceda al Administrador de Grid y a la API de administración de Grid.

Sólo puedes editar usuarios locales. Utilice la fuente de identidad externa para administrar usuarios federados.

- Para ver información básica de todos los usuarios locales y federados, revise la tabla en la página Usuarios.
- 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.

Cualquier edición se aplicará la próxima vez que el usuario cierre sesión y vuelva a iniciar sesión en el Administrador de cuadrícula.



Los usuarios locales pueden cambiar sus propias contraseñas utilizando la opción **Cambiar contraseña** en el banner de Grid Manager.

Tarea	Menú de acciones	Página de detalles
Ver detalles del usuario	- Seleccione la casilla de verificación para el usuario. - Seleccione Acciones > Ver detalles del usuario.	Seleccione el nombre del usuario en la tabla.
Editar nombre completo (solo usuarios locales)	- Seleccione la casilla de verificación para el usuario. - Seleccione Acciones > Editar nombre completo. - Introduzca el nuevo nombre. - Seleccione Guardar cambios.	- Seleccione el nombre del usuario para mostrar los detalles. - Seleccione el icono de edición . - Introduzca el nuevo nombre. - Seleccione Guardar cambios.
Denegar o permitir el acceso a StorageGRID	- Seleccione la casilla de verificación para el usuario. - Seleccione Acciones > Ver detalles del usuario. - Seleccione la pestaña Acceso. - Seleccione Sí para evitar que el usuario inicie sesión en Grid Manager o en la API de administración de Grid, o seleccione No para permitir que el usuario inicie sesión. - Seleccione Guardar cambios.	- Seleccione el nombre del usuario para mostrar los detalles. - Seleccione la pestaña Acceso. - Seleccione Sí para evitar que el usuario inicie sesión en Grid Manager o en la API de administración de Grid, o seleccione No para permitir que el usuario inicie sesión. - Seleccione Guardar cambios.

Tarea	Menú de acciones	Página de detalles
Cambiar contraseña (sólo usuarios locales)	a. Seleccione la casilla de verificación para el usuario. b. Seleccione Acciones > Ver detalles del usuario . c. Seleccione la pestaña Contraseña. d. Introduzca una nueva contraseña. e. Seleccione Cambiar contraseña .	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la pestaña Contraseña. c. Introduzca una nueva contraseña. d. Seleccione Cambiar contraseña .
Cambiar grupos (solo usuarios locales)	a. Seleccione la casilla de verificación para el usuario. b. Seleccione Acciones > Ver detalles del usuario . c. Seleccione la pestaña Grupos. d. Opcionalmente, seleccione el enlace después del nombre de un grupo para ver los detalles del grupo en una nueva pestaña del navegador. 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 pestaña Grupos. c. Opcionalmente, seleccione el enlace después del nombre de un grupo para ver los detalles del grupo en una nueva pestaña del navegador. d. Seleccione Editar grupos para seleccionar diferentes grupos. e. Seleccione Guardar cambios .

Duplicar un usuario

Puede duplicar un usuario existente para crear un nuevo usuario con los mismos permisos.

Pasos

1. Seleccione la casilla de verificación para el usuario.
2. Seleccione **Acciones > Duplicar usuario**.
3. Complete el asistente para duplicar usuarios.

Eliminar un usuario

Puede eliminar un usuario local para eliminarlo permanentemente del sistema.



No puedes eliminar el usuario root.

Pasos

1. Desde la página Usuarios, seleccione la casilla de verificación de cada usuario que desee eliminar.
2. Seleccione **Acciones > Eliminar usuario**.
3. Seleccione **Eliminar usuario**.

Utilice el inicio de sesión único (SSO)

Configurar el inicio de sesión único

Cuando el inicio de sesión único (SSO) está habilitado, los usuarios solo pueden acceder a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API si sus credenciales están autorizadas mediante el proceso de inicio de sesión SSO implementado por su 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) mediante el estándar Security Assertion Markup Language 2.0 (SAML 2.0).

Antes de habilitar el inicio de sesión único (SSO), revise cómo se ven afectados los procesos de inicio y cierre de sesión de StorageGRID cuando se habilita el SSO.

Sign in cuando el SSO esté habilitado

Cuando SSO está habilitado e inicia sesión en StorageGRID, se lo redirige a la página SSO de su organización para validar sus credenciales.

Pasos

1. Ingrese el nombre de dominio completo o la dirección IP de cualquier nodo de administración de StorageGRID en un navegador web.

Aparece la página de Sign in de StorageGRID .

- Si es la primera vez que accede a la URL en este navegador, se le solicitará un ID de cuenta:



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- Si ya ha accedido al Administrador de red o al Administrador de inquilinos, se le solicitará que seleccione una cuenta reciente o que ingrese un ID de cuenta:



Tenant Manager

Recent

Account

Sign in

[NetApp support](#) | [NetApp.com](#)



La página de Sign in de StorageGRID no se muestra cuando ingresa la URL completa para 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 SSO de su organización, donde puede [Inicie sesión con sus credenciales de SSO](#).

2. Indique si desea acceder al Administrador de red o al Administrador de inquilinos:

- Para acceder al Administrador de cuadrícula, deje el campo **ID de cuenta** en blanco, ingrese **0** como ID de cuenta o seleccione **Administrador de cuadrícula** si aparece en la lista de cuentas recientes.
- Para acceder al Administrador de inquilinos, ingrese el ID de la cuenta del inquilino de 20 dígitos o seleccione un inquilino por nombre si aparece en la lista de cuentas recientes.

3. Seleccionar * Sign in*

StorageGRID lo redirecciona a la página de inicio de sesión SSO de su organización. Por ejemplo:

Sign in with your organizational account

someone@example.com

Password

Sign in

4. Sign in con sus credenciales SSO.

Si sus credenciales de SSO son correctas:

- El proveedor de identidad (IdP) proporciona una respuesta de autenticación a StorageGRID.
- StorageGRID valida la respuesta de autenticación.
- Si la respuesta es válida y usted pertenece a un grupo federado con permisos de acceso a StorageGRID, iniciará sesión en Grid Manager o en Tenant Manager, según la cuenta que haya seleccionado.



Si la cuenta de servicio no es accesible, aún puede iniciar sesión, siempre que sea un usuario existente que pertenezca a un grupo federado con permisos de acceso a StorageGRID.

5. Opcionalmente, acceda a otros nodos de administración, o acceda al Administrador de red o al Administrador de inquilinos, si tiene los permisos adecuados.

No es necesario volver a ingresar sus credenciales SSO.

Cerrar sesión cuando el SSO esté habilitado

Cuando SSO está habilitado para StorageGRID, lo que sucede cuando cierra sesión depende de dónde haya iniciado sesión y desde dónde cierre sesión.

Pasos

- 1. Localice el enlace **Cerrar sesión** en la esquina superior derecha de la interfaz de usuario.
- 2. Seleccione **Cerrar sesión**.

Aparece la página de Sign in de StorageGRID . El menú desplegable **Cuentas recientes** se actualiza para incluir **Grid Manager** o el nombre del inquilino, para que pueda acceder a estas interfaces de usuario más rápidamente en el futuro.

Si ha iniciado sesión en...	Y cierras sesión en...	Has cerrado sesión en...
Administrador de cuadrícula en uno o más nodos de administración	Administrador de cuadrícula en cualquier nodo de administración	Administrador de cuadrícula en todos los nodos de administración Nota: Si usa Azure para SSO, puede que lleve algunos minutos cerrar sesión en todos los nodos de administración.
Administrador de inquilinos en uno o más nodos de administración	Administrador de inquilinos en cualquier nodo de administración	Administrador de inquilinos en todos los nodos de administración
Tanto Grid Manager como Tenant Manager	Administrador de red	Sólo el administrador de cuadrícula. También debe cerrar sesión en el Administrador de inquilinos para cerrar sesión en SSO.



La tabla resume lo que sucede cuando cierras sesión si estás usando una sola sesión de navegador. Si ha iniciado sesión en StorageGRID en varias sesiones de navegador, deberá cerrar sesión en todas las sesiones de navegador por separado.

Requisitos y consideraciones para el inicio de sesión único

Antes de habilitar el inicio de sesión único (SSO) para un sistema StorageGRID , revise los requisitos y las consideraciones.

Requisitos del proveedor de identidad

StorageGRID admite los siguientes proveedores de identidad SSO (IdP):

- Servicio de federación de Active Directory (AD FS)
- Directorio activo de Azure (Azure AD)
- Federación de ping

Debe configurar la federación de identidad para su sistema StorageGRID antes de poder configurar un proveedor de identidad SSO. El tipo de servicio LDAP que utiliza para la federación de identidad controla qué tipo de SSO puede implementar.

Tipo de servicio LDAP configurado	Opciones para el proveedor de identidad SSO
Directorio activo	• Directorio activo • Azur • Federación de ping
Azur	Azur

Requisitos de AD FS

Puede utilizar cualquiera de las siguientes versiones de AD FS:

- ADFS de Windows Server 2022
- Servidor AD FS de Windows 2019
- Servidor AD FS de Windows 2016



Windows Server 2016 debería utilizar el ["Actualización KB3201845"](#) , o superior.

Requisitos adicionales

- Seguridad de la capa de transporte (TLS) 1.2 o 1.3
- Microsoft .NET Framework, versión 3.5.1 o superior

Consideraciones para Azure

Si usa Azure como tipo de SSO y los usuarios tienen nombres principales de usuario que no usan sAMAccountName como prefijo, pueden surgir problemas de inicio de sesión si StorageGRID pierde su conexión con el servidor LDAP. Para permitir que los usuarios inicien sesión, debe restaurar la conexión al servidor LDAP.

Requisitos del certificado de servidor

De forma predeterminada, StorageGRID utiliza un certificado de interfaz de administración en cada nodo de administración para proteger el acceso al Administrador de Grid, al Administrador de inquilinos, a la API de administración de Grid y a la API de administración de inquilinos. Cuando configura relaciones de confianza de usuario confiable (AD FS), aplicaciones empresariales (Azure) o conexiones de proveedor de servicios (PingFederate) para StorageGRID, utiliza el certificado del servidor como certificado de firma para las solicitudes de StorageGRID .

Si aún no lo has hecho ["Configuró un certificado personalizado para la interfaz de administración"](#) Deberías hacerlo ahora. Cuando instala un certificado de servidor personalizado, este se utiliza para todos los nodos de administración y puede usarlo en todas las relaciones de confianza de usuarios confiables de StorageGRID , aplicaciones empresariales o conexiones de SP .



No se recomienda utilizar el certificado de servidor predeterminado de un nodo de administración en una relación de confianza de usuario confiable, una aplicación empresarial o una conexión de SP. Si el nodo falla y lo recupera, se genera un nuevo certificado de servidor predeterminado. Antes de poder iniciar sesión en el nodo recuperado, debe actualizar la confianza de la parte confiable, la aplicación empresarial o la conexión del SP con el nuevo certificado.

Puede acceder al certificado de servidor de un nodo de administración iniciando sesión en el shell de comandos del nodo y yendo a `/var/local/mgmt-api` directorio. Un certificado de servidor personalizado se denomina `custom-server.crt`. El certificado de servidor predeterminado del nodo se llama `server.crt`.

Requisitos del puerto

El inicio de sesión único (SSO) no está disponible en los puertos restringidos de Grid Manager o Tenant Manager. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autenticuen con inicio de sesión único. Ver "[Controlar el acceso al firewall externo](#)".

Confirmar que los usuarios federados puedan iniciar sesión

Antes de habilitar el inicio de sesión único (SSO), debe confirmar que al menos un usuario federado pueda iniciar sesión en Grid Manager y en Tenant Manager para cualquier cuenta de inquilino existente.

Antes de empezar

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

Pasos

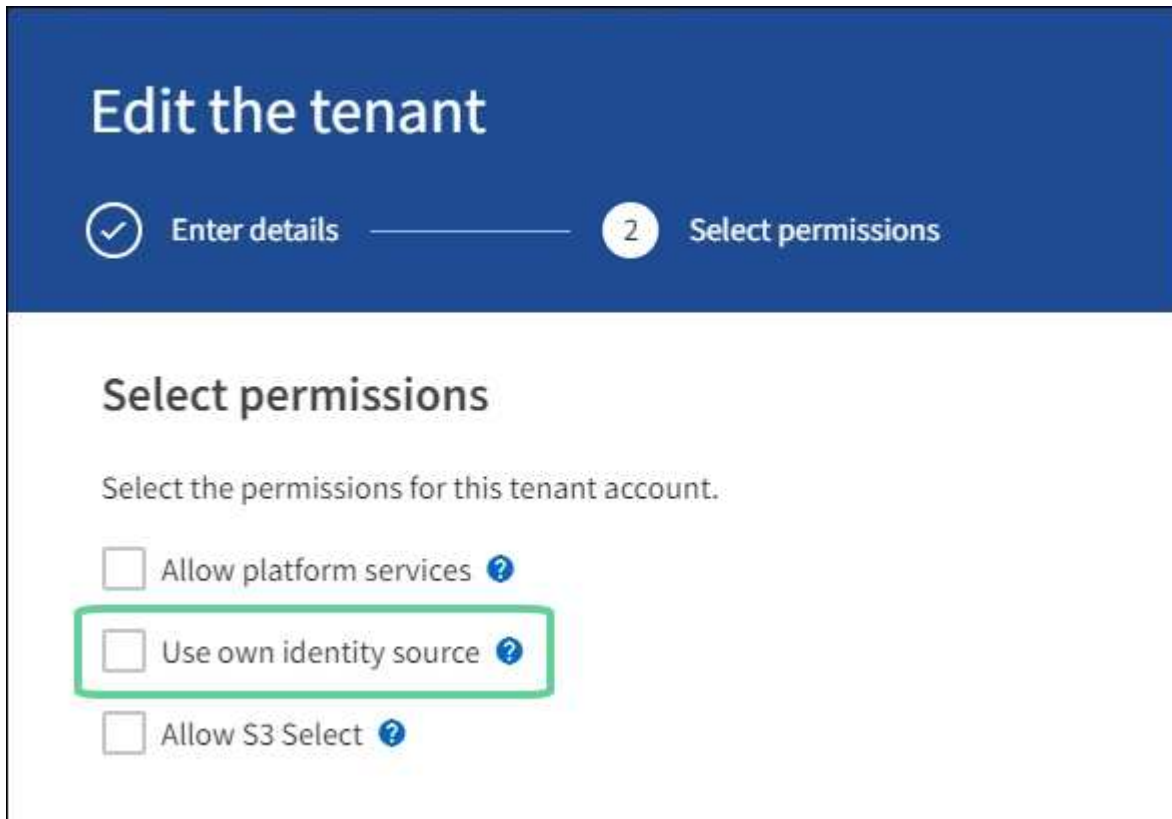
1. Si existen cuentas de inquilinos, confirme que ninguno de ellos esté usando su propia fuente de identidad.



Cuando habilita SSO, una fuente de identidad configurada en Tenant Manager se reemplaza por la fuente de identidad configurada en Grid Manager. Los usuarios que pertenecen a la fuente de identidad del inquilino ya no podrán iniciar sesión a menos que tengan una cuenta con la fuente de identidad de Grid Manager.

- a. Sign in en el Administrador de inquilinos para cada cuenta de inquilino.
 - b. Seleccione **GESTIÓN DE ACCESO > Federación de identidades**.
 - c. Confirme que la casilla de verificación **Habilitar federación de identidad** no esté seleccionada.
 - d. Si es así, confirme que cualquier grupo federado que pueda estar en uso para esta cuenta de inquilino ya no sea necesario, desmarque la casilla de verificación y seleccione **Guardar**.
2. Confirme que un usuario federado puede acceder al Administrador de Grid:
 - a. Desde Grid Manager, seleccione **CONFIGURACIÓN > Control de acceso > Grupos de administración**.
 - b. Asegúrese de que se haya importado al menos un grupo federado desde la fuente de identidad de Active Directory y que se le haya asignado el permiso de acceso raíz.
 - c. Desconectar.

- d. Confirme que puede volver a iniciar sesión en Grid Manager como usuario del grupo federado.
3. Si hay cuentas de inquilino existentes, confirme que un usuario federado que tenga permiso de acceso raíz pueda iniciar sesión:
 - a. Desde el Administrador de red, seleccione **INQUILINOS**.
 - b. Seleccione la cuenta del inquilino y seleccione **Acciones > Editar**.
 - c. En la pestaña Ingresar detalles, seleccione **Continuar**.
 - d. Si la casilla de verificación **Usar fuente de identidad propia** está seleccionada, desmarque la casilla y seleccione **Guardar**.



Aparece la página del inquilino.

- a. Seleccione la cuenta del inquilino, seleccione * Sign in* e inicie sesión en la cuenta del inquilino como usuario raíz local.
- b. Desde el Administrador de inquilinos, seleccione **ADMINISTRACIÓN DE ACCESO > Grupos**.
- c. Asegúrese de que al menos a un grupo federado del Administrador de Grid se le haya asignado el permiso de acceso raíz para este inquilino.
- d. Desconectar.
- e. Confirme que puede volver a iniciar sesión en el inquilino como usuario en el grupo federado.

Información relacionada

- ["Requisitos y consideraciones para el inicio de sesión único"](#)
- ["Administrar grupos de administradores"](#)
- ["Utilice una cuenta de inquilino"](#)

Utilizar el modo sandbox

Puede utilizar el modo sandbox para configurar y probar el inicio de sesión único (SSO) antes de habilitarlo para todos los usuarios de StorageGRID . Una vez habilitado el SSO, puede regresar al modo sandbox siempre que necesite cambiar o volver a probar la configuración.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .
- Ha configurado la federación de identidad para su sistema StorageGRID .
- Para la federación de identidad **tipo de servicio LDAP**, seleccionó Active Directory o Azure, según el proveedor de identidad SSO que planea usar.

Tipo de servicio LDAP configurado	Opciones para el proveedor de identidad SSO
Directorio activo	• Directorio activo • Azur • Federación de ping
Azur	Azur

Acerca de esta tarea

Cuando SSO está habilitado y un usuario intenta iniciar sesión en un nodo de administración, StorageGRID envía una solicitud de autenticación al proveedor de identidad SSO. A su vez, el proveedor de identidad SSO envía una respuesta de autenticación a StorageGRID, indicando si la solicitud de autenticación fue exitosa. Para solicitudes exitosas:

- 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 identidad SSO se comuniquen de forma segura acerca de las solicitudes de autenticación de usuarios, debe configurar ciertas configuraciones en StorageGRID. A continuación, debe utilizar el software del proveedor de identidad SSO para crear una relación de confianza de usuario confiable (AD FS), una aplicación empresarial (Azure) o un proveedor de servicios (PingFederate) para cada nodo de administración. Por último, debes regresar a StorageGRID para habilitar SSO.

El modo Sandbox facilita la realización de esta configuración de ida y vuelta y permite probar todas las configuraciones antes de habilitar SSO. Cuando se utiliza el modo sandbox, los usuarios no pueden iniciar sesión mediante SSO.

Acceder al modo sandbox

Pasos

1. Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.

Aparece la página de inicio de sesión único, con la opción **Deshabilitado** seleccionada.

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO status ⓘ ☒ Disabled ☐ Sandbox Mode ☐ Enabled

Save



Si las opciones de Estado de SSO no aparecen, confirme que haya configurado el proveedor de identidad como fuente de identidad federada. Ver ["Requisitos y consideraciones para el inicio de sesión único"](#).

2. Seleccione **Modo Sandbox**.

Aparece la sección Proveedor de identidad.

Introduzca los datos del proveedor de identidad

Pasos

1. Seleccione el **tipo de SSO** de la lista desplegable.
2. Complete los campos en la sección Proveedor de identidad según el tipo de SSO que haya seleccionado.

Directorio activo

- a. Ingrese el **Nombre del servicio de federación** para el proveedor de identidad, exactamente como aparece en el Servicio de federación de Active Directory (AD FS).



Para localizar el nombre del servicio de federación, vaya al Administrador de servidor de Windows. Seleccione **Herramientas > Administración de AD FS**. En el menú Acción, seleccione **Editar propiedades del servicio de federación**. El nombre del servicio de la federación se muestra en el segundo campo.

- b. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID .

- **Usar certificado CA del sistema operativo:** utilice el certificado CA predeterminado instalado en el sistema operativo para proteger la conexión.
- **Usar certificado CA personalizado:** utilice un certificado 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 utilizar TLS:** No utilice un certificado TLS para proteger la conexión.



Si cambia el certificado de CA, inmediatamente [reiniciar el servicio mgmt-api en los nodos de administración](#) y comprobar que el inicio de sesión único (SSO) en Grid Manager es exitoso.

- c. En la sección Parte confiada, especifique el **Identificador de parte confiada** para StorageGRID. Este valor controla el nombre que utiliza para cada relación de confianza de usuario confiable en AD FS.

- Por ejemplo, si su red tiene solo un nodo de administración y no prevé agregar más nodos de administración en el futuro, ingrese `SG` o `StorageGRID` .
- Si su cuadrícula incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]` . Esto genera una tabla que muestra el identificador de la parte confiable para cada nodo de administración en su sistema, según el nombre de host del nodo.



Debe crear una relación de confianza de usuario autenticado para cada nodo de administración en su sistema StorageGRID . Tener una relación de confianza de parte confiable para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- d. Seleccione **Guardar**.

Aparece una marca de verificación verde en el botón **Guardar** durante unos segundos.



Azur

- a. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID .

- **Usar certificado CA del sistema operativo:** utilice el certificado CA predeterminado instalado en el sistema operativo para proteger la conexión.
- **Usar certificado CA personalizado:** utilice un certificado 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 utilizar TLS:** No utilice un certificado TLS para proteger la conexión.



Si cambia el certificado de CA, inmediatamente ["reiniciar el servicio mgmt-api en los nodos de administración"](#) y comprobar que el inicio de sesión único (SSO) en Grid Manager es exitoso.

- b. En la sección Aplicación empresarial, especifique el **nombre de la aplicación empresarial** para StorageGRID. Este valor controla el nombre que utiliza para cada aplicación empresarial en Azure AD.

- Por ejemplo, si su red tiene solo un nodo de administración y no prevé agregar más nodos de administración en el futuro, ingrese `SG` o `StorageGRID` .
- Si su cuadrícula incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]` . Esto genera una tabla que muestra un nombre de aplicación empresarial para cada nodo de administración en su sistema, según el nombre de host del nodo.



Debe crear una aplicación empresarial para cada nodo de administración en su sistema StorageGRID . Tener una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- c. Siga los pasos en ["Crear aplicaciones empresariales en Azure AD"](#) para crear una aplicación empresarial para cada nodo de administración enumerado en la tabla.
- d. Desde Azure AD, copie la URL de metadatos de federación para cada aplicación empresarial. Luego, pegue esta URL en el campo **URL de metadatos de federación** correspondiente en StorageGRID.
- e. Después de haber copiado y pegado una 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.



Federación de ping

- a. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe información de configuración de SSO en respuesta a las solicitudes de

StorageGRID .

- **Usar certificado CA del sistema operativo:** utilice el certificado CA predeterminado instalado en el sistema operativo para proteger la conexión.
- **Usar certificado CA personalizado:** utilice un certificado 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 utilizar TLS:** No utilice un certificado TLS para proteger la conexión.



Si cambia el certificado de CA, inmediatamente ["reiniciar el servicio mgmt-api en los nodos de administración"](#) y comprobar que el inicio de sesión único (SSO) en Grid Manager es exitoso.

- b. En la sección Proveedor de servicios (SP), especifique el *ID de conexión de SP * para StorageGRID. Este valor controla el nombre que utiliza para cada conexión SP en PingFederate.

- Por ejemplo, si su red tiene solo un nodo de administración y no prevé agregar más nodos de administración en el futuro, ingrese SG o StorageGRID .
- Si su cuadrícula incluye más de un nodo de administración, incluya la cadena [HOSTNAME] en el identificador. Por ejemplo, SG-[HOSTNAME] . Esto genera una tabla que muestra el ID de conexión de SP para cada nodo de administración en su sistema, según el nombre de host del nodo.



Debe crear una conexión SP para cada nodo de administración en su sistema StorageGRID . Tener una conexión SP para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- c. Especifique la URL de metadatos de la federación para cada nodo de administración en el campo **URL de metadatos de la federación**.

Utilice el siguiente formato:

```
https://<Federation Service  
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP  
Connection ID>
```

- d. Seleccione **Guardar**.

Aparece una marca de verificación verde en el botón **Guardar** durante unos segundos.

Save 

Configurar relaciones de confianza entre usuarios, aplicaciones empresariales o conexiones de SP

Cuando se guarda la configuración, aparece el aviso de confirmación del modo Sandbox. Este aviso confirma que el modo sandbox ahora está habilitado y proporciona instrucciones generales.

StorageGRID puede permanecer en modo sandbox tanto tiempo como sea necesario. Sin embargo, cuando se selecciona **Modo Sandbox** en la página de Inicio de sesión único, el SSO se deshabilita para todos los usuarios de StorageGRID . Sólo los usuarios locales pueden iniciar sesión.

Siga estos pasos para configurar relaciones de confianza de usuarios autenticados (Active Directory), completar aplicaciones empresariales (Azure) o configurar conexiones de SP (PingFederate).

Directorio activo

Pasos

1. Vaya a Servicios de federación de Active Directory (AD FS).
2. Cree una o más relaciones de confianza de usuario confiable para StorageGRID, utilizando cada identificador de usuario confiable que se muestra en la tabla de la página de inicio de sesión único de StorageGRID .

Debe crear una confianza para cada nodo de administración que se muestra en la tabla.

Para obtener instrucciones, vaya a ["Crear relaciones de confianza entre usuarios autenticados en AD FS"](#) .

Azur

Pasos

1. Desde la página de inicio de sesión único del nodo de administración en el que está conectado actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. Luego, para cualquier otro nodo de administración en su red, repita estos pasos:
 - a. Sign in en el nodo.
 - b. Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
 - c. Descargue y guarde los metadatos SAML para ese nodo.
3. Vaya al Portal de Azure.
4. Siga los pasos en ["Crear aplicaciones empresariales en Azure AD"](#) para cargar el archivo de metadatos SAML para cada nodo de administración en su aplicación empresarial de Azure correspondiente.

Federación de ping

Pasos

1. Desde la página de inicio de sesión único del nodo de administración en el que está conectado actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. Luego, para cualquier otro nodo de administración en su red, repita estos pasos:
 - a. Sign in en el nodo.
 - b. Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
 - c. Descargue y guarde los metadatos SAML para ese nodo.
3. Vaya a PingFederate.
4. ["Cree una o más conexiones de proveedor de servicios \(SP\) para StorageGRID"](#) . Utilice el ID de conexión de SP para cada nodo de administración (que se muestra en la tabla de la página de inicio de sesión único de StorageGRID) y los metadatos SAML que descargó para ese nodo de administración.

Debe crear una conexión SP para cada nodo de administración que se muestra en la tabla.

Probar conexiones SSO

Antes de implementar 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 estén configurados correctamente para cada nodo de administración.

Directorio activo

Pasos

1. Desde la página de inicio de sesión único de StorageGRID , busque el enlace en el mensaje del modo Sandbox.

La URL se deriva del valor ingresado en el campo **Nombre del servicio de federación**.

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

2. Seleccione el enlace o copie y pegue la URL en un navegador para acceder a la página de inicio de sesión de su proveedor de identidad.
3. Para confirmar que puede usar SSO para iniciar sesión en StorageGRID, seleccione * Sign in en uno de los siguientes sitios , **seleccione el identificador de parte confiable para su nodo de administración principal y seleccione * Sign in**.

You are not signed in.

☐ Sign in to this site.

☒ Sign in to one of the following sites:

SG-DC1-ADM1

Sign in

4. Introduzca su nombre de usuario y contraseña federados.
 - Si las operaciones de inicio y cierre de sesión SSO son exitosas, aparece un mensaje de éxito.

✓ Single sign-on authentication and logout test completed successfully.

- Si la operación SSO no se realiza correctamente, aparece un mensaje de error. Solucione el problema, borre las cookies del navegador y vuelva a intentarlo.
5. Repita estos pasos para verificar la conexión SSO para cada nodo de administración en su red.

Azur

Pasos

1. Vaya a la página de inicio de sesión único en el portal de Azure.
2. Seleccione **Probar esta aplicación**.
3. Introduzca las credenciales de un usuario federado.
 - Si las operaciones de inicio y cierre de sesión SSO son exitosas, aparece un mensaje de éxito.

✓ Single sign-on authentication and logout test completed successfully.

- Si la operación SSO no se realiza correctamente, aparece un mensaje de error. Solucione el problema, borre las cookies del navegador y vuelva a intentarlo.
4. Repita estos pasos para verificar la conexión SSO para cada nodo de administración en su red.

Federación de ping

Pasos

1. Desde la página de inicio de sesión único de StorageGRID , seleccione el primer enlace en el mensaje del modo Sandbox.

Seleccione y pruebe un enlace a la 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://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69)
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73](https://[redacted]/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 y cierre de sesión SSO son exitosas, aparece un mensaje de éxito.

✓ Single sign-on authentication and logout test completed successfully.

- Si la operación SSO no se realiza correctamente, aparece un mensaje de error. Solucione el problema, borre las cookies del navegador y vuelva a intentarlo.
3. Seleccione el siguiente enlace para verificar la conexión SSO para cada nodo de administración en su red.

Si ve un mensaje de Página expirada, seleccione el botón **Atrás** en su navegador y vuelva a enviar sus credenciales.

Habilitar el inicio de sesión único

Cuando haya confirmado que puede usar SSO para iniciar sesión en cada nodo de administración, podrá habilitar SSO para todo su sistema StorageGRID .



Cuando SSO está habilitado, todos los usuarios deben usar SSO para acceder al Administrador de Grid, al Administrador de inquilinos, a la API de administración de Grid y a la API de administración de inquilinos. Los usuarios locales ya no pueden acceder a StorageGRID.

Pasos

1. Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
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 habilitado.



Si usa Azure Portal y accede a StorageGRID desde la misma computadora que usa para acceder a Azure, asegúrese de que el usuario de Azure Portal también sea un usuario autorizado de StorageGRID (un usuario en un grupo federado que se haya importado a StorageGRID) o cierre la sesión en Azure Portal antes de intentar iniciar sesión en StorageGRID.

Crear relaciones de confianza entre usuarios autenticados en AD FS

Debe utilizar los Servicios de federación de Active Directory (AD FS) para crear una relación de confianza de usuario autenticado para cada nodo de administración en su sistema. Puede crear relaciones de confianza de usuario autenticado mediante comandos de PowerShell, importando metadatos SAML desde StorageGRID o ingresando los datos manualmente.

Antes de empezar

- Ha configurado el inicio de sesión único para StorageGRID y seleccionó **AD FS** como tipo de SSO.
- El **modo Sandbox** está seleccionado en la página de inicio de sesión único en Grid Manager. Ver ["Utilizar el modo sandbox"](#) .
- Conoce el nombre de dominio completo (o la dirección IP) y el identificador de la parte confiable para cada nodo de administración en su sistema. Puede encontrar estos valores en la tabla de detalles de Nodos de administración en la página de inicio de sesión único de StorageGRID .



Debe crear una relación de confianza de usuario autenticado para cada nodo de administración en su sistema StorageGRID . Tener una relación de confianza de parte confiable para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- Tiene experiencia en la creación de relaciones de confianza de usuario autenticado 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 está creando la confianza de usuario confiable manualmente, tiene el certificado personalizado que se

cargó para la interfaz de administración de StorageGRID o sabe cómo iniciar sesión en un nodo de administración 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. Si tiene preguntas, consulte la documentación de Microsoft AD FS.

Crear una relación de confianza de usuario autenticado mediante Windows PowerShell

Puede utilizar Windows PowerShell para crear rápidamente una o más relaciones de confianza de usuario autenticado.

Pasos

1. Desde el menú de inicio de Windows, seleccione con el botón derecho el ícono de PowerShell y seleccione **Ejecutar como administrador**.
2. En el símbolo del sistema de PowerShell, ingrese el siguiente comando:

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL  
"https://Admin_Node_FQDN/api/saml-metadata"
```

- Para *Admin_Node_Identifer*, ingrese el Identificador de parte confiable para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único. Por ejemplo, SG-DC1-ADM1 .
- Para *Admin_Node_FQDN*, ingrese el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede utilizar la dirección IP del nodo en su lugar. Sin embargo, si ingresa una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear esta confianza de parte confiable si esa dirección IP alguna vez cambia).

3. Desde el Administrador de servidor de Windows, seleccione **Herramientas > Administración de AD FS**.

Aparece la herramienta de administración de AD FS.

4. Seleccione **AD FS > Confianzas de usuario autenticado**.

Aparece la lista de fideicomisos de partes confiantes.

5. Agregue una Política de control de acceso a la confianza de usuario autenticado recién creada:

- a. Localice el fideicomiso de parte confiante que acaba de crear.
- b. Haga clic derecho en la confianza y seleccione **Editar política de control de acceso**.
- c. Seleccione una política de control de acceso.
- d. Seleccione **Aplicar** y seleccione **Aceptar**

6. Agregue una Política de emisión de reclamaciones al fideicomiso de parte confiada recién creado:

- a. Localice el fideicomiso de parte confiante que acaba de crear.
- b. Haga clic derecho en el fideicomiso 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** de la lista y seleccione **Siguiente**.
- e. En la página Configurar regla, ingrese un nombre para mostrar para esta regla.

Por ejemplo, **ObjectGUID a ID de nombre** o **UPN a ID de nombre**.

- f. Para el almacén de atributos, seleccione **Active Directory**.
 - g. En la columna Atributo LDAP de la tabla Mapeo, escriba **objectGUID** o seleccione **User-Principal-Name**.
 - h. En la columna Tipo de reclamo saliente de la tabla de mapeo, seleccione **ID de nombre** de la lista desplegable.
 - i. Seleccione **Finalizar** y seleccione **Aceptar**.
7. Confirme que los metadatos se importaron correctamente.
- a. Haga clic con el botón derecho en la confianza del usuario confiado para abrir sus propiedades.
 - b. Confirme que los campos en las pestañas **Puntos finales**, **Identificadores** y **Firma** estén completos.
- Si faltan los metadatos, confirme que la dirección de metadatos de la Federación sea correcta o ingrese los valores manualmente.
8. Repita estos pasos para configurar una relación de confianza de usuario confiable para todos los nodos de administración en su sistema StorageGRID .
9. Cuando haya terminado, regrese a StorageGRID y pruebe todas las relaciones de confianza de usuarios autenticados para confirmar que estén configuradas correctamente. Ver "[Utilizar el modo Sandbox](#)" para obtener instrucciones.

Cree una relación de confianza entre usuarios autenticados mediante la importación de metadatos de la federación

Puede importar los valores para cada entidad de confianza accediendo a los metadatos SAML de cada nodo de administración.

Pasos

1. En el Administrador de servidor de Windows, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En Acciones, seleccione **Agregar confianza de usuario autenticado**.
3. En la página de bienvenida, seleccione **Reclamos conscientes** y seleccione **Iniciar**.
4. Seleccione **Importar datos sobre la parte confiante publicados en línea o en una red local**.
5. En **Dirección de metadatos de la 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*, ingrese el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede utilizar la dirección IP del nodo en su lugar. Sin embargo, si ingresa una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear esta confianza de parte confiable si esa dirección IP alguna vez cambia).

6. Complete el asistente de confianza de usuario autenticado, guarde la confianza de usuario autenticado y cierre el asistente.



Al ingresar el nombre para mostrar, utilice el Identificador de usuario confiado para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único en el Administrador de Grid. Por ejemplo, SG-DC1-ADM1 .

7. Agregar una regla de reclamación:

- a. Haga clic derecho en el fideicomiso 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** de la lista y seleccione **Siguiente**.
- d. En la página Configurar regla, ingrese un nombre para mostrar para esta regla.

Por ejemplo, **ObjectGUID a ID de nombre** o **UPN a ID de nombre**.

- e. Para el almacén de atributos, seleccione **Active Directory**.
- f. En la columna Atributo LDAP de la tabla Mapeo, escriba **objectGUID** o seleccione **User-Principal-Name**.
- g. En la columna Tipo de reclamo saliente de la tabla de mapeo, seleccione **ID de nombre** de la lista desplegable.
- h. Seleccione **Finalizar** y seleccione **Aceptar**.

8. Confirme que los metadatos se importaron correctamente.

- a. Haga clic con el botón derecho en la confianza del usuario confiado para abrir sus propiedades.
- b. Confirme que los campos en las pestañas **Puntos finales**, **Identificadores** y **Firma** estén completos.

Si faltan los metadatos, confirme que la dirección de metadatos de la Federación sea correcta o ingrese los valores manualmente.

9. Repita estos pasos para configurar una relación de confianza de usuario confiable para todos los nodos de administración en su sistema StorageGRID .

10. Cuando haya terminado, regrese a StorageGRID y pruebe todas las relaciones de confianza de usuarios autenticados para confirmar que estén configuradas correctamente. Ver "[Utilizar el modo Sandbox](#)" para obtener instrucciones.

Crear una relación de confianza de usuario confiado manualmente

Si decide no importar los datos de las confianzas de las partes confiables, puede ingresar los valores manualmente.

Pasos

1. En el Administrador de servidor de Windows, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En Acciones, seleccione **Agregar confianza de usuario autenticado**.
3. En la página de bienvenida, seleccione **Reclamos conscientes** y seleccione **Iniciar**.
4. Seleccione **Ingresar datos sobre la parte confiada manualmente** y seleccione **Siguiente**.
5. Complete el Asistente de confianza de usuario autenticado:
 - a. Introduzca un nombre para mostrar para este nodo de administración.

Para mantener la coherencia, utilice el Identificador de usuario autenticado para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único en el Administrador de Grid. Por ejemplo, SG-DC1-ADM1 .

- b. Omite el paso para configurar un certificado de cifrado de token opcional.
- c. En la página Configurar URL, seleccione la casilla de verificación **Habilitar soporte para el protocolo SAML 2.0 WebSSO**.
- d. Escriba la URL del punto final del servicio SAML para el nodo de administración:

`https://Admin_Node_FQDN/api/saml-response`

Para *Admin_Node_FQDN*, ingrese el nombre de dominio completo para el nodo de administración. (Si es necesario, puede utilizar la dirección IP del nodo en su lugar. Sin embargo, si ingresa una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear esta confianza de parte confiable si esa dirección IP alguna vez cambia).

- e. En la página Configurar identificadores, especifique el identificador de usuario de confianza para el mismo nodo de administración:

Admin_Node_Identifier

Para *Admin_Node_Identifier*, ingrese el Identificador de parte confiable para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único. Por ejemplo, SG-DC1-ADM1 .

- f. Revise la configuración, guarde la confianza del usuario autenticado y cierre el asistente.

Aparece el cuadro de diálogo Editar política de emisión de reclamaciones.



Si el cuadro de diálogo no aparece, haga clic con el botón derecho en el fideicomiso y seleccione **Editar política de emisión de reclamaciones**.

6. Para iniciar el asistente de reglas de reclamación, seleccione **Agregar regla**:
 - a. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** de la lista y seleccione **Siguiente**.
 - b. En la página Configurar regla, ingrese un nombre para mostrar para esta regla.

Por ejemplo, **ObjectGUID a ID de nombre o UPN a ID de nombre**.
 - c. Para el almacén de atributos, seleccione **Active Directory**.
 - d. En la columna Atributo LDAP de la tabla Mapeo, escriba **objectGUID** o seleccione **User-Principal-Name**.
 - e. En la columna Tipo de reclamo saliente de la tabla de mapeo, seleccione **ID de nombre** de la lista desplegable.
 - f. Seleccione **Finalizar** y seleccione **Aceptar**.
7. Haga clic con el botón derecho en la confianza del usuario confiado para abrir sus propiedades.
8. En la pestaña **Puntos finales**, configure el punto final para el cierre de sesión único (SLO):
 - a. Seleccione **Agregar SAML**.
 - b. Seleccione **Tipo de punto final > Cerrar sesión SAML**.
 - c. Seleccione **Enlace > Redireccionar**.
 - d. En el campo **URL de confianza**, ingrese la URL utilizada para el cierre de sesión único (SLO) desde

este nodo de administración:

`https://Admin_Node_FQDN/api/saml-logout`

Para `Admin_Node_FQDN`, ingrese el nombre de dominio completo del nodo de administración. (Si es necesario, puede utilizar la dirección IP del nodo en su lugar. Sin embargo, si ingresa una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear esta confianza de parte confiable si esa dirección IP alguna vez cambia).

a. Seleccione **Aceptar**.

9. En la pestaña **Firma**, especifique el certificado de firma para esta relación de confianza de usuario autenticado:

a. Agregue el certificado personalizado:

- Si tiene el certificado de administración personalizado que cargó en StorageGRID, seleccione ese certificado.
- Si no tiene el certificado personalizado, inicie sesión en el Nodo de administración, vaya a `/var/local/mgmt-api` directorio del nodo de administración y agregue el `custom-server.crt` archivo de certificado.



Uso del certificado predeterminado del nodo de administración(`server.crt`) no se recomienda. Si el nodo de administración falla, se regenerará el certificado predeterminado cuando recupere el nodo y deberá actualizar la confianza de la parte confiable.

b. Seleccione **Aplicar** y seleccione **Aceptar**.

Las propiedades de la parte confiada se guardan y cierran.

10. Repita estos pasos para configurar una relación de confianza de usuario confiable para todos los nodos de administración en su sistema StorageGRID .
11. Cuando haya terminado, regrese a StorageGRID y pruebe todas las relaciones de confianza de usuarios autenticados para confirmar que estén configuradas correctamente. Ver "[Utilizar el modo sandbox](#)" para obtener instrucciones.

Crear aplicaciones empresariales en Azure AD

Utilice Azure AD para crear una aplicación empresarial para cada nodo de administración en su sistema.

Antes de empezar

- Ha comenzado a configurar el inicio de sesión único para StorageGRID y seleccionó **Azure** como tipo de SSO.
- El **modo Sandbox** está seleccionado en la página de inicio de sesión único en Grid Manager. Ver "[Utilizar el modo sandbox](#)".
- Tiene el **nombre de la aplicación empresarial** para cada nodo de administración en su sistema. Puede copiar estos valores de la tabla de detalles del nodo de administración en la página de inicio de sesión único de StorageGRID .



Debe crear una aplicación empresarial para cada nodo de administración en su sistema StorageGRID . Tener una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar 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 en la nube, Administrador de aplicaciones o propietario de la entidad de servicio.

Acceder a Azure AD

Pasos

1. Iniciar sesión en el "[Portal de Azure](#)" .
2. Navegar a "[Directorio activo de Azure](#)" .
3. Seleccionar "[Aplicaciones empresariales](#)" .

Cree aplicaciones empresariales y guarde la configuración de SSO de StorageGRID

Para guardar la configuración de SSO para Azure en StorageGRID, debe usar Azure para crear una aplicación empresarial para cada nodo de administración. Copiará las URL de metadatos de federación de Azure y las pegará en los campos **URL de metadatos de federación** correspondientes en la página de inicio de sesión único de StorageGRID .

Pasos

1. Repita los siguientes pasos para cada nodo de administración.
 - a. En el panel de aplicaciones empresariales de Azure, seleccione **Nueva aplicación**.
 - b. Seleccione **Crea tu propia aplicación**.
 - c. Para el nombre, ingrese el **nombre de la aplicación empresarial** que copió de la tabla de detalles del nodo de administración en la página de inicio de sesión único de StorageGRID .
 - d. Deje seleccionado el botón de opción **Integrar cualquier otra aplicación que no encuentre en la galería (No galería)**.
 - e. Seleccione **Crear**.
 - f. Seleccione el enlace **Comenzar** en el **2. Configurar el cuadro de inicio de sesión único** o seleccione el enlace **Inicio de sesión único** en el margen izquierdo.
 - g. Seleccione la casilla **SAML**.
 - h. Copie la **URL de metadatos de federación de aplicaciones**, que puede encontrar en el **Paso 3 Certificado de firma SAML**.
 - i. Vaya a la página de inicio de sesión único de StorageGRID y pegue en el campo **URL de metadatos de federación** la URL que corresponde al **nombre de la aplicación empresarial** que utilizó.
2. Después de haber 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 de inicio de sesión único de StorageGRID .

Descargar metadatos SAML para cada nodo de administración

Una vez guardada la configuración de SSO, puede descargar un archivo de metadatos SAML para cada nodo de administración en su sistema StorageGRID .

Pasos

1. Repita estos pasos para cada nodo de administración.
 - a. Sign in en StorageGRID desde el nodo de administración.
 - b. Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
 - c. Seleccione el botón para descargar los metadatos SAML para ese nodo de administración.
 - d. Guarde el archivo que cargará en Azure AD.

Cargar metadatos SAML a cada aplicación empresarial

Después de descargar un archivo de metadatos SAML para cada nodo de administración de StorageGRID , realice los siguientes pasos en Azure AD:

Pasos

1. Regresar al Portal de Azure.
2. Repita estos pasos para cada aplicación empresarial:



Es posible que necesites actualizar la página de aplicaciones empresariales para ver las aplicaciones que agregaste previamente a la lista.

- a. Vaya a la página Propiedades de la aplicación empresarial.
 - b. Establezca **Tarea requerida** en **No** (a menos que desee configurar las asignaciones por separado).
 - c. Vaya a la página de inicio de sesión único.
 - d. Complete la configuración de SAML.
 - e. Seleccione el botón **Cargar archivo de metadatos** y seleccione el archivo de metadatos SAML que descargó para el nodo de administración correspondiente.
 - f. Después de cargar el archivo, seleccione **Guardar** y luego seleccione **X** para cerrar el panel. Regresará a la página Configurar inicio de sesión único con SAML.
3. Siga los pasos en "[Utilizar el modo sandbox](#)" para probar cada aplicación.

Crear conexiones de proveedor de servicios (SP) en PingFederate

Utilice PingFederate para crear una conexión de proveedor de servicios (SP) para cada nodo de administración en su sistema. Para acelerar el proceso, importará los metadatos SAML desde StorageGRID.

Antes de empezar

- Ha configurado el inicio de sesión único para StorageGRID y seleccionó **Ping Federate** como tipo de SSO.
- El **modo Sandbox** está seleccionado en la página de inicio de sesión único en Grid Manager. Ver "[Utilizar el modo sandbox](#)".
- Tienes el *ID de conexión SP * para cada nodo de administración en tu sistema. Puede encontrar estos valores en la tabla de detalles de Nodos de administración en la página de inicio de sesión único de

StorageGRID .

- Ha descargado los **metadatos SAML** para cada nodo de administración en su sistema.
- Tiene experiencia en la creación de conexiones SP en PingFederate Server.
- Tú tienes el https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html ["Guía de referencia del administrador"] para el servidor PingFederate. La documentación de PingFederate proporciona instrucciones y explicaciones detalladas paso a paso.
- Tú tienes el ["Permiso de administrador"](#) para el servidor PingFederate.

Acerca de esta tarea

Estas instrucciones resumen cómo configurar PingFederate Server versión 10.3 como proveedor de SSO para StorageGRID. Si está utilizando otra versión de PingFederate, es posible que deba adaptar estas instrucciones. Consulte la documentación del servidor PingFederate para obtener instrucciones detalladas para su versión.

Requisitos previos completos en PingFederate

Antes de poder crear las conexiones SP que utilizará para StorageGRID, debe completar las tareas previas requeridas en PingFederate. Utilizará la información de estos requisitos previos cuando configure las conexiones del SP .

Crear almacén de datos[[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 ["configuración de la federación de identidades"](#) en StorageGRID.

- **Tipo:** Directorio (LDAP)
- **Tipo LDAP:** Directorio activo
- **Nombre del atributo binario:** Ingrese **objectGUID** en la pestaña Atributos binarios LDAP exactamente como se muestra.

Crear un validador de credenciales de contraseña

Si aún no lo ha hecho, cree un validador de credenciales de contraseña.

- **Tipo:** LDAP Nombre de usuario Contraseña Credencial Validador
- **Almacén de datos:** seleccione el almacén de datos que creó.
- **Base de búsqueda:** Ingrese información de LDAP (por ejemplo, DC=saml,DC=sgws).
- **Filtro de búsqueda:** sAMAccountName=\${username}
- **Alcance:** Subárbol

Crear una instancia de adaptador de IdP

Si aún no lo ha hecho, cree una instancia de adaptador IdP.

Pasos

1. Vaya a **Autenticación > Integración > Adaptadores IdP**.
2. Seleccione **Crear nueva instancia**.

3. En la pestaña Tipo, seleccione **Adaptador IdP de formulario HTML**.
4. En la pestaña Adaptador IdP, seleccione **Agregar una nueva fila a 'Validadores de credenciales'**.
5. Seleccione el [validador de credenciales de contraseña](#) tu creaste
6. En la pestaña Atributos del adaptador, seleccione el atributo **nombre de usuario** para **Seudónimo**.
7. Seleccione **Guardar**.

Crear o importar certificado de firma

Si aún no lo ha hecho, cree o importe el certificado de firma.

Pasos

1. Vaya a **Seguridad > Claves y certificados de firma y descifrado**.
2. Cree o importe el certificado de firma.

Crear una conexión SP en PingFederate

Cuando crea una conexión SP en PingFederate, importa los metadatos SAML que descargó de StorageGRID para el nodo de administración. El archivo de metadatos contiene muchos de los valores específicos que necesita.



Debe crear una conexión SP para cada nodo de administración en su sistema StorageGRID , de modo que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo. Utilice estas instrucciones para crear la primera conexión SP . Luego, ve a [Crear conexiones SP adicionales](#) para crear cualquier conexión adicional que necesites.

Elija el tipo de conexión SP

Pasos

1. Vaya a **Aplicaciones > Integración > *Conexiones SP ***.
2. Seleccione **Crear conexión**.
3. Seleccione **No utilizar una plantilla para esta conexión**.
4. Seleccione **Perfiles SSO del navegador** y **SAML 2.0** como protocolo.

Importar metadatos de SP

Pasos

1. En la pestaña Importar metadatos, seleccione **Archivo**.
2. Elija el archivo de metadatos SAML que descargó de la página de inicio de sesión único de StorageGRID para el nodo de administración.
3. Revise el Resumen de metadatos y la información proporcionada en la pestaña Información general.

El ID de entidad del socio y el nombre de la 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 administración de StorageGRID .

4. Seleccione **Siguiente**.

Configurar el inicio de sesión único (SSO) del navegador IdP

Pasos

1. Desde la pestaña SSO del navegador, seleccione **Configurar SSO del navegador**.
2. En la pestaña Perfiles SAML, seleccione las opciones * SP-initiated SSO*, * SP-initial SLO*, **IdP-initiated SSO** y **IdP-initiated SLO**.
3. Seleccione **Siguiente**.
4. En la pestaña Duración de la afirmación, no realice cambios.
5. En la pestaña Creación de aserciones, seleccione **Configurar creación de aserciones**.
 - a. En la pestaña Asignación de identidad, seleccione **Estándar**.
 - b. En la pestaña Contrato de atributo, utilice **SAML_SUBJECT** como Contrato de atributo y el formato de nombre no especificado que se importó.
6. Para extender el contrato, seleccione **Eliminar** para quitar el `urn:oid`, que no se utiliza.

Instancia del adaptador de mapas

Pasos

1. En la pestaña Mapeo de origen de autenticación, seleccione **Asignar nueva instancia de adaptador**.
2. En la pestaña Instancia del adaptador, seleccione la [instancia de adaptador](#) que creaste.
3. En la pestaña Método de mapeo, seleccione **Recuperar atributos adicionales de un almacén de datos**.
4. En la pestaña Origen de atributos y búsqueda de usuarios, seleccione **Agregar origen de atributos**.
5. En la pestaña Almacén de datos, proporcione una descripción y seleccione el [almacén de datos](#) que usted agregó.
6. En la pestaña Búsqueda de directorio LDAP:
 - Ingrese el **DN base**, que debe coincidir exactamente con el valor ingresado en StorageGRID para el servidor LDAP.
 - Para el ámbito de búsqueda, seleccione **Subárbol**.
 - Para la clase de objeto raíz, busque y agregue cualquiera de estos atributos: **objectGUID** o **userPrincipalName**.
7. En la pestaña Tipos de codificación de atributos binarios LDAP, seleccione **Base64** para el atributo **objectGUID**.
8. En la pestaña Filtro LDAP, ingrese **sAMAccountName=\${username}**.
9. En la pestaña Cumplimiento de contrato de atributo, seleccione **LDAP (atributo)** en el menú desplegable Fuente y seleccione **objectGUID** o **userPrincipalName** en el menú desplegable Valor.
10. Revise y luego guarde la fuente del atributo.
11. En la pestaña Origen del atributo de guardado fallido, seleccione **Anular la transacción SSO**.
12. Revise el resumen y seleccione **Listo**.
13. Seleccione **Listo**.

Configurar los ajustes del protocolo

Pasos

1. En la pestaña **Conexión SP * > *SSO del navegador > Configuración del protocolo**, seleccione

Configurar configuración del protocolo.

2. En la pestaña URL del servicio de consumidor de aserciones, acepte los valores predeterminados, que se importaron de los metadatos SAML de StorageGRID (**POST** para enlace y `/api/saml-response` para la URL del punto final).
3. En la pestaña URL del servicio SLO, acepte los valores predeterminados, que se importaron de los metadatos SAML de StorageGRID (**REDIRECT** para enlace y `/api/saml-logout` para URL de punto final).
4. En la pestaña Enlaces SAML permitidos, desactive **ARTIFACT** y **SOAP**. Sólo se requieren **POST** y **REDIRECT**.
5. En la pestaña Política de firma, deje seleccionadas las casillas de verificación **Requerir que las solicitudes de autenticación estén firmadas** y **Firmar siempre la afirmación**.
6. En la pestaña Política de cifrado, seleccione **Ninguno**.
7. Revise el resumen y seleccione **Listo** para guardar la configuración del protocolo.
8. Revise el resumen y seleccione **Listo** para guardar la configuración de SSO del navegador.

Configurar credenciales

Pasos

1. Desde la pestaña Conexión SP , seleccione **Credenciales**.
2. Desde la pestaña Credenciales, seleccione **Configurar credenciales**.
3. Seleccione el [certificado de firma](#) usted creó o importó.
4. Seleccione **Siguiente** para ir a **Administrar configuración de verificación de firma**.
 - a. En la pestaña Modelo de confianza, seleccione **Sin ancla**.
 - b. En la pestaña Certificado de verificación de firma, revise la información del certificado 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 .

Crear conexiones SP adicionales

Puede copiar la primera conexión SP para crear las conexiones SP que necesita para cada nodo de administración en su red. Carga nuevos metadatos para cada copia.



Las conexiones SP para diferentes nodos de administración utilizan configuraciones idénticas, con la excepción del ID de entidad del socio, la URL base, el ID de conexión, el nombre de la conexión, la verificación de firma y la URL de respuesta de SLO.

Pasos

1. Seleccione **Acción** > **Copiar** para crear una copia de la conexión SP inicial para cada nodo de administración adicional.
2. Ingrese el ID de conexión y el nombre de conexión para la copia y seleccione **Guardar**.
3. Seleccione el archivo de metadatos correspondiente 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 navegador > Configurar creación de afirmaciones > Contrato de atributos**.
 - c. Eliminar la entrada para **urn:oid**.
 - d. Seleccione **Guardar**.

Deshabilitar el inicio de sesión único

Puede desactivar el inicio de sesión único (SSO) si ya no desea utilizar esta funcionalidad. Debe deshabilitar el inicio de sesión único antes de poder deshabilitar la federación de identidad.

Antes de empezar

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

Pasos

1. Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.

Aparece la página de inicio de sesión único.

2. Seleccione la opción **Deshabilitado**.
3. Seleccione **Guardar**.

Aparece un mensaje de advertencia que indica que los usuarios locales ahora podrán iniciar sesión.

4. Seleccione **Aceptar**.

La próxima vez que inicie sesión en StorageGRID, aparecerá la página de Sign in de StorageGRID y deberá ingresar el nombre de usuario y la contraseña de un usuario de StorageGRID local o federado.

Deshabilitar temporalmente y volver a habilitar el inicio de sesión único para un nodo de administración

Es posible que no pueda iniciar sesión en Grid Manager si el sistema de inicio de sesión único (SSO) deja de funcionar. En este caso, puede deshabilitar y volver a habilitar temporalmente el SSO para un nodo de administración. Para deshabilitar y luego volver a habilitar SSO, debe acceder al shell de comandos del nodo.

Antes de empezar

- Tienes ["permisos de acceso específicos"](#).
- Tú tienes el `Passwords.txt` archivo.
- Conoces la contraseña del usuario root 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 su sistema StorageGRID, debe usar el shell de comandos del nodo para

volver a habilitar SSO en el nodo de administración tan pronto como cierre la sesión.



Deshabilitar SSO para un nodo de administración no afecta la configuración de SSO de ningún otro nodo de administración en la red. La casilla de verificación **Habilitar SSO** en la página de Inicio de sesión único en el Administrador de Grid permanece seleccionada y todas las configuraciones de SSO existentes se mantienen a menos que las actualice.

Pasos

1. Inicie sesión en un nodo de administración:

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

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

2. Ejecute el siguiente comando: `disable-saml`

Un mensaje indica que el comando se aplica únicamente a este nodo de administración.

3. Confirme que desea deshabilitar SSO.

Un mensaje indica que el inicio de sesión único está deshabilitado en el nodo.

4. Desde un navegador web, acceda al Administrador de cuadrícula en el mismo nodo de administración.

Ahora se muestra la página de inicio de sesión de Grid Manager porque se ha deshabilitado el SSO.

5. Sign in con el nombre de usuario root y la contraseña del usuario root local.

6. Si deshabilitó SSO temporalmente porque necesitaba corregir la configuración de SSO:

- Seleccione **CONFIGURACIÓN > Control de acceso > Inicio de sesión único**.
- Cambie la configuración de SSO incorrecta o desactualizada.
- Seleccione **Guardar**.

Al seleccionar **Guardar** en la página de inicio de sesión único, se vuelve a habilitar automáticamente el SSO para toda la red.

7. Si deshabilitó el SSO temporalmente porque necesitaba acceder al Administrador de Grid por algún otro motivo:

- Realice cualquier tarea o tareas que necesite realizar.
- Seleccione **Cerrar sesión** y cierre el Administrador de cuadrícula.
- Vuelva a habilitar SSO en el nodo de administración. 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 administración.

Confirme que desea habilitar SSO.

Un mensaje indica que el inicio de sesión único está habilitado en el nodo.

- Reiniciar el nodo de la red: `reboot`

8. Desde un navegador web, acceda al Administrador de cuadrícula desde el mismo nodo de administración.
9. Confirme que aparezca la página de Sign in de StorageGRID y que debe ingresar sus credenciales de SSO para acceder al Administrador de Grid.

Utilizar la federación de red

¿Qué es la federación de red?

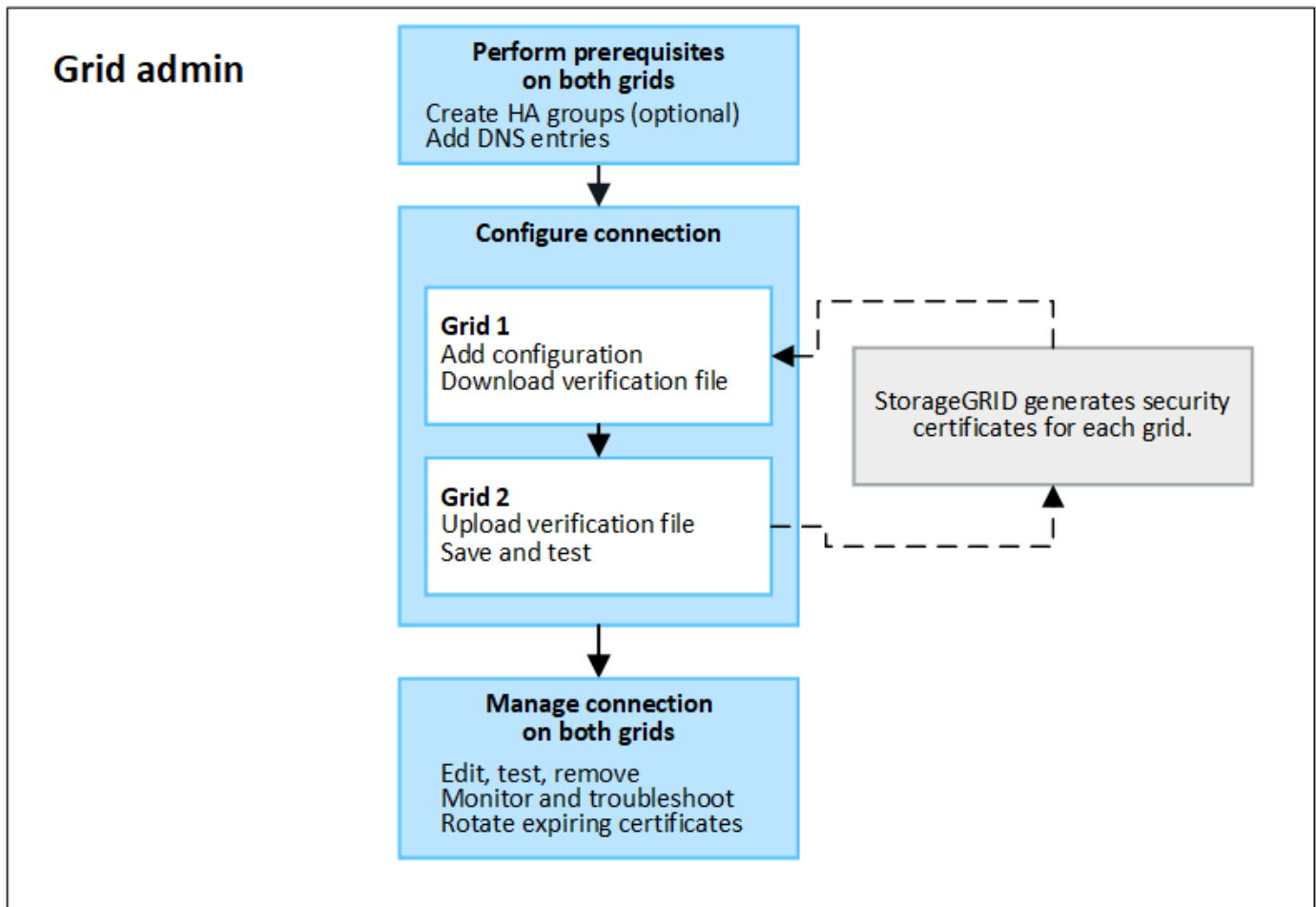
Puede utilizar la federación de red para clonar inquilinos y replicar sus objetos entre dos sistemas StorageGRID para la recuperación ante desastres.

¿Qué es una conexión de federación de red?

Una conexión de federación de red es una conexión bidireccional, confiable y segura entre los nodos de administración y de puerta de enlace en dos sistemas StorageGRID .

Flujo de trabajo para la federación de redes

El diagrama de flujo de trabajo resume los pasos para configurar una conexión de federación de red entre dos redes.



Consideraciones y requisitos para las conexiones de federación de red

- Las cuadrículas utilizadas para la federación de cuadrículas deben ejecutar versiones de StorageGRID que sean idénticas o que no tengan más de una diferencia de versión importante entre ellas.

Para obtener detalles sobre los requisitos de la versión, consulte la ["Notas de la versión"](#).

- Una red puede tener una o más conexiones de federación de redes a otras redes. Cada conexión de federación de red es independiente de cualquier otra conexión. Por ejemplo, si la Red 1 tiene una conexión con la Red 2 y una segunda conexión con la Red 3, no hay ninguna conexión implícita entre la Red 2 y la Red 3.
- Las conexiones de la federación de red son bidireccionales. Una vez establecida la conexión, puedes supervisarla y administrarla desde cualquiera de las redes.
- Debe existir al menos una conexión de federación de red antes de poder usar ["clon de cuenta"](#) o ["replicación entre redes"](#).

Requisitos de red y dirección IP

- Las conexiones de federación de red pueden ocurrir en la red de red, la red de administración o la red de cliente.
- Una conexión de federación de red conecta una red con otra red. La configuración de cada red especifica un punto final de federación de red en la otra red que consta de nodos de administración, nodos de puerta de enlace o ambos.
- La mejor práctica es conectar ["grupos de alta disponibilidad \(HA\)"](#) de nodos de puerta de enlace y de

administración en cada red. El uso de grupos de alta disponibilidad ayuda a garantizar que las conexiones de la federación de red permanecerán en línea si los nodos no están disponibles. Si falla la interfaz activa en cualquiera de los grupos HA, la conexión puede usar una interfaz de respaldo.

- No se recomienda crear una conexión de federación de red que utilice la dirección IP de un solo nodo de administración o nodo de puerta de enlace. Si el nodo deja de estar disponible, la conexión de la federación de red también dejará de estar disponible.
- ["Replicación entre redes"](#) La creación de objetos requiere que los nodos de almacenamiento en cada red puedan acceder a los nodos de administración y de puerta de enlace configurados en la otra red. Para cada cuadrícula, confirme que todos los nodos de almacenamiento tengan una ruta de alto ancho de banda como los nodos de administración o los nodos de puerta de enlace utilizados para la conexión.

Utilice FQDN para equilibrar la carga de la conexión

Para un entorno de producción, utilice nombres de dominio completos (FQDN) para identificar cada cuadrícula en la conexión. Luego, crea las entradas DNS apropiadas, de la siguiente manera:

- El FQDN para Grid 1 asignado a una o más direcciones IP virtuales (VIP) para grupos de HA en Grid 1 o a la dirección IP de uno o más nodos de administración o de puerta de enlace en Grid 1.
- El FQDN para Grid 2 asignado a una o más direcciones VIP para Grid 2 o a la dirección IP de uno o más nodos de administración o de puerta de enlace en Grid 2.

Cuando se utilizan varias entradas DNS, las solicitudes para utilizar la conexión se equilibran de la siguiente manera:

- Las entradas DNS que se asignan a las direcciones VIP de varios grupos de HA se equilibran entre los nodos activos en los grupos de HA.
- Las entradas DNS que se asignan a las direcciones IP de varios nodos de administración o nodos de puerta de enlace se equilibran entre los nodos asignados.

Requisitos del puerto

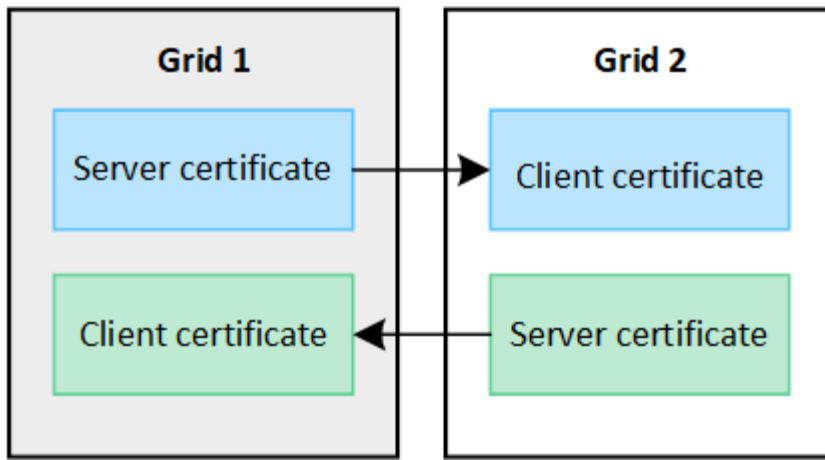
Al crear una conexión de federación de red, puede especificar cualquier número de puerto no utilizado del 23000 al 23999. Ambas redes en esta conexión utilizarán el mismo puerto.

Debe asegurarse de que ningún nodo de ninguna de las redes utilice este puerto para otras conexiones.

Requisitos del certificado

Cuando configura una conexión de federación de red, StorageGRID genera automáticamente cuatro certificados SSL:

- Certificados de servidor y cliente para autenticar y cifrar la información enviada desde la red 1 a la red 2
- Certificados de servidor y cliente para autenticar y cifrar la información enviada desde la red 2 a la red 1



De forma predeterminada, los certificados son válidos durante 730 días (2 años). Cuando estos certificados se acercan a su fecha de vencimiento, la alerta **Vencimiento del certificado de federación de red** le recuerda que debe rotar los certificados, lo que puede hacer utilizando el Administrador de red.



Si los certificados en cualquiera de los extremos de la conexión expiran, la conexión dejará de funcionar. La replicación de datos quedará pendiente hasta que se actualicen los certificados.

Más información

- ["Crear conexiones de federación de red"](#)
- ["Administrar conexiones de federación de red"](#)
- ["Solucionar errores de federación de red"](#)

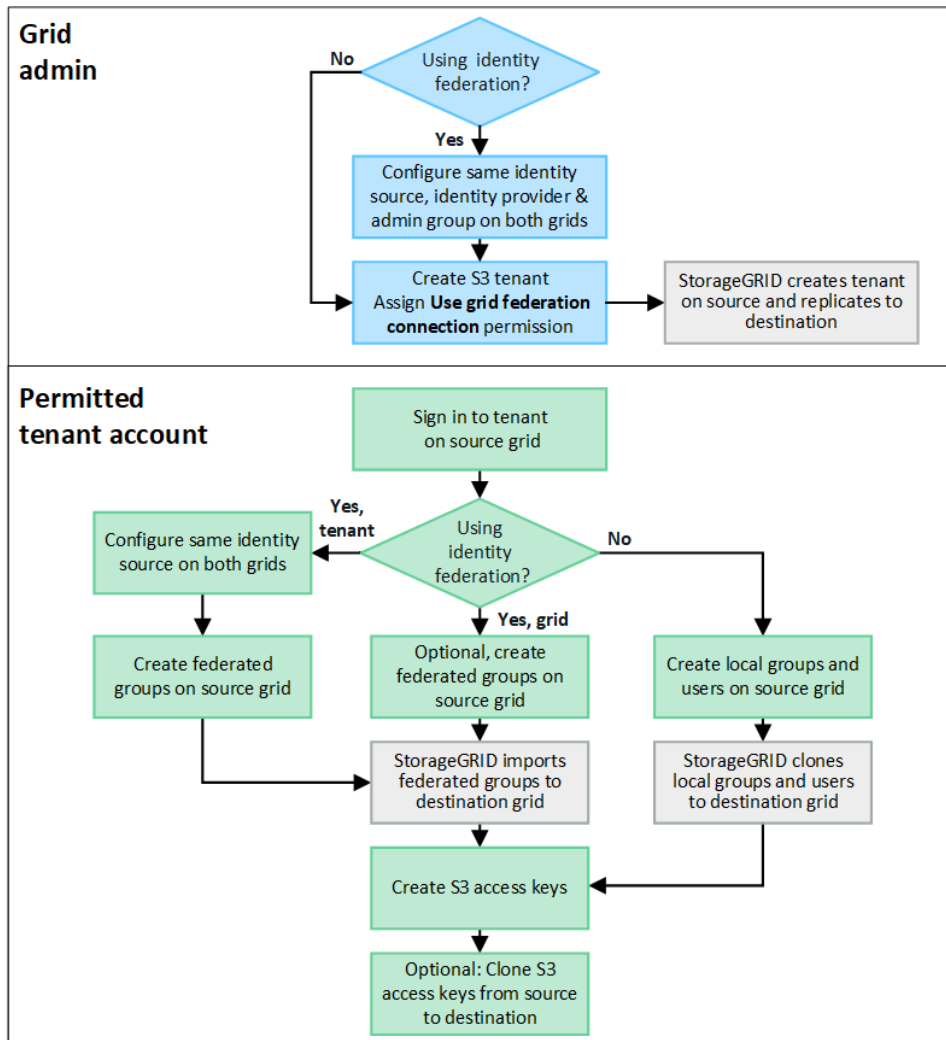
¿Qué es la clonación de cuenta?

La clonación de cuenta es la replicación automática de una cuenta de inquilino, grupos de inquilinos, usuarios de inquilinos y, opcionalmente, claves de acceso S3 entre los sistemas StorageGRID en un ["conexión de federación de red"](#).

Se requiere clonar la cuenta para ["replicación entre redes"](#). La clonación de información de cuentas desde un sistema StorageGRID de origen a un sistema StorageGRID de destino garantiza que los usuarios y grupos de inquilinos puedan acceder a los depósitos y objetos correspondientes en cualquiera de las redes.

Flujo de trabajo para clonar cuentas

El diagrama de flujo de trabajo muestra los pasos que los administradores de la red y los inquilinos permitidos realizarán para configurar la clonación de cuenta. Estos pasos se realizan después de la ["La conexión de la federación de red está configurada"](#).



Flujo de trabajo de administración de la red

Los pasos que realizan los administradores de red dependen de si los sistemas StorageGRID en la "conexión de federación de red" Utilice el inicio de sesión único (SSO) o la federación de identidades.

Configurar SSO para clonar cuenta (opcional)

Si alguno de los sistemas StorageGRID en la conexión de federación de red usa SSO, ambas redes deben usar SSO. Antes de crear las cuentas de inquilino para la federación de red, los administradores de red para las redes de origen y destino del inquilino deben realizar estos pasos.

Pasos

1. Configure la misma fuente de identidad para ambas cuadrículas. Ver "[Utilizar la federación de identidades](#)".
2. Configure el mismo proveedor de identidad SSO (IdP) para ambas redes. Ver "[Configurar el inicio de sesión único](#)".
3. "[Crea el mismo grupo de administradores](#)" en ambas cuadrículas importando el mismo grupo federado.

Cuando cree el inquilino, seleccionará este grupo para que tenga el permiso de acceso raíz inicial para las cuentas de inquilino de origen y de destino.



Si este grupo de administración no existe en ambas cuadrículas antes de crear el inquilino, este no se replicará en el destino.

Configurar la federación de identidad a nivel de cuadrícula para la clonación de cuentas (opcional)

Si alguno de los sistemas StorageGRID utiliza la federación de identidad sin SSO, ambas redes deben utilizar la federación de identidad. Antes de crear las cuentas de inquilino para la federación de red, los administradores de red para las redes de origen y destino del inquilino deben realizar estos pasos.

Pasos

1. Configure la misma fuente de identidad para ambas cuadrículas. Ver "[Utilizar la federación de identidades](#)".
2. Opcionalmente, si un grupo federado tendrá permiso de acceso raíz inicial tanto para las cuentas de inquilino de origen como de destino, "[crear el mismo grupo de administradores](#)" en ambas cuadrículas importando el mismo grupo federado.



Si asigna permiso de acceso raíz a un grupo federado que no existe en ambas redes, el inquilino no se replica en la red de destino.

3. Si no desea que un grupo federado tenga permiso de acceso raíz inicial para ambas cuentas, especifique una contraseña para el usuario raíz local.

Crear una cuenta de inquilino S3 permitida

Después de configurar opcionalmente SSO o la federación de identidad, un administrador de red realiza estos pasos para determinar qué inquilinos pueden replicar objetos de depósito en otros sistemas StorageGRID.

Pasos

1. Determine qué cuadrícula desea que sea la cuadrícula de origen del inquilino para las operaciones de clonación de cuentas.

La cuadrícula donde se crea originalmente el inquilino se conoce como la *cuadrícula de origen* del inquilino. La cuadrícula donde se replica el inquilino se conoce como la *cuadrícula de destino* del inquilino.

2. En esa cuadrícula, cree una nueva cuenta de inquilino S3 o edite una cuenta existente.
3. Asignar el permiso **Usar conexión de federación de red**.
4. Si la cuenta del inquilino administrará sus propios usuarios federados, asigne el permiso **Usar fuente de identidad propia**.

Si se asigna este permiso, las cuentas de inquilino de origen y de destino deben configurar la misma fuente de identidad antes de crear grupos federados. Los grupos federados agregados al inquilino de origen no se pueden clonar en el inquilino de destino a menos que ambas cuadrículas utilicen la misma fuente de identidad.

5. Seleccione una conexión de federación de red específica.
6. Guardar el inquilino nuevo o modificado.

Cuando se guarda un nuevo inquilino con el permiso **Usar conexión de federación de red**, StorageGRID crea automáticamente una réplica de ese inquilino en la otra red, de la siguiente manera:

- Ambas cuentas de inquilino tienen el mismo ID de cuenta, nombre, cuota de almacenamiento y

permisos asignados.

- Si seleccionó un grupo federado para tener permiso de acceso raíz para el inquilino, ese grupo se clona en el inquilino de destino.
- Si seleccionó un usuario local para que tenga permiso de acceso raíz para el inquilino, ese usuario se clonará en el inquilino de destino. Sin embargo, la contraseña de ese usuario no se clona.

Para obtener más información, consulte ["Administrar inquilinos permitidos para la federación de red"](#) .

Flujo de trabajo de cuentas de inquilinos permitidos

Después de que un inquilino con el permiso **Usar conexión de federación de red** se replica en la red de destino, las cuentas de inquilino permitidas pueden realizar estos pasos para clonar grupos de inquilinos, usuarios y claves de acceso S3.

Pasos

1. Sign in en la cuenta del inquilino en la cuadrícula de origen del inquilino.
2. Si está permitido, configure la federación de identidad en las cuentas de inquilino de origen y de destino.
3. Cree grupos y usuarios en el inquilino de origen.

Cuando se crean nuevos grupos o usuarios en el inquilino de origen, StorageGRID los clona automáticamente en el inquilino de destino, pero no se produce ninguna clonación desde el destino hasta el origen.

4. Crear claves de acceso S3.
5. Opcionalmente, clone las claves de acceso S3 del inquilino de origen al inquilino de destino.

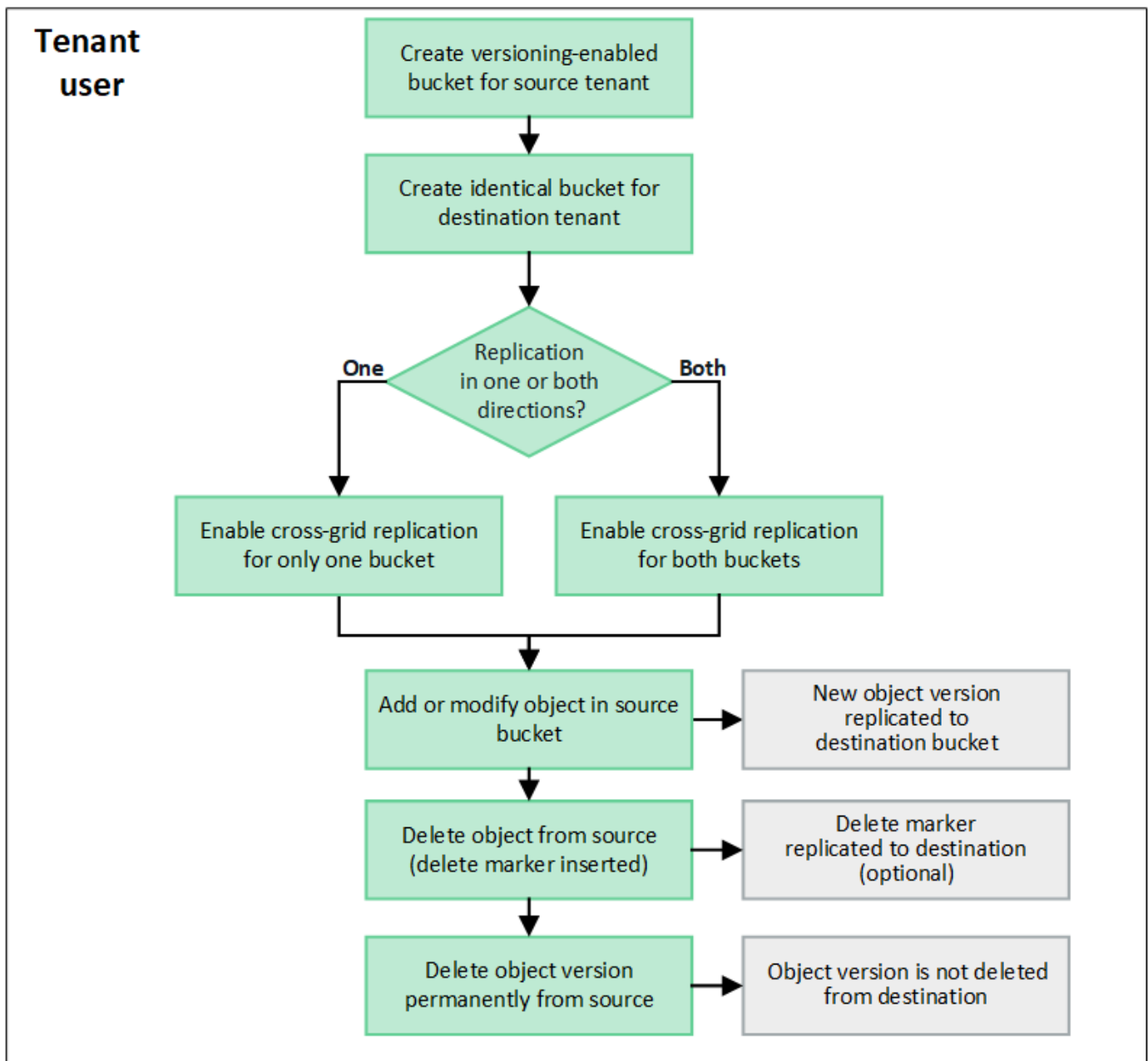
Para obtener detalles sobre el flujo de trabajo de la cuenta de inquilino permitida y para aprender cómo se clonan los grupos, los usuarios y las claves de acceso de S3, consulte ["Clonar grupos de inquilinos y usuarios"](#) y ["Clonar claves de acceso S3 usando la API"](#) .

¿Qué es la replicación entre redes?

La replicación entre redes es la replicación automática de objetos entre depósitos S3 seleccionados en dos sistemas StorageGRID que están conectados en una ["conexión de federación de red"](#) . ["Clon de cuenta"](#) es necesario para la replicación entre redes.

Flujo de trabajo para la replicación entre redes

El diagrama de flujo de trabajo resume los pasos para configurar la replicación entre cuadrículas entre depósitos en dos cuadrículas.



Requisitos para la replicación entre redes

Si una cuenta de inquilino tiene el permiso **Usar conexión de federación de red** para usar una o más ["conexiones de federación de red"](#) Un usuario inquilino con permiso de acceso raíz puede crear depósitos idénticos en las cuentas de inquilino correspondientes en cada red. Estos cubos:

- Debe tener el mismo nombre pero puede tener diferentes regiones
- Debe tener habilitada la versión
- Debe tener el bloqueo de objetos S3 deshabilitado
- Debe estar vacío

Una vez creados ambos buckets, se puede configurar la replicación entre redes para uno o ambos buckets.

Más información

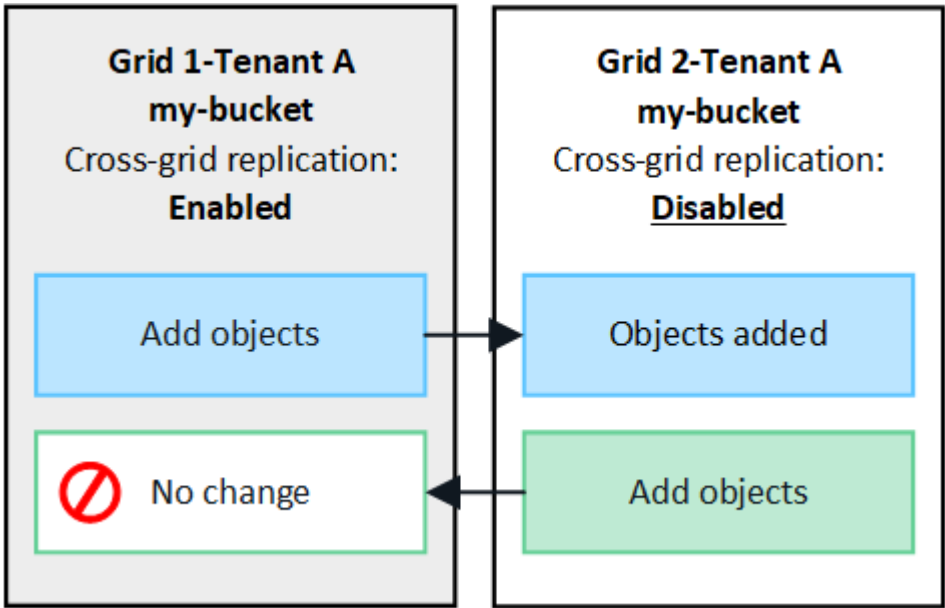
["Administrar la replicación entre redes"](#)

Cómo funciona la replicación entre redes

La replicación entre redes se puede configurar para que ocurra en una dirección o en ambas direcciones.

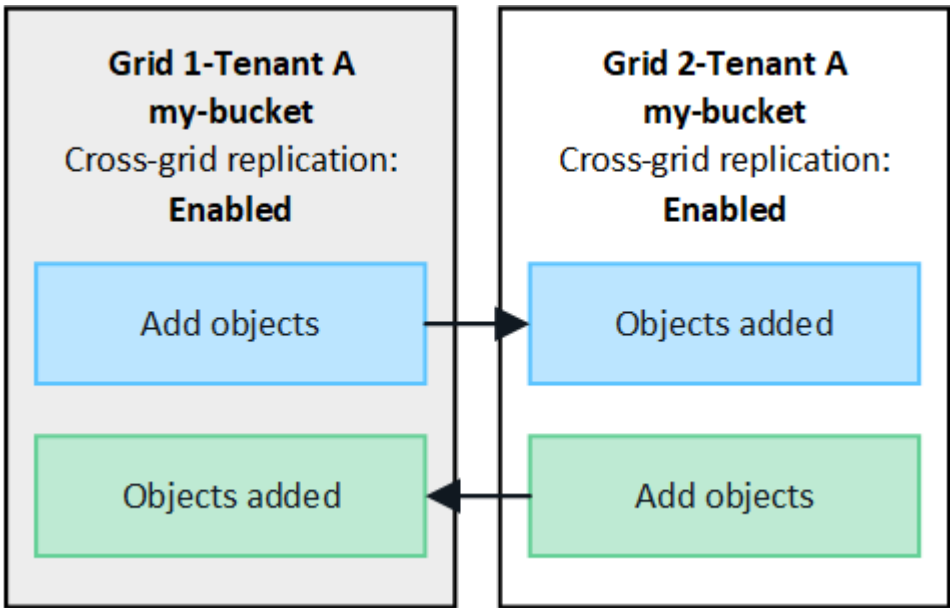
Replicación en una dirección

Si habilita la replicación entre cuadrículas para un depósito en una sola cuadrícula, los objetos agregados a ese depósito (el depósito de origen) se replican en el depósito correspondiente en la otra cuadrícula (el depósito de destino). Sin embargo, los objetos agregados al depósito de destino no se replican en el origen. En la figura, la replicación entre redes está habilitada para my-bucket de la cuadrícula 1 a la cuadrícula 2, pero no está habilitado en la otra dirección.



Replicación en ambas direcciones

Si habilita la replicación entre cuadrículas para el mismo depósito en ambas cuadrículas, los objetos agregados a cualquiera de los depósitos se replicarán en la otra cuadrícula. En la figura, la replicación entre redes está habilitada para my-bucket en ambas direcciones.



¿Qué sucede cuando se ingieren objetos?

Cuando un cliente S3 agrega un objeto a un bucket que tiene habilitada la replicación entre redes, sucede lo siguiente:

1. StorageGRID replica automáticamente el objeto desde el depósito de origen al depósito de destino. El tiempo necesario para realizar esta operación de replicación en segundo plano depende de varios factores, incluida la cantidad de otras operaciones de replicación que estén pendientes.

El cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud `GetObject` o `HeadObject`. La respuesta incluye un StorageGRID específico `x-ntap-sg-cgr-replication-status` encabezado de respuesta, que tendrá uno de los siguientes valores: El cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud `GetObject` o `HeadObject`. La respuesta incluye un StorageGRID específico `x-ntap-sg-cgr-replication-status` encabezado de respuesta, que tendrá uno de los siguientes valores:

Red	Estado de replicación
Fuente	• COMPLETADO: La replicación fue exitosa para todas las conexiones de red. • PENDIENTE: El objeto no se ha replicado a al menos una conexión de red. • FALLA: La replicación no está pendiente para ninguna conexión a la red y al menos una falló con una falla permanente. Un usuario debe resolver el error.
Destino	RÉPLICA: El objeto fue replicado desde la cuadrícula de origen.



StorageGRID no es compatible con `x-amz-replication-status` encabezamiento.

2. StorageGRID utiliza las políticas ILM activas de cada red para administrar los objetos, tal como lo haría con cualquier otro objeto. Por ejemplo, el Objeto A en la Cuadrícula 1 podría almacenarse como dos copias replicadas y conservarse para siempre, mientras que la copia del Objeto A que se replicó en la Cuadrícula 2 podría almacenarse utilizando una codificación de borrado 2+1 y eliminarse después de tres años.

¿Qué sucede cuando se eliminan objetos?

Como se describe en "[Eliminar flujo de datos](#)" StorageGRID puede eliminar un objeto por cualquiera de estos motivos:

- El cliente S3 emite una solicitud de eliminación.
- Un usuario de administrador de inquilinos selecciona el "[Eliminar objetos en el depósito](#)" Opción para eliminar todos los objetos de un depósito.
- El bucket tiene una configuración de ciclo de vida que expira.
- Finaliza el último período de tiempo de la regla ILM para el objeto y no se especifican más ubicaciones.

Cuando StorageGRID elimina un objeto debido a una operación Eliminar objetos en el depósito, vencimiento del ciclo de vida del depósito o vencimiento de la ubicación de ILM, el objeto replicado nunca se elimina de la otra red en una conexión de federación de redes. Sin embargo, los marcadores de eliminación agregados al depósito de origen mediante eliminaciones del cliente S3 se pueden replicar opcionalmente en el depósito de

destino.

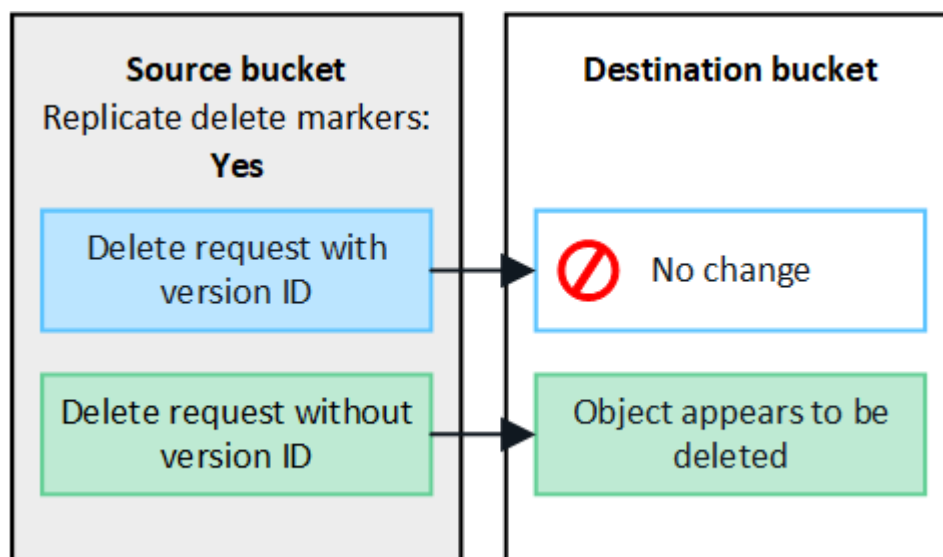
Para comprender qué sucede cuando un cliente S3 elimina objetos de un depósito que tiene habilitada la replicación entre cuadrículas, revise cómo los clientes S3 eliminan objetos de depósitos que tienen habilitada la gestión de versiones, de la siguiente manera:

- Si un cliente S3 emite una solicitud de eliminación que incluye un ID de versión, esa versión del objeto se elimina de forma permanente. No se agrega ningún marcador de eliminación al depósito.
- Si un cliente S3 emite una solicitud de eliminación que no incluye un ID de versión, StorageGRID no elimina ninguna versión de objeto. En lugar de ello, agrega un marcador de eliminación al depósito. El marcador de eliminación hace que StorageGRID actúe como si el objeto hubiera sido eliminado:
 - Una solicitud `GetObject` sin un ID de versión fallará con `404 No Object Found`
 - Una solicitud `GetObject` con un ID de versión válido tendrá éxito y devolverá la versión del objeto solicitada.

Cuando un cliente S3 elimina un objeto de un bucket que tiene habilitada la replicación entre redes, StorageGRID determina si debe replicar la solicitud de eliminación al destino, de la siguiente manera:

- Si la solicitud de eliminación incluye un ID de versión, esa versión del objeto se elimina de forma permanente de la cuadrícula de origen. Sin embargo, StorageGRID no replica las solicitudes de eliminación que incluyen un ID de versión, por lo que la misma versión del objeto no se elimina del destino.
- Si la solicitud de eliminación no incluye un ID de versión, StorageGRID puede replicar opcionalmente el marcador de eliminación, según cómo esté configurada la replicación entre redes para el depósito:
 - Si elige replicar marcadores de eliminación (predeterminado), se agrega un marcador de eliminación al depósito de origen y se replica en el depósito de destino. En efecto, el objeto parece estar eliminado en ambas cuadrículas.
 - Si elige no replicar los marcadores de eliminación, se agrega un marcador de eliminación al depósito de origen, pero no se replica en el depósito de destino. En efecto, los objetos que se eliminan en la cuadrícula de origen no se eliminan en la cuadrícula de destino.

En la figura, **Replicar marcadores de eliminación** se configuró en **Sí** cuando "[Se habilitó la replicación entre redes](#)". Las solicitudes de eliminación del depósito de origen que incluyen un ID de versión no eliminarán objetos del depósito de destino. Las solicitudes de eliminación del depósito de origen que no incluyen un ID de versión parecerán eliminar objetos en el depósito de destino.





Si desea mantener las eliminaciones de objetos sincronizadas entre cuadrículas, cree las correspondientes ["Configuraciones del ciclo de vida de S3"](#) para los cubos en ambas cuadrículas.

Cómo se replican los objetos cifrados

Cuando utiliza la replicación entre cuadrículas para replicar objetos entre cuadrículas, puede cifrar objetos individuales, usar el cifrado de depósito predeterminado o configurar el cifrado de toda la cuadrícula. Puede agregar, modificar o eliminar configuraciones de cifrado predeterminadas de toda la red o del bucket antes o después de habilitar la replicación entre redes para un bucket.

Para cifrar objetos individuales, puede utilizar SSE (cifrado del lado del servidor con claves administradas StorageGRID) al agregar los objetos al depósito de origen. Utilice el `x-amz-server-side-encryption` encabezado de solicitud y especifique AES256. Ver ["Utilice cifrado del lado del servidor"](#).



No se admite el uso de SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente) para la replicación entre redes. La operación de ingesta fallará.

Para utilizar el cifrado predeterminado para un depósito, utilice una solicitud `PutBucketEncryption` y configure el `SSEAlgorithm` parámetro a AES256. El cifrado a nivel de depósito se aplica a cualquier objeto ingerido sin la `x-amz-server-side-encryption` encabezado de solicitud. Ver ["Operaciones en buckets"](#).

Para utilizar el cifrado a nivel de cuadrícula, configure la opción **Cifrado de objetos almacenados en AES-256**. El cifrado a nivel de red se aplica a cualquier objeto que no esté cifrado a nivel de depósito o que se ingiera sin el `x-amz-server-side-encryption` encabezado de solicitud. Ver ["Configurar opciones de red y objetos"](#).



SSE no admite AES-128. Si la opción **Cifrado de objetos almacenados** está habilitada para la cuadrícula de origen que utiliza la opción **AES-128**, el uso del algoritmo AES-128 no se propagará al objeto replicado. En su lugar, el objeto replicado utilizará el depósito predeterminado del destino o la configuración de cifrado a nivel de cuadrícula, si está disponible.

Al determinar cómo cifrar los objetos de origen, StorageGRID aplica estas reglas:

1. Utilice el `x-amz-server-side-encryption` encabezado de ingesta, si está presente.
2. Si no hay un encabezado de ingesta presente, utilice la configuración de cifrado predeterminada del depósito, si está configurada.
3. Si no se configura una configuración de depósito, utilice la configuración de cifrado de toda la red, si está configurada.
4. Si no hay una configuración para toda la cuadrícula, no cifre el objeto de origen.

Al determinar cómo cifrar objetos replicados, StorageGRID aplica estas reglas en este orden:

1. Utilice el mismo cifrado que el objeto de origen, a menos que ese objeto utilice cifrado AES-128.
2. Si el objeto de origen no está cifrado o utiliza AES-128, utilice la configuración de cifrado predeterminada del depósito de destino, si está configurada.
3. Si el depósito de destino no tiene una configuración de cifrado, utilice la configuración de cifrado de toda la red del destino, si está configurada.
4. Si no hay una configuración para toda la cuadrícula, no cifre el objeto de destino.

PutObjectTagging y DeleteObjectTagging no son compatibles

Las solicitudes PutObjectTagging y DeleteObjectTagging no se admiten para objetos en depósitos que tienen habilitada la replicación entre cuadrículas.

Si un cliente S3 emite una solicitud PutObjectTagging o DeleteObjectTagging, 501 Not Implemented se devuelve. El mensaje es Put (Delete) ObjectTagging is not available for buckets that have cross-grid replication configured.

Cómo se replican los objetos segmentados

El tamaño máximo de segmento de la cuadrícula de origen se aplica a los objetos replicados en la cuadrícula de destino. Cuando los objetos se replican en otra cuadrícula, la configuración **Tamaño máximo de segmento (CONFIGURACIÓN > Sistema > Opciones de almacenamiento)** de la cuadrícula de origen se utilizará en ambas cuadrículas. Por ejemplo, supongamos que el tamaño máximo de segmento para la cuadrícula de origen es 1 GB, mientras que el tamaño máximo de segmento de la cuadrícula de destino es 50 MB. Si ingiere un objeto de 2 GB en la cuadrícula de origen, ese objeto se guarda como dos segmentos de 1 GB. También se replicará en la red de destino como dos segmentos de 1 GB, aunque el tamaño máximo de segmento de esa red es de 50 MB.

Comparar la replicación entre redes y la replicación de CloudMirror

A medida que comience a utilizar la federación de red, revise las similitudes y diferencias entre ["replicación entre redes"](#) y el ["Servicio de replicación StorageGRID CloudMirror"](#).

	Replicación entre redes	Servicio de replicación CloudMirror
¿Cuál es el propósito principal?	Un sistema StorageGRID actúa como un sistema de recuperación ante desastres. Los objetos de un bucket se pueden replicar entre las cuadrículas en una o ambas direcciones.	Permite que un inquilino replique automáticamente objetos desde un depósito en StorageGRID (origen) a un depósito S3 externo (destino). La replicación de CloudMirror crea una copia independiente de un objeto en una infraestructura S3 independiente. Esta copia independiente no se utiliza como copia de seguridad, sino que a menudo se procesa en la nube.
¿Cómo está configurado?	1. Configurar una conexión de federación de red entre dos redes. 2. Agregue nuevas cuentas de inquilinos, que se clonarán automáticamente en la otra red. 3. Agregue nuevos grupos de inquilinos y usuarios, que también se clonan. 4. Cree depósitos correspondientes en cada cuadrícula y habilite la replicación entre cuadrículas para que se produzca en una o ambas direcciones.	1. Un usuario inquilino configura la replicación de CloudMirror definiendo un punto final de CloudMirror (dirección IP, credenciales, etc.) mediante el Administrador de inquilinos o la API S3. 2. Cualquier depósito propiedad de esa cuenta de inquilino se puede configurar para apuntar al punto final de CloudMirror.

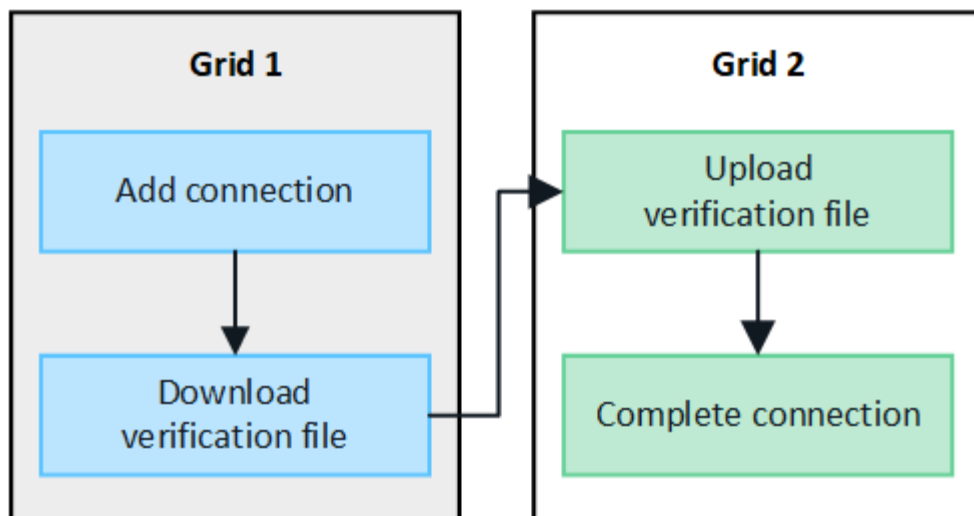
	Replicación entre redes	Servicio de replicación CloudMirror
¿Quién es responsable de configurarlo?	• Un administrador de red configura la conexión y los inquilinos. • Los usuarios inquilinos configuran los grupos, usuarios, claves y depósitos.	Normalmente, un usuario inquilino.
¿Cual es el destino?	Un bucket S3 correspondiente e idéntico en el otro sistema StorageGRID en la conexión de federación de red.	• Cualquier infraestructura S3 compatible (incluido Amazon S3). • Plataforma de Google Cloud (GCP)
¿Es necesario el control de versiones de objetos?	Sí, tanto los depósitos de origen como los de destino deben tener habilitada la versión de objetos.	No, la replicación de CloudMirror admite cualquier combinación de depósitos versionados y no versionados tanto en el origen como en el destino.
¿Qué hace que los objetos se muevan al destino?	Los objetos se replican automáticamente cuando se agregan a un depósito que tiene habilitada la replicación entre cuadrículas.	Los objetos se replican automáticamente cuando se agregan a un depósito que se ha configurado con un punto final de CloudMirror. Los objetos que existían en el depósito de origen antes de que este se configurara con el punto final de CloudMirror no se replican, a menos que se modifiquen.
¿Cómo se replican los objetos?	La replicación entre cuadrículas crea objetos versionados y replica el ID de la versión del depósito de origen al depósito de destino. Esto permite mantener el orden de las versiones en ambas cuadrículas.	La replicación de CloudMirror no requiere depósitos con control de versiones habilitado, por lo que CloudMirror solo puede mantener el orden de una clave dentro de un sitio. No hay garantías de que se mantenga el orden para las solicitudes de un objeto en un sitio diferente.
¿Qué pasa si un objeto no se puede replicar?	El objeto se pone en cola para su replicación, sujeto a los límites de almacenamiento de metadatos.	El objeto se pone en cola para la replicación, sujeto a los límites de los servicios de la plataforma (consulte "Recomendaciones para el uso de los servicios de la plataforma").
¿Se replican los metadatos del sistema del objeto?	Sí, cuando un objeto se replica en la otra red, sus metadatos del sistema también se replican. Los metadatos serán idénticos en ambas cuadrículas.	No, cuando un objeto se replica en el depósito externo, se actualizan sus metadatos del sistema. Los metadatos variarán según la ubicación, dependiendo del momento de la ingesta y del comportamiento de la infraestructura S3 independiente.

	Replicación entre redes	Servicio de replicación CloudMirror
¿Cómo se recuperan los objetos?	Las aplicaciones pueden recuperar o leer objetos realizando una solicitud al depósito en cualquiera de las cuadrículas.	Las aplicaciones pueden recuperar o leer objetos realizando una solicitud a StorageGRID o al destino S3. Por ejemplo, supongamos que utiliza la replicación de CloudMirror para reflejar objetos en una organización asociada. El socio puede utilizar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario utilizar StorageGRID .
¿Qué pasa si se elimina un objeto?	- Las solicitudes de eliminación que incluyen un ID de versión nunca se replican en la cuadrícula de destino. - Las solicitudes de eliminación que no incluyen un ID de versión agregan un marcador de eliminación al depósito de origen, que opcionalmente se puede replicar en la cuadrícula de destino. - Si la replicación entre redes está configurada para una sola dirección, los objetos en el depósito de destino se pueden eliminar sin afectar el origen.	Los resultados variarán según el estado de la versión de los depósitos de origen y destino (que no necesitan ser los mismos): - Si ambos depósitos están versionados, una solicitud de eliminación agregará un marcador de eliminación en ambas ubicaciones. - Si solo está versionado el depósito de origen, una solicitud de eliminación agregará un marcador de eliminación al origen, pero no al destino. - Si ninguno de los buckets tiene versión, una solicitud de eliminación eliminará el objeto del origen pero no del destino. De manera similar, los objetos en el depósito de destino se pueden eliminar sin afectar el origen.

Crear conexiones de federación de red

Puede crear una conexión de federación de red entre dos sistemas StorageGRID si desea clonar detalles de inquilinos y replicar datos de objetos.

Como se muestra en la figura, la creación de una conexión de federación de red incluye pasos en ambas redes. Añade la conexión en una cuadrícula y complétala en la otra cuadrícula. Puedes empezar desde cualquiera de las cuadrículas.



Antes de empezar

- Usted ha revisado el "[Consideraciones y requisitos](#)" para configurar conexiones de federación de red.
- Si planea utilizar nombres de dominio completos (FQDN) para cada cuadrícula en lugar de direcciones IP o VIP, sabe qué nombres usar y ha confirmado que el servidor DNS de cada cuadrícula tiene las entradas adecuadas.
- Está usando un "[navegador web compatible](#)".
- Tiene permiso de acceso de root y la contraseña de aprovisionamiento para ambas redes.

Agregar conexión

Realice estos pasos en cualquiera de los dos sistemas StorageGRID .

Pasos

1. Sign in en el Administrador de cuadrícula desde el nodo de administración principal en cualquiera de las cuadrículas.
2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
3. Seleccione **Agregar conexión**.
4. Introduzca detalles para la conexión.

Campo	Descripción
Nombre de la conexión	Un nombre único para ayudarle a reconocer esta conexión, por ejemplo, "Cuadrícula 1-Cuadrícula 2".
FQDN o IP para esta cuadrícula	Uno de los siguientes: • El FQDN de la red en la que está conectado actualmente • Una dirección VIP de un grupo HA en esta red • Una dirección IP de un nodo de administración o de puerta de enlace en esta red. La IP puede estar en cualquier red a la que pueda acceder la red de destino.

Campo	Descripción
Puerto	El puerto que desea utilizar para esta conexión. Puede ingresar cualquier número de puerto no utilizado del 23000 al 23999. Ambas redes en esta conexión utilizarán el mismo puerto. Debe asegurarse de que ningún nodo de ninguna de las redes utilice este puerto para otras conexiones.
Días de validez del certificado para esta red	El número de días que desea que los certificados de seguridad para esta red en la conexión sean válidos. El valor predeterminado es 730 días (2 años), pero puede ingresar cualquier valor entre 1 y 762 días. StorageGRID genera automáticamente certificados de cliente y servidor para cada cuadrícula cuando guarda la conexión.
Frase de contraseña de aprovisionamiento para esta red	La contraseña de aprovisionamiento para la red en la que ha iniciado sesión.
FQDN o IP para la otra red	Uno de los siguientes: • El FQDN de la red a la que desea conectarse • Una dirección VIP de un grupo HA en la otra red • Una dirección IP de un nodo de administración o de puerta de enlace en la otra red. La IP puede estar en cualquier red a la que la red de origen pueda acceder.

5. Seleccione **Guardar y continuar**.

6. Para el paso Descargar archivo de verificación, seleccione **Descargar archivo de verificación**.

Una vez completada la conexión en la otra red, ya no podrás descargar el archivo de verificación de ninguna de las redes.

7. Localice el archivo descargado(*connection-name.grid-federation*) y guárdelo en un lugar seguro.



Este archivo contiene secretos (enmascarados como *****) y otros detalles confidenciales y deben almacenarse y transmitirse de forma segura.

8. Seleccione **Cerrar** para regresar a la página de federación de Grid.

9. Confirme que se muestra la nueva conexión y que su **Estado de conexión** es **Esperando para conectar**.

10. Proporcionar el *connection-name.grid-federation* archivo al administrador de la red para la otra red.

Conexión completa

Realice estos pasos en el sistema StorageGRID al que se está conectando (la otra red).

Pasos

1. Sign in en Grid Manager desde el nodo de administración principal.

2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
3. Seleccione **Cargar archivo de verificación** para acceder a la página de carga.
4. Seleccione **Subir archivo de verificación**. Luego, busque y seleccione el archivo que se descargó de la primera cuadrícula.(*connection-name.grid-federation*).

Se muestran los detalles de la conexión.

5. Opcionalmente, ingrese un número diferente de días válidos para los certificados de seguridad de esta cuadrícula. La entrada **Días de validez del certificado** tiene como valor predeterminado el que ingresó en la primera cuadrícula, pero cada cuadrícula puede usar fechas de vencimiento diferentes.

En general, utilice la misma cantidad de días para los certificados en ambos lados de la conexión.



Si los certificados en cualquiera de los extremos de la conexión caducan, la conexión dejará de funcionar y las replicaciones quedarán pendientes hasta que se actualicen los certificados.

6. Ingrese la contraseña de aprovisionamiento para la red en la que está conectado actualmente.
7. Seleccione **Guardar y probar**.

Se generan los certificados y se prueba la conexión. Si la conexión es válida, aparece un mensaje de éxito y la nueva conexión aparece en la página de federación de Grid. El **Estado de conexión** será **Conectado**.

Si aparece un mensaje de error, solucione cualquier problema. Ver "[Solucionar errores de federación de red](#)".

8. Vaya a la página de federación de Grid en la primera cuadrícula y actualice el navegador. Confirme que el **Estado de conexión** ahora es **Conectado**.
9. Una vez establecida la conexión, elimine de forma segura todas las copias del archivo de verificación.

Si edita esta conexión, se creará un nuevo archivo de verificación. El archivo original no se puede reutilizar.

Después de terminar

- Revise las consideraciones para "[gestión de inquilinos permitidos](#)".
- "[Crear una o más cuentas de inquilino nuevas](#)", asigne el permiso **Usar conexión de federación de red** y seleccione la nueva conexión.
- "[Administrar la conexión](#)" según sea necesario. Puede editar valores de conexión, probar una conexión, rotar certificados de conexión o eliminar una conexión.
- "[Monitorizar la conexión](#)" como parte de sus actividades normales de monitoreo de StorageGRID .
- "[Solucionar problemas de conexión](#)", incluida la resolución de alertas y errores relacionados con la clonación de cuentas y la replicación entre redes.

Administrar conexiones de federación de red

La administración de las conexiones de federación de red entre sistemas StorageGRID incluye editar los detalles de conexión, rotar los certificados, eliminar los permisos de inquilinos y eliminar las conexiones no utilizadas.

Antes de empezar

- Ha iniciado sesión en el Administrador de cuadrícula en cualquiera de las cuadrículas mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#) para la red en la que ha iniciado sesión.

Editar una conexión de federación de red

Puede editar una conexión de federación de red iniciando sesión en el nodo de administración principal en cualquiera de las redes de la conexión. Después de realizar cambios en la primera cuadrícula, deberá descargar un nuevo archivo de verificación y cargarlo en la otra cuadrícula.



Mientras se edita la conexión, las solicitudes de clonación de cuenta o replicación entre redes continuarán usando las configuraciones de conexión existentes. Cualquier modificación que realice en la primera cuadrícula se guarda localmente, pero no se utiliza hasta que se haya cargado en la segunda cuadrícula, se haya guardado y se haya probado.

Comience a editar la conexión

Pasos

1. Sign in en el Administrador de cuadrícula desde el nodo de administración principal en cualquiera de las cuadrículas.
2. Seleccione **NODOS** y confirme que todos los demás nodos de administración en su sistema estén en línea.



Cuando edita una conexión de federación de red, StorageGRID intenta guardar un archivo de "configuración candidata" en todos los nodos de administración de la primera red. Si este archivo no se puede guardar en todos los nodos de administración, aparecerá un mensaje de advertencia cuando seleccione **Guardar y probar**.

3. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
4. Edite los detalles de la conexión utilizando el menú **Acciones** en la página de federación de Grid o la página de detalles de una conexión específica. Ver ["Crear conexiones de federación de red"](#) para qué entrar.

Menú de acciones

- a. Seleccione el botón de opción para la conexión.
- b. Seleccione **Acciones > Editar**.
- c. Introduzca la nueva información.

Página de detalles

- a. Seleccione un nombre de conexión para mostrar sus detalles.
- b. Seleccione **Editar**.
- c. Introduzca la nueva información.

5. Introduzca la contraseña de aprovisionamiento para la red en la que ha iniciado sesión.
6. Seleccione **Guardar y continuar**.

Los nuevos valores se guardan, pero no se aplicarán a la conexión hasta que haya cargado el nuevo archivo de verificación en la otra cuadrícula.

7. Seleccione **Descargar archivo de verificación**.

Para descargar este archivo más tarde, vaya a la página de detalles de la conexión.

8. Localice el archivo descargado(*connection-name.grid-federation*) y guárdelo en un lugar seguro.



El archivo de verificación contiene secretos y debe almacenarse y transmitirse de forma segura.

9. Seleccione **Cerrar** para regresar a la página de federación de Grid.

10. Confirme que el **Estado de conexión** sea **Pendiente de edición**.



Si el estado de la conexión era distinto de **Conectado** cuando comenzó a editar la conexión, no cambiará a **Pendiente de edición**.

11. Proporcionar el *connection-name.grid-federation* archivo al administrador de la red para la otra red.

Terminar de editar la conexión

Termine de editar la conexión cargando el archivo de verificación en la otra cuadrícula.

Pasos

1. Sign in en Grid Manager desde el nodo de administración principal.
2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
3. Seleccione **Cargar archivo de verificación** para acceder a la página de carga.
4. Seleccione **Subir archivo de verificación**. Luego, busque y seleccione el archivo que se descargó de la primera cuadrícula.
5. Ingrese la contraseña de aprovisionamiento para la red en la que está conectado actualmente.
6. Seleccione **Guardar y probar**.

Si se puede establecer la conexión utilizando los valores editados, aparecerá un mensaje de éxito. De lo contrario, aparecerá un mensaje de error. Revise el mensaje y solucione cualquier problema.

7. Cierre el asistente para regresar a la página de federación de Grid.
8. Confirme que el **Estado de conexión** sea **Conectado**.
9. Vaya a la página de federación de Grid en la primera cuadrícula y actualice el navegador. Confirme que el **Estado de conexión** ahora es **Conectado**.
10. Una vez establecida la conexión, elimine de forma segura todas las copias del archivo de verificación.

Pruebe una conexión de federación de red

Pasos

1. Sign in en Grid Manager desde el nodo de administración principal.
2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.

3. Pruebe la conexión utilizando el menú **Acciones** en la página de federación de Grid o la página de detalles de una conexión específica.

Menú de acciones

- a. Seleccione el botón de opción para la conexión.
- b. Seleccione **Acciones > Prueba**.

Página de detalles

- a. Seleccione un nombre de conexión para mostrar sus detalles.
- b. Seleccione **Probar conexión**.

4. Revisar el estado de la conexión:

Estado de la conexión	Descripción
Conectado	Ambas redes están conectadas y se comunican normalmente.
Error	La conexión está en un estado de error. Por ejemplo, un certificado ha expirado o un valor de configuración ya no es válido.
Pendiente de edición	Ha editado la conexión en esta cuadrícula, pero la conexión aún utiliza la configuración existente. Para completar la edición, cargue el nuevo archivo de verificación en la otra cuadrícula.
Esperando para conectar	Ha configurado la conexión en esta red, pero la conexión no se ha completado en la otra red. Descargue el archivo de verificación de esta cuadrícula y cárguelo en la otra cuadrícula.
Desconocido	La conexión está en un estado desconocido, posiblemente debido a un problema de red o un nodo fuera de línea.

5. Si el estado de la conexión es **Error**, resuelva cualquier problema. Luego, seleccione **Probar conexión** nuevamente para confirmar que el problema se ha solucionado.

Rotar certificados de conexión

Cada conexión de federación de red utiliza cuatro certificados SSL generados automáticamente para proteger la conexión. Cuando los dos certificados de cada red se acercan a su fecha de vencimiento, la alerta **Vencimiento del certificado de federación de red** le recuerda que debe rotar los certificados.



Si los certificados en cualquiera de los extremos de la conexión caducan, la conexión dejará de funcionar y las replicaciones quedarán pendientes hasta que se actualicen los certificados.

Pasos

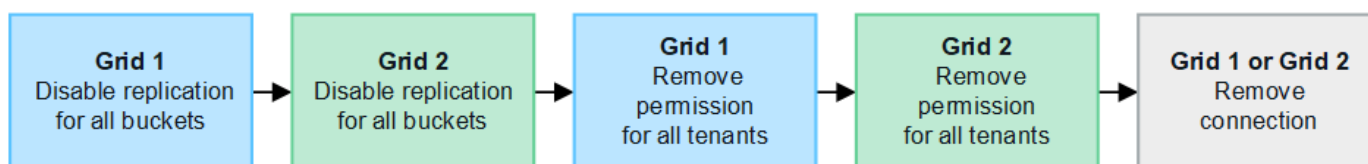
1. Sign in en el Administrador de cuadrícula desde el nodo de administración principal en cualquiera de las cuadrículas.
2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.

- Desde cualquiera de las pestañas de la página de federación de Grid, seleccione el nombre de la conexión para mostrar sus detalles.
- Seleccione la pestaña **Certificados**.
- Seleccione **Rotar certificados**.
- Especifique cuántos días deben ser válidos los nuevos certificados.
- Introduzca la contraseña de aprovisionamiento para la red en la que ha iniciado sesión.
- Seleccione **Rotar certificados**.
- Según sea necesario, repita estos pasos en la otra cuadrícula de la conexión.

En general, utilice la misma cantidad de días para los certificados en ambos lados de la conexión.

Eliminar una conexión de federación de red

Puede eliminar una conexión de federación de red de cualquiera de las redes en la conexión. Como se muestra en la figura, debe realizar los pasos previos necesarios en ambas redes para confirmar que ningún inquilino en ninguna de las redes esté utilizando la conexión.



Antes de eliminar una conexión, tenga en cuenta lo siguiente:

- Eliminar una conexión no elimina ningún elemento que ya se haya copiado entre cuadrículas. Por ejemplo, los usuarios, grupos y objetos del inquilino que existen en ambas cuadrículas no se eliminan de ninguna de las cuadrículas cuando se elimina el permiso del inquilino. Si desea eliminar estos elementos, deberá eliminarlos manualmente de ambas cuadrículas.
- Cuando elimina una conexión, todos los objetos que estén pendientes de replicación (ingeridos pero aún no replicados en la otra red) tendrán una falla permanente en su replicación.

Deshabilitar la replicación para todos los depósitos de inquilinos

Pasos

- Para comenzar desde cualquiera de las cuadrículas, inicie sesión en el Administrador de cuadrícula desde el nodo de administración principal.
- Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
- Seleccione el nombre de la conexión para mostrar sus detalles.
- En la pestaña **Inquilinos permitidos**, determine si algún inquilino está utilizando la conexión.
- Si hay inquilinos en la lista, instruya a todos los inquilinos a ["Deshabilitar la replicación entre redes"](#) para todos sus cubos en ambas redes en la conexión.



No puedes eliminar el permiso **Usar conexión de federación de red** si alguno de los depósitos de inquilinos tiene habilitada la replicación entre redes. Cada cuenta de inquilino debe deshabilitar la replicación entre redes para sus depósitos en ambas redes.

Eliminar el permiso para cada inquilino

Una vez que se haya deshabilitado la replicación entre redes para todos los grupos de inquilinos, elimine el **permiso de uso de federación de red** de todos los inquilinos en ambas redes.

Pasos

1. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
2. Seleccione el nombre de la conexión para mostrar sus detalles.
3. Para cada inquilino en la pestaña **Inquilinos permitidos**, elimine el permiso **Usar conexión de federación de red** de cada inquilino. Ver "[Gestionar inquilinos permitidos](#)".
4. Repita estos pasos para los inquilinos permitidos en la otra cuadrícula.

Eliminar conexión

Pasos

1. Cuando ningún inquilino en ninguna de las redes esté usando la conexión, seleccione **Eliminar**.
2. Revise el mensaje de confirmación y seleccione **Eliminar**.
 - Si se puede eliminar la conexión, se muestra un mensaje de éxito. La conexión de federación de red ahora se elimina de ambas redes.
 - Si no se puede eliminar la conexión (por ejemplo, todavía está en uso o hay un error de conexión), se muestra un mensaje de error. Puede realizar cualquiera de las siguientes acciones:
 - Resolver el error (recomendado). Ver "[Solucionar errores de federación de red](#)".
 - Retire la conexión a la fuerza. Vea la siguiente sección.

Eliminar una conexión de federación de red por la fuerza

Si es necesario, puede forzar la eliminación de una conexión que no tenga el estado **Conectado**.

La eliminación forzada solo elimina la conexión de la red local. Para eliminar completamente la conexión, realice los mismos pasos en ambas rejillas.

Pasos

1. Desde el cuadro de diálogo de confirmación, seleccione **Forzar eliminación**.

Aparece un mensaje de éxito. Esta conexión de federación de red ya no se puede utilizar. Sin embargo, es posible que los depósitos de inquilinos aún tengan habilitada la replicación entre redes y que algunas copias de objetos ya se hayan replicado entre las redes de la conexión.
2. Desde la otra cuadrícula en la conexión, inicie sesión en el Administrador de cuadrícula desde el nodo de administración principal.
3. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
4. Seleccione el nombre de la conexión para mostrar sus detalles.
5. Seleccione **Eliminar y Sí**.
6. Seleccione **Eliminar forzosamente** para eliminar la conexión de esta red.

Gestionar los inquilinos permitidos para la federación de red

Puede permitir que las cuentas de inquilinos de S3 utilicen una conexión de federación

de red entre dos sistemas StorageGRID . Cuando a los inquilinos se les permite usar una conexión, se requieren pasos especiales para editar los detalles del inquilino o eliminar de forma permanente el permiso de un inquilino para usar la conexión.

Antes de empezar

- Ha iniciado sesión en el Administrador de cuadrícula en cualquiera de las cuadrículas mediante un [navegador web compatible](#) .
- Tú tienes el ["Permiso de acceso root"](#) para la red en la que ha iniciado sesión.
- Tienes ["creó una conexión de federación de red"](#) entre dos rejillas.
- Has revisado los flujos de trabajo para ["clon de cuenta"](#) y ["replicación entre redes"](#) .
- Según sea necesario, ya ha configurado el inicio de sesión único (SSO) o la federación de identidad para ambas redes en la conexión. Ver ["¿Qué es la clonación de cuenta?"](#) .

Crear un inquilino permitido

Si desea permitir que una cuenta de inquilino nueva o existente utilice una conexión de federación de red para la clonación de cuentas y la replicación entre redes, siga las instrucciones generales para ["crear un nuevo inquilino S3"](#) o ["editar una cuenta de inquilino"](#) y tenga en cuenta lo siguiente:

- Puede crear el inquilino desde cualquiera de las cuadrículas en la conexión. La cuadrícula en la que se crea un inquilino es la cuadrícula de origen del inquilino.
- El estado de la conexión debe ser **Conectado**.
- Cuando se crea o edita el inquilino para habilitar el permiso **Usar conexión de federación de red** y luego se guarda en la primera red, un inquilino idéntico se replica automáticamente en la otra red. La cuadrícula en la que se replica el inquilino es la cuadrícula de destino del inquilino.
- Los inquilinos de ambas redes tendrán el mismo ID de cuenta de 20 dígitos, nombre, descripción, cuota y permisos. Opcionalmente, puede utilizar el campo **Descripción** para ayudar a identificar cuál es el inquilino de origen y cuál es el inquilino de destino. Por ejemplo, esta descripción para un inquilino creado en la Red 1 también aparecerá para el inquilino replicado en la Red 2: "Este inquilino fue creado en la Red 1".
- Por razones de seguridad, la contraseña de un usuario root local no se copia a la red de destino.



Antes de que un usuario raíz local pueda iniciar sesión en el inquilino replicado en la red de destino, un administrador de red para esa red debe ["cambiar la contraseña del usuario root local"](#) .

- Una vez que el inquilino nuevo o editado esté disponible en ambas cuadrículas, los usuarios inquilinos pueden realizar estas operaciones:
 - Desde la red de origen del inquilino, cree grupos y usuarios locales, que se clonarán automáticamente en la red de destino del inquilino. Ver ["Clonar grupos de inquilinos y usuarios"](#) .
 - Cree nuevas claves de acceso S3, que pueden clonarse opcionalmente en la red de destino del inquilino. Ver ["Clonar claves de acceso S3 usando la API"](#) .
 - Cree depósitos idénticos en ambas cuadrículas de la conexión y habilite la replicación entre cuadrículas en una dirección o en ambas direcciones. Ver ["Administrar la replicación entre redes"](#) .

Ver un inquilino permitido

Puede ver los detalles de un inquilino que tiene permiso para utilizar una conexión de federación de red.

Pasos

1. Seleccione **INQUILINOS**.
2. Desde la página Inquilinos, seleccione el nombre del inquilino para ver la página de detalles del inquilino.

Si esta es la cuadrícula de origen del inquilino (es decir, si el inquilino se creó en esta cuadrícula), aparece un banner para recordarle que el inquilino se clonó en otra cuadrícula. Si edita o elimina este inquilino, sus cambios no se sincronizarán con la otra cuadrícula.

Tenants > tenant A for grid federation

tenant A for grid federation

Tenant ID: 0899 6970 1700 0930 0009

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Description: this tenant was created on Grid 1

Sign in

Edit

Actions ▾

This tenant has been cloned to another grid. If you edit or delete this tenant, your changes will not be synced to the other grid.

Space breakdown

Allowed features

Grid federation

Remove permission

Clear error

Search...

Displaying one result

Connection name	Connection status	Remote grid hostname	Last error
Grid 1 to Grid 2	✓ Connected	10.96.106.230	Check for errors

3. Opcionalmente, seleccione la pestaña **Federación de red** para [supervisar la conexión de la federación de red](#).

Editar un inquilino permitido

Si necesita editar un inquilino que tiene el permiso **Usar conexión de federación de red**, siga las instrucciones generales para [editar una cuenta de inquilino](#) y tenga en cuenta lo siguiente:

- Si un inquilino tiene el permiso **Usar conexión de federación de red**, puede editar los detalles del inquilino desde cualquiera de las redes en la conexión. Sin embargo, cualquier cambio que realice no se copiará a la otra cuadrícula. Si desea mantener los detalles del inquilino sincronizados entre las cuadrículas, debe realizar las mismas ediciones en ambas cuadrículas.

- No puedes borrar el permiso **Usar conexión de federación de red** cuando estás editando un inquilino.
- No puedes seleccionar una conexión de federación de red diferente cuando estás editando un inquilino.

Eliminar un inquilino permitido

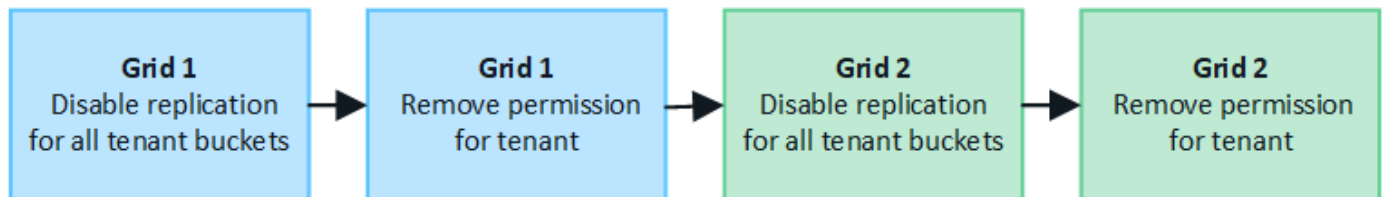
Si necesita eliminar un inquilino que tiene el permiso **Usar conexión de federación de red**, siga las instrucciones generales para ["eliminar una cuenta de inquilino"](#) y tenga en cuenta lo siguiente:

- Antes de poder eliminar al inquilino original en la red de origen, debe eliminar todos los depósitos de la cuenta en la red de origen.
- Antes de poder eliminar el inquilino clonado en la cuadrícula de destino, debe eliminar todos los depósitos de la cuenta en la cuadrícula de destino.
- Si elimina el inquilino original o el clonado, la cuenta ya no podrá usarse para la replicación entre redes.
- Si elimina el inquilino original de la red de origen, los grupos de inquilinos, usuarios o claves que se hayan clonado en la red de destino no se verán afectados. Puede eliminar el inquilino clonado o permitirle administrar sus propios grupos, usuarios, claves de acceso y depósitos.
- Si elimina el inquilino clonado en la cuadrícula de destino, se producirán errores de clonación si se agregan nuevos grupos o usuarios al inquilino original.

Para evitar estos errores, elimine el permiso del inquilino para usar la conexión de federación de red antes de eliminarlo de esta red.

Eliminar el permiso de conexión de federación de red

Para evitar que un inquilino utilice una conexión de federación de red, debe eliminar el permiso **Usar conexión de federación de red**.



Antes de quitarle el permiso a un inquilino para usar una conexión de federación de red, tenga en cuenta lo siguiente:

- No puedes eliminar el permiso **Usar conexión de federación de red** si alguno de los depósitos del inquilino tiene habilitada la replicación entre redes. Primero, la cuenta del inquilino debe deshabilitar la replicación entre redes para todos sus depósitos.
- Quitar el permiso **Usar conexión de federación de red** no elimina ningún elemento que ya se haya replicado entre redes. Por ejemplo, los usuarios, grupos y objetos de inquilinos que existen en ambas cuadrículas no se eliminan de ninguna de ellas cuando se elimina el permiso del inquilino. Si desea eliminar estos elementos, deberá eliminarlos manualmente de ambas cuadrículas.
- Si desea volver a habilitar este permiso con la misma conexión de federación de red, elimine primero este inquilino en la red de destino; de lo contrario, volver a habilitar este permiso generará un error.



Al volver a habilitar el permiso **Usar conexión de federación de red**, la red local se convierte en la red de origen y activa la clonación a la red remota especificada por la conexión de federación de red seleccionada. Si la cuenta del inquilino ya existe en la red remota, la clonación generará un error de conflicto.

Antes de empezar

- Estás usando un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) para ambas cuadrículas.

Deshabilitar la replicación para los depósitos de inquilinos

Como primer paso, deshabilite la replicación entre redes para todos los grupos de inquilinos.

Pasos

1. Para comenzar desde cualquiera de las cuadrículas, inicie sesión en el Administrador de cuadrícula desde el nodo de administración principal.
2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
3. Seleccione el nombre de la conexión para mostrar sus detalles.
4. En la pestaña **Inquilinos permitidos**, determine si el inquilino está usando la conexión.
5. Si el inquilino está en la lista, indíquele que ["Deshabilitar la replicación entre redes"](#) para todos sus cubos en ambas redes en la conexión.



No puedes eliminar el permiso **Usar conexión de federación de red** si alguno de los depósitos de inquilinos tiene habilitada la replicación entre redes. El inquilino debe deshabilitar la replicación entre redes para sus depósitos en ambas redes.

Quitar el permiso al inquilino

Una vez deshabilitada la replicación entre redes para los depósitos de inquilinos, puede eliminar el permiso del inquilino para usar la conexión de federación de red.

Pasos

1. Sign in en Grid Manager desde el nodo de administración principal.
2. Eliminar el permiso de la página de federación de Grid o de la página de inquilinos.

Página de federación de red

- a. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
- b. Seleccione el nombre de la conexión para mostrar su página de detalles.
- c. En la pestaña **Inquilinos permitidos**, seleccione el botón de opción para el inquilino.
- d. Seleccione **Quitar permiso**.

Página de inquilinos

- a. Seleccione **INQUILINOS**.
- b. Seleccione el nombre del inquilino para mostrar la página de detalles.
- c. En la pestaña **Federación de red**, seleccione el botón de opción para la conexión.
- d. Seleccione **Quitar permiso**.

3. Revise las advertencias en el cuadro de diálogo de confirmación y seleccione **Eliminar**.
 - Si se puede eliminar el permiso, regresará a la página de detalles y se mostrará un mensaje de éxito.

Este inquilino ya no puede utilizar la conexión de federación de red.

- Si uno o más depósitos de inquilinos aún tienen habilitada la replicación entre redes, se muestra un error.

 **Remove permission to use grid federation connection** 

Are you sure you want to prevent **Tenant A** from performing account sync and cross-grid replication using grid federation connection **Grid 1-Grid 2**?

- Removing this permission does not delete any items that have already been copied to the other grid.
- After removing this permission for the tenant on this grid, go to the other grid and remove the permission for the corresponding tenant account.

 Connection '5427cbf8-0dd0-4b83-a2c8-e5e23cc49cc5' is used by bucket 'my-cgr-bucket' for cross-grid replication, so it can't be removed. From Tenant Manager, remove the cross-grid configuration from the tenant bucket and retry.

 Using **Force remove** removes the tenant's permission to use the grid federation connection even if tenant buckets still have cross-grid replication enabled. When the permission is removed, data in these buckets can no longer be copied between the grids.

Cancel Force remove Remove

Puede realizar cualquiera de las siguientes acciones:

- (Recomendado.) Sign in en el Administrador de inquilinos y deshabilite la replicación para cada uno de los grupos de inquilinos. Ver ["Administrar la replicación entre redes"](#) . Luego, repita los pasos para eliminar el permiso **Usar conexión a la red**.
 - Quitar el permiso por la fuerza. Vea la siguiente sección.
4. Vaya a la otra cuadrícula y repita estos pasos para eliminar el permiso para el mismo inquilino en la otra cuadrícula.

Eliminar el permiso por la fuerza

Si es necesario, puede forzar la eliminación del permiso de un inquilino para usar una conexión de federación de red incluso si los depósitos de inquilinos tienen habilitada la replicación entre redes.

Antes de retirar por la fuerza el permiso de un inquilino, tenga en cuenta las consideraciones generales para [eliminando el permiso](#) así como estas consideraciones adicionales:

- Si elimina el permiso **Usar conexión de federación de red** por la fuerza, todos los objetos que estén pendientes de replicación en la otra red (ingeridos pero aún no replicados) continuarán replicándose. Para evitar que estos objetos en proceso lleguen al depósito de destino, también debe eliminar el permiso del inquilino en la otra cuadrícula.
- Cualquier objeto ingerido en el depósito de origen después de eliminar el permiso **Usar conexión de federación de red** nunca se replicará en el depósito de destino.

Pasos

1. Sign in en Grid Manager desde el nodo de administración principal.
2. Seleccione **CONFIGURACIÓN > Sistema > Federación de red**.
3. Seleccione el nombre de la conexión para mostrar su página de detalles.
4. En la pestaña **Inquilinos permitidos**, seleccione el botón de opción para el inquilino.
5. Seleccione **Quitar permiso**.
6. Revise las advertencias en el cuadro de diálogo de confirmación y seleccione **Forzar eliminación**.

Aparece un mensaje de éxito. Este inquilino ya no puede utilizar la conexión de federación de red.

7. Según sea necesario, vaya a la otra cuadrícula y repita estos pasos para eliminar a la fuerza el permiso para la misma cuenta de inquilino en la otra cuadrícula. Por ejemplo, debe repetir estos pasos en la otra cuadrícula para evitar que los objetos en proceso lleguen al depósito de destino.

Solucionar errores de federación de red

Es posible que necesite solucionar alertas y errores relacionados con las conexiones de federación de red, la clonación de cuentas y la replicación entre redes.

Alertas y errores de conexión de la federación de red

Es posible que reciba alertas o experimente errores con sus conexiones de federación de red.

Después de realizar cualquier cambio para resolver un problema de conexión, pruebe la conexión para asegurarse de que el estado de la conexión vuelva a **Conectado**. Para obtener instrucciones, consulte ["Administrar conexiones de federación de red"](#).

Alerta de fallo de conexión de la federación de red

Asunto

Se activó la alerta **Error de conexión de federación de red**.

Detalles

Esta alerta indica que la conexión de federación de red entre las redes no está funcionando.

Acciones recomendadas

1. Revise la configuración en la página Federación de cuadrícula para ambas cuadrículas. Confirme que todos los valores sean correctos. Ver ["Administrar conexiones de federación de red"](#).
2. Revise los certificados utilizados para la conexión. Asegúrese de que no haya alertas de certificados de federación de red vencidos y que los detalles de cada certificado sean válidos. Consulte las instrucciones para rotar los certificados de conexión en ["Administrar conexiones de federación de red"](#).
3. Confirme que todos los nodos de administración y de puerta de enlace en ambas redes estén en línea y disponibles. Resuelva cualquier alerta que pueda estar afectando a estos nodos y vuelva a intentarlo.

4. Si proporcionó un nombre de dominio completo (FQDN) para la red local o remota, confirme que el servidor DNS esté en línea y disponible. Ver "[¿Qué es la federación de red?](#)" para requisitos de redes, direcciones IP y DNS.

Alerta de vencimiento del certificado de federación de red

Asunto

Se activó la alerta **Expiración del certificado de federación de red**.

Detalles

Esta alerta indica que uno o más certificados de federación de red están a punto de vencer.

Acciones recomendadas

Consulte las instrucciones para rotar los certificados de conexión en "[Administrar conexiones de federación de red](#)".

Error al editar una conexión de federación de red

Asunto

Al editar una conexión de federación de red, verá el siguiente mensaje de advertencia cuando seleccione **Guardar y probar**: "Error al crear un archivo de configuración candidato en uno o más nodos".

Detalles

Cuando edita una conexión de federación de red, StorageGRID intenta guardar un archivo de "configuración candidata" en todos los nodos de administración de la primera red. Aparece un mensaje de advertencia si este archivo no se puede guardar en todos los nodos de administración, por ejemplo, porque un nodo de administración está desconectado.

Acciones recomendadas

1. Desde la cuadrícula que está utilizando para editar la conexión, seleccione **NODOS**.
2. Confirme que todos los nodos de administración de esa red estén en línea.
3. Si algún nodo está fuera de línea, vuelva a conectarlo e intente editar la conexión nuevamente.

Errores de clonación de cuenta

No puedo iniciar sesión en una cuenta de inquilino clonada

Asunto

No puedes iniciar sesión en una cuenta de inquilino clonada. El mensaje de error en la página de inicio de sesión del Administrador de inquilinos es "Sus credenciales para esta cuenta no son válidas". Por favor, inténtelo de nuevo."

Detalles

Por razones de seguridad, cuando se clona una cuenta de inquilino desde la red de origen del inquilino a la red de destino del inquilino, la contraseña establecida para el usuario raíz local del inquilino no se clona. De manera similar, cuando un inquilino crea usuarios locales en su red de origen, las contraseñas de los usuarios locales no se clonan en la red de destino.

Acciones recomendadas

Antes de que el usuario raíz pueda iniciar sesión en la red de destino del inquilino, un administrador de la red debe primero "[cambiar la contraseña del usuario root local](#)" en la cuadrícula de destino.

Antes de que un usuario local clonado pueda iniciar sesión en la red de destino del inquilino, el usuario raíz del inquilino clonado debe agregar una contraseña para el usuario en la red de destino. Para obtener instrucciones, consulte "[Administrar usuarios locales](#)" en las instrucciones para utilizar el Administrador de inquilinos.

Inquilino creado sin un clon

Asunto

Verá el mensaje "Inquilino creado sin un clon" después de crear un nuevo inquilino con el permiso **Usar conexión de federación de red**.

Detalles

Este problema puede ocurrir si las actualizaciones del estado de la conexión se retrasan, lo que podría provocar que una conexión no saludable aparezca como **Conectada**.

Acciones recomendadas

1. Revise el motivo que aparece en el mensaje de error y resuelva cualquier problema de red o de otro tipo que pueda impedir que la conexión funcione. Ver [Alertas y errores de conexión de la federación de red](#) .
2. Siga las instrucciones para probar una conexión de federación de red en "[Administrar conexiones de federación de red](#)" para confirmar que el problema se ha solucionado.
3. Desde la cuadrícula de origen del inquilino, seleccione **INQUILINOS**.
4. Localice la cuenta de inquilino que no se pudo clonar.
5. Seleccione el nombre del inquilino para mostrar la página de detalles.
6. Seleccione **Reintentar clonar cuenta**.

Tenants > test

test

Tenant ID:0040 2213 8117 4859 6503

Protocol:S3

Object count:0

Quota utilization:—

Logical space used:0 bytes

Quota:—

Sign in

Edit

Actions

Tenant account could not be cloned to the other grid.
Reason: Internal server error. The server encountered an error and could not complete your request. Try again. If the problem persists, contact support. Internal Server Error

Retry account clone

Si se ha resuelto el error, la cuenta del inquilino ahora se clonará a la otra red.

Alertas y errores de replicación entre redes

Último error mostrado para la conexión o el inquilino

Asunto

Cuando "Visualización de una conexión de federación de red" (o cuando "gestión de los inquilinos permitidos" para una conexión), observa un error en la columna **Último error** en la página de detalles de la conexión. Por ejemplo:

Grid 1 - Grid 2

Local hostname (this grid):

10.96.130.64

Port:

23000

Remote hostname (other grid):

10.96.130.76

Connection status:

✓

Connected

Edit

Download file

Test connection

Remove

Permitted tenants

Certificates

Remove permission

Clear error

Search...

Displaying one result

Tenant name	Last error
Tenant A	2022-12-22 16:19:20 MST Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-bucket' to destination bucket 'my-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 13916508109026943924) Check for errors

Detalles

Para cada conexión de federación de red, la columna **Último error** muestra el error más reciente que ocurrió, si lo hubo, cuando los datos de un inquilino se estaban replicando a la otra red. Esta columna solo muestra el último error de replicación entre redes que ocurrió; no se mostrarán los errores anteriores que pudieran haber ocurrido. Un error en esta columna podría ocurrir por una de estas razones:

- No se encontró la versión del objeto de origen.
- No se encontró el depósito de origen.
- Se eliminó el depósito de destino.
- El depósito de destino fue recreado por una cuenta diferente.
- El bucket de destino tiene la versión suspendida.
- El depósito de destino fue recreado por la misma cuenta pero ahora no tiene versión.

Acciones recomendadas

Si aparece un mensaje de error en la columna **Último error**, siga estos pasos:

1. Revise el texto del mensaje.
2. Realice cualquier acción recomendada. Por ejemplo, si se suspendió el control de versiones en el depósito de destino para la replicación entre redes, vuelva a habilitar el control de versiones para ese depósito.

3. Seleccione la conexión o la cuenta de inquilino de la tabla.
4. Seleccione **Borrar error**.
5. Seleccione **Sí** para borrar el mensaje y actualizar el estado del sistema.
6. Espere 5-6 minutos y luego ingiera un nuevo objeto en el balde. Confirme que el mensaje de error no vuelva a aparecer.



Para garantizar que se borre el mensaje de error, espere al menos 5 minutos después de la marca de tiempo en el mensaje antes de ingerir un nuevo objeto.



Después de eliminar el error, es posible que aparezca un nuevo **Último error** si los objetos se ingieren en un depósito diferente que también tiene un error.

7. Para determinar si algún objeto no se pudo replicar debido al error del depósito, consulte "[Identificar y reintentar operaciones de replicación fallidas](#)".

Alerta de fallo permanente de replicación entre redes

Asunto

Se activó la alerta **Error permanente de replicación entre redes**.

Detalles

Esta alerta indica que los objetos de inquilino no se pueden replicar entre los depósitos en dos cuadrículas por un motivo que requiere la intervención del usuario para resolverlo. Esta alerta generalmente es causada por un cambio en el depósito de origen o de destino.

Acciones recomendadas

1. Sign in en la red donde se activó la alerta.
2. Vaya a **CONFIGURACIÓN > Sistema > Federación de red** y localice el nombre de la conexión que aparece en la alerta.
3. En la pestaña Inquilinos permitidos, mire la columna **Último error** para determinar qué cuentas de inquilino tienen errores.
4. Para obtener más información sobre la falla, consulte las instrucciones en "[Supervisar las conexiones de la federación de red](#)" para revisar las métricas de replicación entre redes.
5. Para cada cuenta de inquilino afectada:
 - a. Vea las instrucciones en "[Supervisar la actividad de los inquilinos](#)" para confirmar que el inquilino no ha excedido su cuota en la red de destino para la replicación entre redes.
 - b. Según sea necesario, aumente la cuota del inquilino en la red de destino para permitir que se guarden nuevos objetos.
6. Para cada inquilino afectado, inicie sesión en Tenant Manager en ambas cuadrículas, para que pueda comparar la lista de grupos.
7. Para cada bucket que tenga habilitada la replicación entre redes, confirme lo siguiente:
 - Hay un depósito correspondiente para el mismo inquilino en la otra cuadrícula (debe usar el nombre exacto).
 - Ambos depósitos tienen habilitada la versión de objetos (la versión no se puede suspender en ninguna de las cuadrículas).
 - Ambos depósitos tienen el bloqueo de objetos S3 deshabilitado.

- Ninguno de los depósitos está en estado **Eliminando objetos: solo lectura**.

8. Para confirmar que el problema se resolvió, consulte las instrucciones en "[Supervisar las conexiones de la federación de red](#)" para revisar las métricas de replicación entre redes o realizar estos pasos:
 - a. Regresar a la página de federación de Grid.
 - b. Seleccione el inquilino afectado y seleccione **Borrar error** en la columna **Último error**.
 - c. Seleccione **Sí** para borrar el mensaje y actualizar el estado del sistema.
 - d. Espere 5-6 minutos y luego ingiera un nuevo objeto en el balde. Confirme que el mensaje de error no vuelva a aparecer.



Para garantizar que se borre el mensaje de error, espere al menos 5 minutos después de la marca de tiempo en el mensaje antes de ingerir un nuevo objeto.



La alerta podría tardar hasta un día en desaparecer después de resolverse.

- a. Ir a "[Identificar y reintentar operaciones de replicación fallidas](#)" para identificar cualquier objeto o eliminar marcadores que no se pudieron replicar en la otra cuadrícula y volver a intentar la replicación según sea necesario.

Alerta de recurso de replicación entre redes no disponible

Asunto

Se activó la alerta **Recurso de replicación entre redes no disponible**.

Detalles

Esta alerta indica que hay solicitudes de replicación entre redes pendientes porque un recurso no está disponible. Por ejemplo, podría haber un error de red.

Acciones recomendadas

1. Monitoree la alerta para ver si el problema se resuelve por sí solo.
2. Si el problema persiste, determine si alguna de las redes tiene una alerta de **Fallo de conexión de federación de red** para la misma conexión o una alerta de **No se puede comunicar con el nodo** para un nodo. Esta alerta podría resolverse cuando resuelvas esas alertas.
3. Para obtener más información sobre la falla, consulte las instrucciones en "[Supervisar las conexiones de la federación de red](#)" para revisar las métricas de replicación entre redes.
4. Si no puede resolver la alerta, comuníquese con el soporte técnico.

La replicación entre redes continuará de manera normal luego de que se resuelva el problema.

Identificar y reintentar operaciones de replicación fallidas

Después de resolver la alerta **Error permanente de replicación entre cuadrículas**, debe determinar si algún objeto o marcador de eliminación no se pudo replicar en la otra cuadrícula. Luego puede volver a ingerir estos objetos o utilizar la API de administración de cuadrícula para volver a intentar la replicación.

La alerta **Error permanente de replicación entre cuadrículas** indica que los objetos de inquilino no se pueden replicar entre los depósitos en dos cuadrículas por un motivo que requiere la intervención del usuario para resolverlo. Esta alerta generalmente es causada por un cambio en el depósito de origen o de destino.

Para obtener más información, consulte ["Solucionar errores de federación de red"](#) .

Determinar si algún objeto no se pudo replicar

Para determinar si algún objeto o marcador de eliminación no se ha replicado en la otra cuadrícula, puede buscar en el registro de auditoría ["CGRR \(Solicitud de replicación entre redes\)"](#) mensajes. Este mensaje se agrega al registro cuando StorageGRID no puede replicar un objeto, un objeto multiparte o un marcador de eliminación en el depósito de destino.

Puedes utilizar el ["herramienta de auditoría y explicación"](#) para traducir los resultados a un formato más fácil de leer.

Antes de empezar

- Tienes permiso de acceso root.
- Tú tienes el `Passwords.txt` archivo.
- Conoces la dirección IP del nodo de administración principal.

Pasos

1. Inicie sesión en el nodo de administración principal:
 - a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

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

2. Busque mensajes CGRR en `audit.log` y utilice la herramienta `audit-explain` para dar formato a los resultados.

Por ejemplo, este comando busca todos los mensajes CGRR de los últimos 30 minutos y utiliza la herramienta `audit-explain`.

```
# awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date {
print }' audit.log | grep CGRR | audit-explain
```

Los resultados del comando se verán como este ejemplo, que tiene entradas para seis mensajes CGRR. En el ejemplo, todas las solicitudes de replicación entre redes devolvieron un error general porque no se pudo replicar el objeto. Los primeros tres errores son para operaciones de "replicar objeto" y los últimos tres errores son para operaciones de "replicar marcador de eliminación".

```

CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error

```

Cada entrada contiene la siguiente información:

Campo	Descripción
Solicitud de replicación entre redes CGRR	El nombre de la solicitud
arrendatario	ID de la cuenta del inquilino
conexión	El ID de la conexión de la federación de red
operación	El tipo de operación de replicación que se estaba intentando: • replicar objeto • replicar marcador de eliminación • replicar objeto multiparte
balde	El nombre del cubo
objeto	El nombre del objeto
versión	El ID de la versión del objeto

Campo	Descripción
error	El tipo de error. Si la replicación entre redes falla, el error es "Error general".

Reintentar replicaciones fallidas

Después de generar una lista de objetos y eliminar marcadores que no se replicaron en el depósito de destino y resolver los problemas subyacentes, puede volver a intentar la replicación de una de estas dos maneras:

- Reingerir cada objeto en el depósito de origen.
- Utilice la API privada de administración de cuadrícula, como se describe.

Pasos

1. Desde la parte superior del Administrador de cuadrícula, seleccione el ícono de ayuda y seleccione **Documentación de API**.
2. Seleccione **Ir a la documentación de API privada**.



Los puntos finales de la API de StorageGRID que están marcados como "Privados" están sujetos a cambios sin previo aviso. Los puntos finales privados de StorageGRID también ignoran la versión API de la solicitud.

3. En la sección **cross-grid-replication-advanced**, seleccione el siguiente punto final:

```
POST /private/cross-grid-replication-retry-failed
```

4. Seleccione **Probarlo**.
5. En el cuadro de texto **body**, reemplace la entrada de ejemplo para **versionID** con un ID de versión del audit.log que corresponde a una solicitud de replicación entre redes fallida.

Asegúrese de conservar las comillas dobles alrededor de la cadena.

6. Seleccione **Ejecutar**.
7. Confirme que el código de respuesta del servidor es **204**, lo que indica que el objeto o el marcador de eliminación se ha marcado como pendiente para la replicación entre cuadrículas a la otra cuadrícula.



Pendiente significa que la solicitud de replicación entre redes se ha agregado a la cola interna para su procesamiento.

Monitorear reintentos de replicación

Debe supervisar las operaciones de reintento de replicación para asegurarse de que se completen.



Podría tomar varias horas o más para que un objeto o un marcador de eliminación se replique en la otra cuadrícula.

Puede supervisar las operaciones de reintento de dos maneras:

- Utilice un S3 "[Objeto principal](#)" o "[Obtener objeto](#)" pedido. La respuesta incluye el StorageGRID específico

x-ntap-sg-cgr-replication-status encabezado de respuesta, que tendrá uno de los siguientes valores:

Red	Estado de replicación
Fuente	• COMPLETADO: La replicación fue exitosa. • PENDIENTE: El objeto aún no ha sido replicado. • FALLO: La replicación falló con un error permanente. Un usuario debe resolver el error.
Destino	RÉPLICA : El objeto fue replicado desde la cuadrícula de origen.

- Utilice la API privada de administración de cuadrícula, como se describe.

Pasos

1. En la sección **cross-grid-replication-advanced** de la documentación de la API privada, seleccione el siguiente punto final:

```
GET /private/cross-grid-replication-object-status/{id}
```

2. Seleccione **Probarlo**.
3. En la sección Parámetro, ingrese el ID de la versión que utilizó en el `cross-grid-replication-retry-failed` pedido.
4. Seleccione **Ejecutar**.
5. Confirme que el código de respuesta del servidor es **200**.
6. Revise el estado de la replicación, que será uno de los siguientes:
 - **PENDIENTE**: El objeto aún no ha sido replicado.
 - **COMPLETADO**: La replicación fue exitosa.
 - **FALLÓ**: La replicación falló con un error permanente. Un usuario debe resolver el error.

Gestionar la seguridad

Gestionar la seguridad

Puede configurar varias configuraciones de seguridad desde Grid Manager para ayudar a proteger su sistema StorageGRID .

Administrar el cifrado

StorageGRID ofrece varias opciones para cifrar datos. Debería [revisar los métodos de cifrado disponibles](#) para determinar cuáles cumplen con sus requisitos de protección de datos.

Administrar certificados

Puede [configurar y administrar los certificados del servidor](#) Se utiliza para conexiones HTTP o los certificados de cliente utilizados para autenticar la identidad de un cliente o usuario en el servidor.

Configurar servidores de administración de claves

Usando un ["servidor de gestión de claves"](#) Le permite proteger los datos de StorageGRID incluso si se elimina un dispositivo del centro de datos. Una vez cifrados los volúmenes del dispositivo, no podrá acceder a ningún dato del dispositivo a menos que el nodo pueda comunicarse con el KMS.



Para utilizar la administración de claves de cifrado, debe habilitar la configuración **Cifrado de nodo** para cada dispositivo durante la instalación, antes de agregar el dispositivo a la red.

Administrar la configuración del proxy

Si está utilizando servicios de la plataforma S3 o grupos de almacenamiento en la nube, puede configurar un ["servidor proxy de almacenamiento"](#) entre los nodos de almacenamiento y los puntos finales externos de S3. Si envía paquetes de AutoSupport mediante HTTPS o HTTP, puede configurar un ["servidor proxy de administración"](#) entre los nodos de administración y el soporte técnico.

Controlar cortafuegos

Para mejorar la seguridad de su sistema, puede controlar el acceso a los nodos de administración de StorageGRID abriendo o cerrando puertos específicos en el ["cortafuegos externo"](#). También puede controlar el acceso a la red de cada nodo configurando su ["cortafuegos interno"](#). Puede evitar el acceso a todos los puertos excepto aquellos necesarios para su implementación.

Revisar los métodos de cifrado de StorageGRID

StorageGRID ofrece varias opciones para cifrar datos. Debe revisar los métodos disponibles para determinar cuáles cumplen con 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 administración de claves (KMS) en Grid Manager	Tú "configurar un servidor de administración de claves" para el sitio StorageGRID y "Habilitar el cifrado de nodos para el dispositivo" . Luego, un nodo del dispositivo se conecta al KMS para solicitar una clave de cifrado de clave (KEK). Esta clave cifra y descifra la clave de cifrado de datos (DEK) en cada volumen.	Nodos de dispositivo que tienen Cifrado de nodo habilitado durante la instalación. Todos los datos del dispositivo están protegidos contra pérdida física o eliminación del centro de datos. Nota: La administración de claves de cifrado con un KMS solo es compatible con nodos de almacenamiento y dispositivos de servicios.

Opción de cifrado	Cómo funciona	Se aplica a
Página de cifrado de unidad en el instalador del dispositivo StorageGRID	Si el dispositivo contiene unidades que admiten cifrado de hardware, puede establecer una frase de contraseña para la unidad durante la instalación. Cuando se establece una frase de contraseña de unidad, es imposible que alguien recupere datos válidos de unidades que se han eliminado del sistema, a menos que conozca la frase de contraseña. Antes de comenzar la instalación, vaya a Configurar hardware > Cifrado de unidad para establecer una frase de contraseña de unidad que se aplique a todas las unidades con cifrado automático administradas por StorageGRID en un nodo.	Dispositivos que contienen unidades con cifrado automático. Todos los datos de las unidades seguras están protegidos contra pérdida física o eliminación del centro de datos. El cifrado de unidad no se aplica a las unidades administradas SANtricity. Si tiene un dispositivo de almacenamiento con unidades de autocifrado y controladores SANtricity , puede habilitar la seguridad de la unidad en SANtricity.
Impulse la seguridad en SANtricity System Manager	Si la función Seguridad de la unidad está habilitada para su dispositivo StorageGRID , puede usar " SANtricity System Manager " para crear y gestionar la clave de seguridad. La clave es necesaria para acceder a los datos de las unidades protegidas.	Dispositivos de almacenamiento que tienen unidades de cifrado de disco completo (FDE) o unidades de cifrado automático. Todos los datos de las unidades seguras están protegidos contra pérdida física o eliminación del centro de datos. No se puede utilizar con algunos dispositivos de almacenamiento ni con ningún dispositivo de servicio.
Cifrado de objetos almacenados	Habilitas el " Cifrado de objetos almacenados " opción en el Administrador de cuadrícula. Cuando esta opción está habilitada, todos los objetos nuevos que no estén cifrados en el nivel de depósito o en el nivel de objeto se cifran durante la ingesta.	Datos de objetos S3 recién ingeridos. Los objetos almacenados existentes no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados.

Opción de cifrado	Cómo funciona	Se aplica a
Cifrado de buckets S3	Emite una solicitud PutBucketEncryption para habilitar el cifrado para el depósito. Cualquier objeto nuevo que no esté cifrado a nivel de objeto se cifra durante la ingesta.	Solo datos de objetos S3 recién ingeridos. Se debe especificar el cifrado para el depósito. Los objetos de bucket existentes no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados. "Operaciones en buckets"
Cifrado del lado del servidor de objetos S3 (SSE)	Emite una solicitud S3 para almacenar un objeto e incluirlo x-amz-server-side-encryption encabezado de solicitud.	Solo datos de objetos S3 recién ingeridos. Se debe especificar el cifrado para el objeto. Los metadatos de los objetos y otros datos confidenciales no están cifrados. StorageGRID administra las claves. "Utilice cifrado del lado del servidor"
Cifrado del lado del servidor de objetos S3 con claves proporcionadas por el cliente (SSE-C)	Emite una solicitud S3 para almacenar un objeto e incluye 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 recién ingeridos. Se debe especificar el cifrado para el objeto. Los metadatos de los objetos y otros datos confidenciales no están cifrados. Las claves se administran fuera de StorageGRID. "Utilice cifrado del lado del servidor"

Opción de cifrado	Cómo funciona	Se aplica a
Cifrado de volumen externo o almacén de datos	Utilice un método de cifrado externo a StorageGRID para cifrar un volumen o almacén de datos completo, si su plataforma de implementación lo admite.	Todos los datos de objetos, metadatos y datos de configuración del sistema, asumiendo que cada volumen o almacén de datos está cifrado. 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.
Cifrado de objetos fuera de StorageGRID	Utilice un método de cifrado externo a StorageGRID para cifrar datos y metadatos de objetos antes de que se ingieran en StorageGRID.	Solo datos de objeto 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 del usuario: Protección de datos mediante cifrado del lado del cliente"

Utilice múltiples métodos de cifrado

Dependiendo de sus requisitos, puede utilizar más de un método de cifrado a la vez. Por ejemplo:

- Puede utilizar un KMS para proteger los nodos del dispositivo y también usar la función de seguridad de la unidad en SANtricity System Manager para "cifrar doblemente" los datos en las unidades con cifrado automático en los mismos dispositivos.
- Puede utilizar un KMS para proteger datos en los nodos del dispositivo y también utilizar la opción de cifrado de objetos almacenados para cifrar todos los objetos cuando se ingieren.

Si solo una pequeña parte de sus objetos requieren cifrado, considere controlar el cifrado a nivel de depósito o de objeto individual. Habilitar múltiples niveles de cifrado tiene un costo de rendimiento adicional.

Administrar certificados

Administrar certificados de seguridad

Los certificados de seguridad son pequeños archivos de datos que se utilizan para crear conexiones seguras y confiables entre los componentes de StorageGRID y entre los 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, autenticando la identidad de un servidor ante sus clientes y proporcionando una ruta de comunicación segura para los datos. Tanto el servidor como el cliente tienen una copia del certificado.
- Los **certificados de cliente** autentican la identidad de un cliente o usuario en el servidor, proporcionando una autenticación más segura que las contraseñas solas. Los certificados de cliente no cifran los datos.

Cuando un cliente se conecta al servidor mediante HTTPS, el servidor responde con el certificado del 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 punto final del equilibrador de carga) o como cliente para otras conexiones (como el servicio de replicación CloudMirror).

Certificado CA de Grid predeterminado

StorageGRID incluye una autoridad de certificación (CA) incorporada que genera un certificado CA de Grid interno durante la instalación del sistema. El certificado CA de Grid se utiliza, de forma predeterminada, para proteger el tráfico interno de StorageGRID. Una autoridad de certificación (CA) externa puede emitir certificados personalizados que cumplan totalmente con las políticas de seguridad de la información de su organización. Si bien puede utilizar el certificado CA de Grid para un entorno que no sea de producción, la mejor práctica para un entorno de producción es utilizar certificados personalizados firmados por una autoridad de certificación externa. También se admiten conexiones no seguras sin certificado, pero no se recomiendan.

- Los certificados CA personalizados no eliminan los certificados internos; sin embargo, los certificados personalizados deben ser los especificados para verificar las conexiones del servidor.
- Todos los certificados personalizados deben cumplir con los ["Pautas de fortalecimiento del sistema para certificados de servidor"](#).
- StorageGRID admite la agrupación de certificados de una CA en un solo archivo (conocido como paquete de certificados de CA).



StorageGRID también incluye certificados CA del sistema operativo que son los mismos en todas las redes. En entornos de producción, asegúrese de especificar un certificado personalizado firmado por una autoridad de certificación externa en lugar del certificado CA del sistema operativo.

Las variantes de los tipos de certificado de servidor y cliente se implementan de varias maneras. Debe tener todos los certificados necesarios para su configuración específica de StorageGRID listos antes de configurar el sistema.

Certificados de seguridad de acceso

Puede acceder a información sobre todos los certificados StorageGRID en una sola ubicación, junto con enlaces al flujo de trabajo de configuración para cada certificado.

Pasos

1. Desde Grid Manager, seleccione **CONFIGURACIÓN > Seguridad > Certificados**.

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

Global

Grid CA

Client

Load balancer endpoints

Tenants

Other

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type ⓘ	Expiration date ⓘ ⌵
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Seleccione una pestaña en la página Certificados para obtener información sobre cada categoría de certificado y acceder a la configuración del certificado. Puedes acceder a una pestaña si tienes la "[permiso apropiado](#)".

- **Global:** protege el acceso a StorageGRID desde navegadores web y clientes API externos.
- **Grid CA:** protege el tráfico interno de StorageGRID .
- **Cliente:** protege las conexiones entre clientes externos y la base de datos StorageGRID Prometheus.
- **Puntos finales del balanceador de carga:** protege las conexiones entre los clientes S3 y el balanceador de carga StorageGRID .
- **Inquilinos:** protege las conexiones a servidores de federación de identidad o desde puntos finales de servicio de la plataforma a recursos de almacenamiento S3.
- **Otro:** Protege las conexiones StorageGRID que requieren certificados específicos.

A continuación se describe cada pestaña con enlaces a detalles adicionales del certificado.

Global

Los certificados globales protegen el acceso a StorageGRID desde navegadores web y clientes API S3 externos. La autoridad de certificación StorageGRID genera inicialmente dos certificados globales durante la instalación. La mejor práctica para un entorno de producción es utilizar certificados personalizados firmados por una autoridad de certificación externa.

- [Certificado de interfaz de gestión](#): Asegura las conexiones del navegador web del cliente a las interfaces de administración de StorageGRID .
- [Certificado API S3](#): Asegura las conexiones de API de cliente a los nodos de almacenamiento, nodos de administración y nodos de puerta de enlace, que las aplicaciones de cliente S3 utilizan para cargar y descargar datos de objetos.

La información sobre los certificados globales que están instalados incluye:

- **Nombre**: Nombre del certificado con enlace para administrar el certificado.
- **Descripción**
- **Tipo**: Personalizado o predeterminado. + Siempre debe utilizar un certificado personalizado para mejorar la seguridad de la red.
- **Fecha de vencimiento**: si se utiliza el certificado predeterminado, no se muestra ninguna fecha de vencimiento.

Puede:

- Reemplace los certificados predeterminados con certificados personalizados firmados por una autoridad de certificación externa para mejorar la seguridad de la red:
 - ["Reemplazar el certificado de interfaz de administración generado por StorageGRID predeterminado"](#) Se utiliza para conexiones de Grid Manager y Tenant Manager.
 - ["Reemplazar el certificado de API S3"](#) Se utiliza para conexiones de nodo de almacenamiento y punto final del equilibrador de carga (opcional).
- ["Restaurar el certificado de interfaz de administración predeterminado"](#) .
- ["Restaurar el certificado API S3 predeterminado"](#) .
- ["Utilice un script para generar un nuevo certificado de interfaz de administración autofirmado"](#) .
- Copiar o descargar el ["certificado de interfaz de gestión"](#) o ["Certificado API S3"](#) .

Red CA

El [Certificado de CA de Grid](#) , generado por la autoridad de certificación de StorageGRID durante la instalación de StorageGRID , protege todo el tráfico interno de StorageGRID .

La información del certificado incluye la fecha de vencimiento del certificado y el contenido del certificado.

Puede ["copiar o descargar el certificado de Grid CA"](#) , pero no puedes cambiarlo.

Cliente

[Certificados de cliente](#) , generado por una autoridad de certificación externa, protege las conexiones entre las herramientas de monitoreo externas y la base de datos StorageGRID Prometheus.

La tabla de certificados tiene una fila para cada certificado de cliente configurado e indica si el certificado se puede usar para acceder a la base de datos de Prometheus, junto con la fecha de

vencimiento del certificado.

Puede:

- ["Cargar o generar un nuevo certificado de cliente."](#)
- Seleccione un nombre de certificado para mostrar los detalles del certificado donde podrá:
 - ["Cambiar el nombre del certificado del cliente."](#)
 - ["Establecer el permiso de acceso de Prometheus."](#)
 - ["Cargar y reemplazar el certificado del cliente."](#)
 - ["Copie o descargue el certificado del cliente."](#)
 - ["Eliminar el certificado del cliente."](#)
- Seleccione **Acciones** para acceder rápidamente ["editar"](#) , ["adjuntar"](#) , o ["eliminar"](#) un certificado de cliente. Puede seleccionar hasta 10 certificados de cliente y eliminarlos a la vez usando **Acciones > Eliminar**.

Puntos finales del balanceador de carga

[Certificados de punto final del balanceador de carga](#) Asegure las conexiones entre los clientes S3 y el servicio StorageGRID Load Balancer en los nodos de puerta de enlace y los nodos de administración.

La tabla de puntos finales del equilibrador de carga tiene una fila para cada punto final del equilibrador de carga configurado e indica si se utiliza el certificado de API S3 global o un certificado de punto final del equilibrador de carga personalizado para el punto final. También se muestra la fecha de vencimiento de cada certificado.



Los cambios en un certificado de punto final pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Puede:

- ["Ver un punto final del balanceador de carga"](#), incluidos los detalles de su certificado.
- ["Especifique un certificado de punto final del equilibrador de carga para FabricPool."](#)
- ["Utilice el certificado API global de S3"](#) en lugar de generar un nuevo certificado de punto final del equilibrador de carga.

Inquilinos

Los inquilinos pueden utilizar [certificados de servidor de federación de identidad](#) o [certificados de punto final del servicio de plataforma](#) para proteger sus conexiones con StorageGRID.

La tabla de inquilinos tiene una fila para cada inquilino e indica si cada inquilino tiene permiso para usar su propia fuente de identidad o servicios de plataforma.

Puede:

- ["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 identidad del inquilino"](#)
- ["Seleccione el nombre de un inquilino para ver los detalles de los servicios de la plataforma de inquilinos"](#)

- "Especifique un certificado de punto final del servicio de plataforma durante la creación del punto final"

Otro

StorageGRID utiliza otros certificados de seguridad para fines específicos. Estos certificados se enumeran por su nombre funcional. Otros certificados de seguridad incluyen:

- [Certificados de grupo de almacenamiento en la nube](#)
- [Certificados de notificación de alertas por correo electrónico](#)
- [Certificados de servidor syslog externo](#)
- [Certificados de conexión de la federación de red](#)
- [Certificados de federación de identidad](#)
- [Certificados de servidor de administración de claves \(KMS\)](#)
- [Certificados de inicio de sesión único](#)

La información indica el tipo de certificado que utiliza una función y las fechas de vencimiento de sus certificados de servidor y cliente, según corresponda. Al seleccionar un nombre de función, se abre una pestaña del navegador donde puede ver y editar los detalles del certificado.



Solo puede ver y acceder a la información de otros certificados si tiene la ["permiso apropiado"](#).

Puede:

- ["Especifique un certificado de grupo de almacenamiento en la nube para S3, C2S S3 o Azure"](#)
- ["Especificar un certificado para notificaciones de alerta por correo electrónico"](#)
- ["Utilice un certificado para un servidor syslog externo"](#)
- ["Rotar certificados de conexión de federación de red"](#)
- ["Ver y editar un certificado de federación de identidad"](#)
- ["Cargar certificados de cliente y servidor del servidor de administración de claves \(KMS\)"](#)
- ["Especificar manualmente un certificado SSO para una relación de confianza de usuario autenticado"](#)

Detalles del certificado de seguridad

A continuación se describe cada tipo de certificado de seguridad, con enlaces a las instrucciones de implementación.

Certificado de interfaz de gestión

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los navegadores web del cliente y la interfaz de administración de StorageGRID , lo que permite a los usuarios acceder a Grid Manager y Tenant Manager sin advertencias de seguridad. Este certificado también autentica las conexiones de la API de administración de red y la API de administración de inquilinos. Puede utilizar el certificado predeterminado creado durante la instalación o cargar un certificado personalizado.	CONFIGURACIÓN > Seguridad > Certificados , seleccione la pestaña Global y luego seleccione Certificado de interfaz de administración	"Configurar certificados de interfaz de administración"

Certificado API S3

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica conexiones seguras de cliente S3 a un nodo de almacenamiento y a puntos finales del balanceador de carga (opcional).	CONFIGURACIÓN > Seguridad > Certificados , seleccione la pestaña Global y luego seleccione Certificado API S3	"Configurar certificados de API S3"

Certificado de CA de Grid

Ver el [Descripción del certificado de CA de Grid predeterminado](#) .

Certificado de cliente administrador

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Cliente	Se instala en cada cliente, lo que permite que StorageGRID autentique el acceso de clientes externos. • Permite que los clientes externos autorizados accedan a la base de datos StorageGRID Prometheus. • Permite la monitorización segura de StorageGRID mediante herramientas externas.	CONFIGURACIÓN > Seguridad > Certificados y luego seleccione la pestaña Cliente	"Configurar certificados de cliente"

Certificado de punto final del balanceador de carga

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los clientes S3 y el servicio StorageGRID Load Balancer en los nodos de puerta de enlace y los nodos de administración. Puede cargar o generar un certificado de equilibrador de carga cuando configura un punto final de equilibrador de carga. Las aplicaciones cliente utilizan el certificado del equilibrador de carga cuando se conectan a StorageGRID para guardar y recuperar datos de objetos. También puedes utilizar una versión personalizada del global Certificado API S3 Certificado para autenticar conexiones al servicio Load Balancer. Si el certificado global se utiliza para autenticar las conexiones del balanceador de carga, no es necesario cargar ni generar un certificado separado para cada punto final del balanceador de carga. Nota: El certificado utilizado para la autenticación del equilibrador de carga es el certificado más usado durante el funcionamiento normal de StorageGRID .	CONFIGURACIÓN > Red > Puntos finales del balanceador de carga	• "Configurar los puntos finales del balanceador de carga" • "Crear un punto final de balanceador de carga para FabricPool"

Certificado de punto final del grupo de almacenamiento en la nube

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión desde un grupo de almacenamiento en la nube StorageGRID a una ubicación de almacenamiento externa, como S3 Glacier o Microsoft Azure Blob Storage. Se requiere un certificado diferente para cada tipo de proveedor de nube.	ILM > Grupos de almacenamiento	"Crear un grupo de almacenamiento en la nube"

Certificado de notificación de alerta 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 StorageGRID que se utiliza para notificaciones de alerta. • Si las comunicaciones con el servidor SMTP requieren seguridad de la capa de transporte (TLS), debe especificar el certificado CA del servidor de correo electrónico. • Especifique un certificado de cliente solo si el servidor de correo electrónico SMTP requiere certificados de cliente para la autenticación.	ALERTAS > Configuración de correo electrónico	"Configurar notificaciones por correo electrónico para alertas"

Certificado de servidor syslog externo

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión TLS o RELP/TLS entre un servidor syslog externo que registra eventos en StorageGRID. Nota: No se requiere un certificado de servidor syslog externo para conexiones TCP, RELP/TCP y UDP a un servidor syslog externo.	CONFIGURACIÓN > Monitoreo > Servidor de auditoría y syslog	"Utilice un servidor syslog externo"

Certificado de conexión de federación de red

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autenticar y cifrar la información enviada entre el sistema StorageGRID actual y otra red en una conexión de federación de redes.	CONFIGURACIÓN > Sistema > Federación de red	• "Crear conexiones de federación de red" • "Rotar certificados de conexión"

Certificado de federación de identidad

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre StorageGRID y un proveedor de identidad externo, como Active Directory, OpenLDAP u Oracle Directory Server. Se utiliza para la federación de identidad, que permite que los grupos de administradores y los usuarios sean gestionados por un sistema externo.	CONFIGURACIÓN > Control de acceso > Federación de identidades	"Utilizar la federación de identidades"

Certificado de servidor de administración de claves (KMS)

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autentica la conexión entre StorageGRID y un servidor de administración de claves externo (KMS), que proporciona claves de cifrado a los nodos del dispositivo StorageGRID .	CONFIGURACIÓN > Seguridad > Servidor de gestión de claves	"Agregar servidor de administración de claves (KMS)"

Certificado de punto final de servicios de plataforma

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión del servicio de la plataforma StorageGRID a un recurso de almacenamiento S3.	Administrador de inquilinos > ALMACENAMIENTO (S3) > Puntos finales de servicios de plataforma	"Crear punto final de servicios de plataforma" "Editar el punto final de los servicios de la plataforma"

Certificado de inicio de sesión único (SSO)

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los servicios de federación de identidad, como los Servicios de federación de Active Directory (AD FS) y StorageGRID , que se utilizan para solicitudes de inicio de sesión único (SSO).	CONFIGURACIÓN > Control de acceso > Inicio de sesión único	"Configurar el inicio de sesión único"

Ejemplos de certificados

Ejemplo 1: Servicio de balanceo de carga

En este ejemplo, StorageGRID actúa como servidor.

1. Configura un punto final del equilibrador de carga y carga o genera un certificado de servidor en StorageGRID.
2. Configura una conexión de cliente S3 al punto final del equilibrador de carga y carga el mismo certificado en el cliente.
3. Cuando el cliente desea guardar o recuperar datos, se conecta al punto final del balanceador de carga

mediante HTTPS.

4. StorageGRID responde con el certificado del servidor, que contiene una clave pública, y con 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 objetos a StorageGRID.

Ejemplo 2: Servidor de administración de claves externo (KMS)

En este ejemplo, StorageGRID actúa como cliente.

1. Al utilizar el software de servidor de administración de claves externo, configura StorageGRID como un cliente KMS y obtiene un certificado de servidor firmado por una CA, un certificado de cliente público y la clave privada para el certificado de cliente.
2. Con Grid Manager, configura un servidor KMS y carga los certificados del servidor y del cliente y la clave privada del 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 utilizando la conexión validada.

Tipos de certificados de servidor admitidos

El sistema StorageGRID admite certificados personalizados cifrados con RSA o ECDSA (algoritmo de firma digital de curva elíptica).



El tipo de cifrado para la política de seguridad debe coincidir con el tipo de certificado del servidor. Por ejemplo, los cifrados RSA requieren certificados RSA y los cifrados ECDSA requieren certificados ECDSA. Ver ["Administrar certificados de seguridad"](#) . Si configura una política de seguridad personalizada que no es compatible con el certificado del servidor, puede ["volver temporalmente a la política de seguridad predeterminada"](#) .

Para obtener más información sobre cómo StorageGRID protege las conexiones de los clientes, consulte ["Seguridad para clientes S3"](#) .

Configurar certificados de interfaz de administración

Puede reemplazar el certificado de interfaz de administración predeterminado con un único certificado personalizado que permita a los usuarios acceder al Administrador de Grid y al Administrador de inquilinos sin encontrar advertencias de seguridad. También puede volver al certificado de interfaz de administración predeterminado o generar uno nuevo.

Acerca de esta tarea

De forma predeterminada, a cada nodo de administración se le emite un certificado firmado por la CA de la red. Estos certificados firmados por CA se pueden reemplazar por un único certificado de interfaz de administración personalizada común y su clave privada correspondiente.

Debido a que se utiliza un único certificado de interfaz de administración personalizado para todos los nodos

de administración, debe especificar el certificado como comodín o como certificado multidominio si los clientes necesitan verificar el nombre de host al conectarse al Administrador de red y al Administrador de inquilinos. Defina el certificado personalizado de modo que coincida con todos los nodos de administración en la cuadrícula.

Debe completar la configuración en el servidor y, dependiendo de la autoridad de certificación raíz (CA) que esté utilizando, los usuarios también podrían necesitar instalar el certificado de CA de Grid en el navegador web que usarán para acceder a Grid Manager y Tenant Manager.



Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, se activa la alerta **Expiración del certificado de servidor para la interfaz de administración** cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **CONFIGURACIÓN > Seguridad > Certificados** y mirando la fecha de vencimiento del certificado de la interfaz de administración en la pestaña Global.



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

- Su certificado de interfaz de administración personalizada caduca.
- Tú [Revertir de un certificado de interfaz de administración personalizado al certificado de servidor predeterminado](#) .

Agregar un certificado de interfaz de administración personalizado

Para agregar un certificado de interfaz de administración personalizado, puede proporcionar su propio certificado o generar uno utilizando Grid Manager.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados**.
2. En la pestaña **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione **Usar certificado personalizado**.
4. Subir o generar el certificado.

Subir certificado

Cargue los archivos de certificado de servidor necesarios.

a. Seleccione **Subir certificado**.

b. Cargue los archivos de certificado de servidor necesarios:

- **Certificado de servidor:** el archivo de certificado de servidor personalizado (codificado en PEM).
- **Clave privada del certificado:** El archivo de clave privada del certificado del servidor personalizado(`.key`).



Las claves privadas EC deben tener 224 bits o más. Las claves privadas RSA deben tener 2048 bits o más.

- **Paquete CA:** un único archivo opcional que contiene los certificados de cada autoridad de certificación (CA) emisora intermedia. El archivo debe contener cada uno de los archivos de certificado CA codificados en PEM, concatenados en el orden de la cadena de certificados.

c. Expande **Detalles del certificado** para ver los metadatos de cada certificado que hayas cargado. Si cargó un paquete de CA opcional, cada certificado se muestra 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 del 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 CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

d. Seleccione **Guardar**. + El certificado de interfaz de administración personalizada se utiliza para todas las nuevas conexiones posteriores a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

Generar certificado

Generar los archivos de certificado del servidor.



La mejor práctica para un entorno de producción es utilizar un certificado de interfaz de administración personalizado firmado por una autoridad de certificación externa.

a. Seleccione **Generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o más nombres de dominio completos para incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
Propiedad intelectual	Una o más direcciones IP para incluir en el certificado.

Campo	Descripción
Asunto (opcional)	Sujeto X.509 o nombre distinguido (DN) del propietario del certificado. Si no se ingresa ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o dirección IP como nombre común del sujeto (CN).
Días válidos	Número de días después de su creación que expira el certificado.
Agregar extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y uso de clave extendido se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. Nota: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.

c. Seleccione **Generar**.

d. Seleccione **Detalles del certificado** para ver los metadatos del certificado generado.

- Seleccione **Descargar certificado** para guardar el archivo del certificado.

Especifique el nombre del archivo del 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 y pegarlo en otro lugar.

e. Seleccione **Guardar**. + El certificado de interfaz de administración personalizada se utiliza para todas las nuevas conexiones posteriores a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

5. Actualice la página para asegurarse de que el navegador web esté actualizado.



Después de cargar o generar un nuevo certificado, espere hasta un día para que desaparezcan las alertas de vencimiento del certificado relacionadas.

6. Después de agregar un certificado de interfaz de administración personalizado, la página Certificado de interfaz de administración muestra información detallada de los certificados que están en uso. + Puede descargar o copiar el certificado PEM según sea necesario.

Restaurar el certificado de interfaz de administración predeterminado

Puede volver a utilizar el certificado de interfaz de administración predeterminado para las conexiones de Grid Manager y Tenant Manager.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados**.
2. En la pestaña **Global**, seleccione **Certificado de interfaz de administración**.
3. Seleccione **Usar certificado predeterminado**.

Cuando restaura el certificado de interfaz de administración predeterminado, los archivos de certificado de servidor personalizados que configuró se eliminan y no se pueden recuperar del sistema. El certificado de interfaz de administración predeterminado se utiliza para todas las conexiones de nuevos clientes posteriores.

4. Actualice la página para asegurarse de que el navegador web esté actualizado.

Utilice un script para generar un nuevo certificado de interfaz de administración autofirmado

Si se requiere una validación estricta del nombre de host, puede utilizar un script para generar el certificado de interfaz de administración.

Antes de empezar

- Tienes "[permisos de acceso específicos](#)".
- Tú tienes el `Passwords.txt` archivo.

Acerca de esta tarea

La mejor práctica para un entorno de producción es utilizar un certificado firmado por una autoridad de certificación externa.

Pasos

1. Obtenga el nombre de dominio completo (FQDN) de cada nodo de administración.
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 el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

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

3. Configure StorageGRID con un nuevo certificado autofirmado.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- Para `--domains`, utilice caracteres comodín para representar los nombres de dominio completos de todos los nodos de administración. Por ejemplo, `*.ui.storagegrid.example.com` utiliza el comodín `*` para representar `admin1.ui.storagegrid.example.com` y `admin2.ui.storagegrid.example.com`.
- Colocar `--type` a `management` para configurar el certificado de la interfaz de administración, que utilizan Grid Manager y Tenant Manager.
- De forma predeterminada, los certificados generados son válidos por un año (365 días) y deben volver a crearse antes de que caduquen. Puedes 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 administración esté sincronizado con la misma fuente de tiempo que StorageGRID; de lo contrario, el cliente podría rechazar el certificado.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 720
```

La salida resultante contiene el certificado público que necesita su cliente de API de administración.

4. Seleccione y copie el certificado.

Incluya las etiquetas BEGIN y END en su selección.

5. Cierre la sesión del shell de comandos. `$ exit`

6. Confirme que se configuró el certificado:

- Acceda al Administrador de cuadrícula.
- Seleccione **CONFIGURACIÓN > Seguridad > Certificados**
- En la pestaña **Global**, seleccione **Certificado de interfaz de administración**.

7. Configure su cliente de administración para utilizar el certificado público que copió. Incluya las etiquetas BEGIN y END.

Descargue o copie el certificado de interfaz de administración

Puede guardar o copiar el contenido del certificado de la interfaz de administración para usarlo en otro lugar.

Pasos

- Seleccione **CONFIGURACIÓN > Seguridad > Certificados**.
- En la pestaña **Global**, seleccione **Certificado de interfaz de administración**.
- Seleccione la pestaña **Servidor** o **Paquete CA** y luego descargue o copie el certificado.

Descargar archivo de certificado o paquete de CA

Descargar el certificado o paquete de CA .pem archivo. Si está utilizando un paquete 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 paquete de CA, todos los certificados en las pestañas secundarias del paquete de CA se descargan como un solo archivo.

- b. Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión .pem .

Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado o paquete de CA PEM

Copie el texto del certificado para pegarlo en otro lugar. Si está utilizando un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

- a. Seleccione **Copiar certificado PEM** o **Copiar paquete CA PEM**.

Si está copiando un paquete de CA, todos los certificados en las pestañas secundarias del paquete de CA se copian juntos.

- 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`

Configurar certificados de API S3

Puede reemplazar o restaurar el certificado de servidor que se utiliza para las conexiones de cliente S3 a los nodos de almacenamiento o a los puntos finales del equilibrador de carga. El certificado de servidor personalizado de reemplazo es específico para su organización.



Se han eliminado los detalles rápidos de esta versión del sitio de documentación. Ver ["StorageGRID 11.8: Configurar certificados de API de S3 y Swift"](#) .

Acerca de esta tarea

De forma predeterminada, a cada nodo de almacenamiento se le emite un certificado de servidor X.509 firmado por la CA de la red. Estos certificados firmados por CA se pueden reemplazar por un único certificado de servidor personalizado común y su clave privada correspondiente.

Se utiliza un único certificado de servidor personalizado para todos los nodos de almacenamiento, por lo que debe especificar el certificado como comodín o un certificado multidominio si los clientes necesitan verificar el nombre de host al conectarse al punto final de almacenamiento. Defina el certificado personalizado de modo que coincida con todos los nodos de almacenamiento de la red.

Después de completar la configuración en el servidor, es posible que también necesite instalar el certificado

CA de Grid en el cliente API S3 que usará para acceder al sistema, dependiendo de la autoridad de certificación raíz (CA) que esté utilizando.



Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, la alerta **Expiración del certificado de servidor global para la API S3** se activa cuando el certificado del servidor raíz está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **CONFIGURACIÓN > Seguridad > Certificados** y mirando la fecha de vencimiento del certificado de API S3 en la pestaña Global.

Puede cargar o generar un certificado API S3 personalizado.

Agregar un certificado API S3 personalizado

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados**.
2. En la pestaña **Global**, seleccione **Certificado API S3**.
3. Seleccione **Usar certificado personalizado**.
4. Subir o generar el certificado.

Subir certificado

Cargue los archivos de certificado de servidor necesarios.

a. Seleccione **Subir certificado**.

b. Cargue los archivos de certificado de servidor necesarios:

- **Certificado de servidor:** el archivo de certificado de servidor personalizado (codificado en PEM).
- **Clave privada del certificado:** El archivo de clave privada del certificado del servidor personalizado(`.key`).



Las claves privadas EC deben tener 224 bits o más. Las claves privadas RSA deben tener 2048 bits o más.

- **Paquete CA:** un único archivo opcional que contiene los certificados de cada autoridad de certificación emisora intermedia. El archivo debe contener cada uno de los archivos de certificado CA codificados en 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 S3 personalizado que se cargó. Si cargó un paquete de CA opcional, cada certificado se muestra 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 del 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 CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

d. Seleccione **Guardar**.

El certificado de servidor personalizado se utiliza para nuevas conexiones de cliente S3 posteriores.

Generar certificado

Generar los archivos de certificado del servidor.

a. Seleccione **Generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o más nombres de dominio completos para incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
Propiedad intelectual	Una o más direcciones IP para incluir en el certificado.

Campo	Descripción
Asunto (opcional)	Sujeto X.509 o nombre distinguido (DN) del propietario del certificado. Si no se ingresa ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o dirección IP como nombre común del sujeto (CN).
Días válidos	Número de días después de su creación que expira el certificado.
Agregar extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y uso de clave extendido se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. Nota: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.

c. Seleccione **Generar**.

d. Seleccione **Detalles del certificado** para mostrar los metadatos y PEM del certificado API S3 personalizado que se generó.

- Seleccione **Descargar certificado** para guardar el archivo del certificado.

Especifique el nombre del archivo del 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 y pegarlo en otro lugar.

e. Seleccione **Guardar**.

El certificado de servidor personalizado se utiliza para nuevas conexiones de cliente S3 posteriores.

5. Seleccione una pestaña para mostrar los metadatos del certificado de servidor StorageGRID predeterminado, un certificado firmado por CA que se cargó o un certificado personalizado que se generó.



Después de cargar o generar un nuevo certificado, espere hasta un día para que desaparezcan las alertas de vencimiento del certificado relacionadas.

6. Actualice la página para asegurarse de que el navegador web esté actualizado.

7. Después de agregar un certificado API S3 personalizado, la página del certificado API S3 muestra información detallada del certificado API S3 personalizado que está en uso. + Puede descargar o copiar el certificado PEM según sea necesario.

Restaurar el certificado API S3 predeterminado

Puede volver a utilizar el certificado API S3 predeterminado para las conexiones de cliente S3 a los nodos de almacenamiento. Sin embargo, no puedes usar el certificado API S3 predeterminado para un punto final del balanceador de carga.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados**.
2. En la pestaña **Global**, seleccione **Certificado API S3**.
3. Seleccione **Usar certificado predeterminado**.

Cuando restaura la versión predeterminada del certificado API S3 global, los archivos de certificado de servidor personalizados que configuró se eliminan y no se pueden recuperar del sistema. El certificado API S3 predeterminado se utilizará para las nuevas conexiones de clientes S3 posteriores a los nodos de almacenamiento.

4. Seleccione **Aceptar** para confirmar la advertencia y restaurar el certificado API S3 predeterminado.

Si tiene permiso de acceso de root y se utilizó el certificado API S3 personalizado para las conexiones de puntos finales del balanceador de carga, se muestra una lista de puntos finales del balanceador de carga que ya no serán accesibles mediante el certificado API S3 predeterminado. Ir a ["Configurar los puntos finales del balanceador de carga"](#) para editar o eliminar los puntos finales afectados.

5. Actualice la página para asegurarse de que el navegador web esté actualizado.

Descargue o copie el certificado de API S3

Puede guardar o copiar el contenido del certificado API S3 para usarlo en otro lugar.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados**.
2. En la pestaña **Global**, seleccione **Certificado API S3**.
3. Seleccione la pestaña **Servidor** o **Paquete CA** y luego descargue o copie el certificado.

Descargar archivo de certificado o paquete de CA

Descargar el certificado o paquete de CA .pem archivo. Si está utilizando un paquete 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 paquete de CA, todos los certificados en las pestañas secundarias del paquete de CA se descargan como un solo archivo.

- b. Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión .pem .

Por ejemplo: storagegrid_certificate.pem

Copiar certificado o paquete de CA PEM

Copie el texto del certificado para pegarlo en otro lugar. Si está utilizando un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

- a. Seleccione **Copiar certificado PEM** o **Copiar paquete CA PEM**.

Si está copiando un paquete de CA, todos los certificados en las pestañas secundarias del paquete de CA se copian juntos.

- 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

- ["Utilice la API REST de S3"](#)
- ["Configurar nombres de dominio de puntos finales S3"](#)

Copiar el certificado de CA de Grid

StorageGRID utiliza una autoridad de certificación (CA) interna para proteger el tráfico interno. Este certificado no cambia si carga sus propios certificados.

Antes de empezar

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

Acerca de esta tarea

Si se ha configurado un certificado de servidor personalizado, las aplicaciones cliente deben verificar el servidor utilizando el certificado de servidor personalizado. No deben copiar el certificado CA del sistema StorageGRID .

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Grid CA**.

2. En la sección **Certificado PEM**, descargue o copie el certificado.

Descargar archivo de certificado

Descargar el certificado .pem archivo.

- Seleccione **Descargar certificado**.
- Especifique el nombre del archivo del certificado y la ubicación de descarga. Guarde el archivo con la extensión .pem .

Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado PEM

Copie el texto del certificado para pegarlo en otro lugar.

- Seleccione **Copiar certificado PEM**.
- Pegue el certificado copiado en un editor de texto.
- Guarde el archivo de texto con la extensión .pem .

Por ejemplo: `storagegrid_certificate.pem`

Configurar certificados StorageGRID para FabricPool

Para los clientes S3 que realizan una validación estricta del nombre de host y no admiten la desactivación de la validación estricta del nombre de host, como los clientes ONTAP que usan FabricPool, puede generar o cargar un certificado de servidor cuando configura el punto final del equilibrador de carga.

Antes de empezar

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

Acerca de esta tarea

Cuando crea un punto final de balanceador de carga, puede generar un certificado de servidor autofirmado o cargar un certificado firmado por una autoridad de certificación (CA) conocida. En entornos de producción, debe utilizar un certificado firmado por una CA conocida. Los certificados firmados por una CA se pueden rotar sin interrupciones. También son más seguros porque ofrecen una mejor protección contra ataques del tipo "man-in-the-middle".

Los siguientes pasos proporcionan pautas generales para los clientes S3 que utilizan FabricPool. Para obtener información y procedimientos más detallados, consulte ["Configurar StorageGRID para FabricPool"](#) .

Pasos

- Opcionalmente, configure un grupo de alta disponibilidad (HA) para que lo utilice FabricPool .
- Cree un punto final de balanceador de carga S3 para que lo utilice FabricPool .

Cuando crea un punto final de balanceador de carga HTTPS, se le solicita que cargue su certificado de servidor, la clave privada del certificado y el paquete de CA opcional.

3. Adjunte StorageGRID como un nivel de nube en ONTAP.

Especifique el puerto del punto final del equilibrador de carga y el nombre de dominio completo utilizado en el certificado de CA que cargó. Luego, proporcione el certificado CA.



Si una CA intermedia emitió el certificado StorageGRID, debe proporcionar el certificado de CA intermedia. Si el certificado StorageGRID fue emitido directamente por la CA raíz, debe proporcionar el certificado de la CA raíz.

Configurar certificados de cliente

Los certificados de cliente permiten que los clientes externos autorizados accedan a la base de datos Prometheus de StorageGRID, lo que proporciona una forma segura para que las herramientas externas monitoreen StorageGRID.

Si necesita acceder a StorageGRID mediante una herramienta de monitoreo externa, debe cargar o generar un certificado de cliente utilizando Grid Manager y copiar la información del certificado a la herramienta externa.

Ver "[Administrar certificados de seguridad](#)" y "[Configurar certificados de servidor personalizados](#)".



Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, se activa la alerta **Expiración de certificados de cliente configurados en la página Certificados** cuando este certificado de servidor está a punto de expirar. Según sea necesario, puede ver cuándo vence el certificado actual seleccionando **CONFIGURACIÓN > Seguridad > Certificados** y mirando la fecha de vencimiento del certificado del cliente en la pestaña Cliente.



Si está utilizando un servidor de administración de claves (KMS) para proteger los datos en nodos de dispositivos especialmente configurados, consulte la información específica sobre "[Cargar un certificado de cliente KMS](#)".

Antes de empezar

- Tienes permiso de acceso root.
- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Para configurar un certificado de cliente:
 - Tienes la dirección IP o el nombre de dominio del nodo de administración.
 - Si ha configurado el certificado de interfaz de administración de StorageGRID, tiene la CA, el certificado de cliente y la clave privada que se utilizan para configurar el certificado de interfaz de administración.
 - Para cargar su propio certificado, la clave privada del certificado está disponible en su computadora local.
 - La clave privada debe haber sido guardada o registrada en el momento de su creación. Si no tiene la clave privada original, debe crear una nueva.
- Para editar un certificado de cliente:
 - Tienes la dirección IP o el nombre de dominio del nodo de administración.
 - Para cargar su propio certificado o un certificado nuevo, la clave privada, el certificado del cliente y la CA (si se utiliza) están disponibles en su computadora local.

Agregar certificados de cliente

Para agregar el certificado de cliente, utilice uno de estos procedimientos:

- [Certificado de interfaz de administración ya configurado](#)
- [Certificado de cliente emitido por CA](#)
- [Certificado generado desde Grid Manager](#)

Certificado de interfaz de administración ya configurado

Utilice este procedimiento para agregar un certificado de cliente si ya hay configurado un certificado de interfaz de administración mediante una CA proporcionada por el cliente, un certificado de cliente y una clave privada.

Pasos

1. En el Administrador de red, seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado.
4. Para acceder a las métricas de Prometheus usando su herramienta de monitoreo externa, seleccione **Permitir Prometheus**.
5. Seleccione **Continuar**.
6. Para el paso **Adjuntar certificados**, cargue el certificado de la interfaz de administración.
 - a. Seleccione **Subir certificado**.
 - b. Seleccione **Explorar** y seleccione el archivo de certificado de la interfaz de administración(.pem).
 - Seleccione **Detalles del certificado del cliente** para mostrar los metadatos del certificado y el PEM del certificado.
 - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
 - c. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

El nuevo certificado aparece en la pestaña Cliente.

7. [Configurar una herramienta de monitorización externa](#), como Grafana.

Certificado de cliente emitido por CA

Utilice este procedimiento para agregar un certificado de cliente administrador si no se configuró un certificado de interfaz de administración y planea agregar un certificado de cliente para Prometheus que utiliza un certificado de cliente emitido por una CA y una clave privada.

Pasos

1. Realice los pasos para "[configurar un certificado de interfaz de administración](#)".
2. En el Administrador de red, seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
3. Seleccione **Agregar**.
4. Introduzca un nombre de certificado.

5. Para acceder a las métricas de Prometheus usando su herramienta de monitoreo externa, seleccione **Permitir Prometheus**.
6. Seleccione **Continuar**.
7. Para el paso **Adjuntar certificados**, cargue el certificado del cliente, la clave privada y los archivos del paquete de CA:
 - a. Seleccione **Subir certificado**.
 - b. Seleccione **Explorar** y seleccione el certificado del cliente, la clave privada y los archivos del paquete de CA(.pem).
 - Seleccione **Detalles del certificado del cliente** para mostrar los metadatos del certificado y el PEM del certificado.
 - Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
 - c. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

Los nuevos certificados aparecen en la pestaña Cliente.

8. [Configurar una herramienta de monitorización externa](#), como Grafana.

Certificado generado desde Grid Manager

Utilice este procedimiento para agregar un certificado de cliente administrador si no se configuró un certificado de interfaz de administración y planea agregar un certificado de cliente para Prometheus que use la función de generar certificado en Grid Manager.

Pasos

1. En el Administrador de red, seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione **Agregar**.
3. Introduzca un nombre de certificado.
4. Para acceder a las métricas de Prometheus usando su herramienta de monitoreo externa, seleccione **Permitir Prometheus**.
5. Seleccione **Continuar**.
6. Para el paso **Adjuntar certificados**, seleccione **Generar certificado**.
7. Especifique la información del certificado:
 - **Asunto** (opcional): sujeto X.509 o nombre distinguido (DN) del propietario del certificado.
 - **Días de validez**: La cantidad de días que el certificado generado es válido, a partir del momento en que se genera.
 - **Agregar extensiones de uso de clave**: si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y de uso de clave extendida se agregan al certificado generado.

Estas extensiones definen el propósito de la clave contenida en el certificado.



Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.

8. Seleccione **Generar**.

9. Seleccione **Detalles del certificado del 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 un lugar seguro.

- Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
- Seleccione **Descargar certificado** para guardar el archivo del certificado.

Especifique el nombre del archivo del 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 y pegarla en otro lugar.
- Seleccione **Descargar clave privada** para guardar la clave privada como un archivo.

Especifique el nombre del archivo de clave privada y la ubicación de descarga.

10. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

El nuevo certificado aparece en la pestaña Cliente.

11. En el Administrador de red, seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Global**.
12. Seleccione **Certificado de interfaz de administración**.
13. Seleccione **Usar certificado personalizado**.
14. Cargue los archivos `certificate.pem` y `private_key.pem` desde el [detalles del certificado del cliente](#) paso. No es necesario cargar el paquete CA.
- a. Seleccione **Cargar certificado** y luego seleccione **Continuar**.
 - b. Subir cada archivo de certificado(`.pem`).
 - c. Seleccione **Guardar** para guardar el certificado en el Administrador de Grid.

El nuevo certificado aparece en la página de certificados de la interfaz de administración.

15. [Configurar una herramienta de monitorización externa](#), como Grafana.

Configurar una herramienta de monitoreo externo

Pasos

1. Configure los siguientes ajustes en su herramienta de monitoreo externa, como Grafana.
 - a. **Nombre:** Ingrese un nombre para la conexión.

StorageGRID no requiere esta información, pero debe proporcionar un nombre para probar la conexión.
 - b. **URL:** Ingrese 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. Habilitar **Autenticación de cliente TLS y Con certificado CA**.

d. En Detalles de autenticación TLS/SSL, copie y pegue: +

- El certificado CA de la interfaz de administración para **CA Cert**
- El certificado de cliente para **Certificado de cliente**
- La clave privada de **Clave de cliente**

e. **ServerName**: Ingrese el nombre de dominio del nodo de administración.

ServerName debe coincidir con el nombre de dominio tal como aparece en el certificado de la interfaz de administración.

2. Guarde y pruebe el certificado y la clave privada que copió de StorageGRID o de un archivo local.

Ahora puede acceder a las métricas de Prometheus desde StorageGRID con su herramienta de monitoreo externa.

Para obtener información sobre las métricas, consulte la ["Instrucciones para monitorear StorageGRID"](#).

Editar certificados de cliente

Puede editar un certificado de cliente administrador para cambiar su nombre, habilitar o deshabilitar el acceso a Prometheus o cargar un nuevo certificado cuando el actual haya expirado.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.

Las fechas de vencimiento de los certificados y los permisos de acceso de Prometheus se enumeran en la tabla. Si un certificado caducará pronto o ya caducó, aparece un mensaje en la tabla y se activa una alerta.

2. Seleccione el certificado que desea editar.

3. Seleccione **Editar** y luego seleccione **Editar nombre y permiso**

4. Introduzca un nombre de certificado.

5. Para acceder a las métricas de Prometheus usando su herramienta de monitoreo externa, seleccione **Permitir Prometheus**.

6. Seleccione **Continuar** para guardar el certificado en el Administrador de Grid.

El certificado actualizado se muestra en la pestaña Cliente.

Adjuntar nuevo certificado de cliente

Puede cargar un nuevo certificado cuando el actual haya expirado.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.

Las fechas de vencimiento de los certificados y los permisos de acceso de Prometheus se enumeran en la tabla. Si un certificado caducará pronto o ya caducó, aparece un mensaje en la tabla y se activa una alerta.

2. Seleccione el certificado que desea editar.
3. Seleccione **Editar** y luego seleccione una opción de edición.

Subir certificado

Copie el texto del certificado para pegarlo en otro lugar.

- a. Seleccione **Cargar certificado** y luego seleccione **Continuar**.
- b. Subir el nombre del certificado del cliente(.pem).

Seleccione **Detalles del certificado del cliente** para mostrar los metadatos del certificado y el PEM del certificado.

- Seleccione **Descargar certificado** para guardar el archivo del certificado.

Especifique el nombre del archivo del 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 y pegarlo en otro lugar.
- c. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

El certificado actualizado se muestra en la pestaña Cliente.

Generar certificado

Generar el texto del certificado para pegarlo en otro lugar.

- a. Seleccione **Generar certificado**.
- b. Especifique la información del certificado:

- **Asunto** (opcional): sujeto X.509 o nombre distinguido (DN) del propietario del certificado.
- **Días de validez**: La cantidad de días que el certificado generado es válido, a partir del momento en que se genera.
- **Agregar extensiones de uso de clave**: si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y de uso de clave extendida se agregan al certificado generado.

Estas extensiones definen el propósito de la clave contenida en el certificado.



Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.

- c. Seleccione **Generar**.
- d. Seleccione **Detalles del certificado del 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 un lugar seguro.

- Seleccione **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro

lugar.

- Seleccione **Descargar certificado** para guardar el archivo del certificado.

Especifique el nombre del archivo del 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 y pegarla en otro lugar.
- Seleccione **Descargar clave privada** para guardar la clave privada como un archivo.

Especifique el nombre del archivo de clave privada y la ubicación de descarga.

e. Seleccione **Crear** para guardar el certificado en el Administrador de Grid.

El nuevo certificado aparece en la pestaña Cliente.

Descargar o copiar certificados de cliente

Puede descargar o copiar un certificado de cliente para usarlo en otro lugar.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione el certificado que desea copiar o descargar.
3. Descargue o copie el certificado.

Descargar archivo de certificado

Descargar el certificado `.pem` archivo.

- a. Seleccione **Descargar certificado**.
- b. Especifique el nombre del archivo del 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 para pegarlo 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`

Eliminar certificados de cliente

Si ya no necesita un certificado de cliente administrador, puede eliminarlo.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego seleccione la pestaña **Cliente**.
2. Seleccione el certificado que desea eliminar.
3. Seleccione **Eliminar** y luego confirme.



Para eliminar hasta 10 certificados, seleccione cada certificado que desee eliminar en la pestaña Cliente y luego seleccione **Acciones > Eliminar**.

Después de eliminar un certificado, los clientes que lo usaron deben especificar un nuevo certificado de cliente para acceder a la base de datos StorageGRID Prometheus.

Configurar ajustes de seguridad

Administrar la política TLS y SSH

La política TLS y SSH determina qué protocolos y cifrados se utilizan para establecer conexiones TLS seguras con aplicaciones cliente y conexiones SSH seguras con servicios internos de StorageGRID .

La política de seguridad controla cómo TLS y SSH cifran los datos en movimiento. En general, utilice la política de compatibilidad moderna (predeterminada), a menos que su sistema necesite cumplir con los Criterios comunes o necesite utilizar otros cifrados.



Algunos servicios de StorageGRID no se han actualizado para usar los cifrados en estas políticas.

Antes de empezar

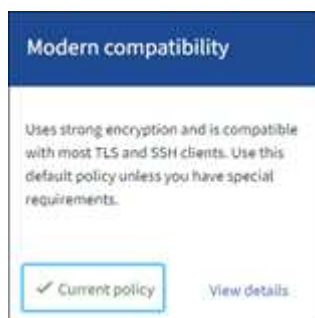
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .

Seleccione una política de seguridad

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Configuración de seguridad**.

La pestaña **Políticas TLS y SSH** muestra las políticas disponibles. La política actualmente activa se indica mediante una marca de verificación verde en el mosaico de políticas.



2. Revise los mosaicos para conocer las políticas disponibles.

Política	Descripción
Compatibilidad moderna (predeterminada)	Utilice la política predeterminada si necesita un cifrado fuerte y a menos que tenga requisitos especiales. Esta política es compatible con la mayoría de los clientes TLS y SSH.
Compatibilidad heredada	Utilice esta política si necesita opciones de compatibilidad adicionales para clientes más antiguos. Las opciones adicionales en esta política podrían hacerla menos segura que la política de compatibilidad moderna.
Criterios comunes	Utilice esta política si necesita la certificación Common Criteria.
FIPS estricto	Utilice esta política si necesita la certificación Common Criteria y usar el Módulo de seguridad criptográfica de NetApp 3.0.8 para conexiones de clientes externos a puntos finales de balanceador de carga, Tenant Manager y Grid Manager. El uso de esta política podría reducir el rendimiento. Nota: Después de seleccionar esta política, todos los nodos deben estar "reiniciado de forma continua" para activar el módulo de seguridad criptográfica de NetApp . Utilice Mantenimiento > Reinicio progresivo para iniciar y supervisar los reinicios.
Costumbre	Cree una política personalizada si necesita aplicar sus propios cifrados.

3. Para ver detalles sobre los cifrados, protocolos y algoritmos de cada política, seleccione **Ver detalles**.
4. Para cambiar la política actual, seleccione **Usar política**.

Aparece una marca de verificación verde junto a **Política actual** en el mosaico de políticas.

Crear una política de seguridad personalizada

Puede crear una política personalizada si necesita aplicar sus propios cifrados.

Pasos

1. Desde el mosaico de la política que sea más similar a la política personalizada que desea crear, seleccione **Ver detalles**.
2. Seleccione **Copiar al portapapeles** y luego seleccione **Cancelar**.



3. Desde el mosaico **Política personalizada**, seleccione **Configurar y usar**.
4. Pegue el JSON que copió y realice los cambios necesarios.
5. Seleccione **Política de uso**.

Aparece una marca de verificación verde junto a **Política actual** en el mosaico Política personalizada.

6. Opcionalmente, seleccione **Editar configuración** para realizar más cambios en la nueva política personalizada.

Revertir temporalmente a la política de seguridad predeterminada

Si configuró una política de seguridad personalizada, es posible que no pueda iniciar sesión en Grid Manager si la política TLS configurada es incompatible con la ["certificado de servidor configurado"](#).

Puede volver temporalmente a la política de seguridad predeterminada.

Pasos

1. Inicie sesión en un nodo de administración:
 - a. Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

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

2. Ejecute el siguiente comando:

```
restore-default-cipher-configurations
```

3. Desde un navegador web, acceda al Administrador de cuadrícula en el mismo nodo de administración.
4. Siga los pasos en [Seleccione una política de seguridad](#) para configurar la política nuevamente.

Configurar la seguridad de la red y de los objetos

Puede configurar la seguridad de la red y de los objetos para cifrar los objetos almacenados, evitar ciertas solicitudes S3 o permitir que las conexiones de los clientes a los nodos de almacenamiento utilicen HTTP en lugar de HTTPS.

Cifrado de objetos almacenados

El cifrado de objetos almacenados permite el cifrado de todos los datos de los objetos a medida que se ingieren a través de S3. De forma predeterminada, los objetos almacenados no están cifrados, pero puede elegir cifrarlos utilizando el algoritmo de cifrado AES-128 o AES-256. Cuando habilita 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 actualmente cifrados permanecerán cifrados, pero los objetos recién ingeridos no lo estarán.

La configuración de cifrado de objetos almacenados se aplica únicamente a los objetos S3 que no se han cifrado mediante cifrado a nivel de depósito o de objeto.

Para obtener más detalles sobre los métodos de cifrado de StorageGRID , consulte ["Revisar los métodos de cifrado de StorageGRID"](#) .

Evitar modificaciones del cliente

Evitar modificaciones del cliente es una configuración de todo el sistema. Cuando se selecciona la opción **Impedir modificación del cliente**, se rechazan las siguientes solicitudes.

API REST de S3

- Solicitudes de DeleteBucket
- Cualquier solicitud para modificar los datos de un objeto existente, los metadatos definidos por el usuario o el etiquetado de objetos S3

Habilitar HTTP para conexiones de nodo de almacenamiento

De forma predeterminada, las aplicaciones cliente utilizan el protocolo de red HTTPS para cualquier conexión directa a los nodos de almacenamiento. Opcionalmente, puede habilitar HTTP para estas conexiones, por ejemplo, al probar una cuadrícula que no es de producción.

Utilice HTTP para las conexiones de nodo de almacenamiento solo si los clientes S3 necesitan realizar conexiones HTTP directamente a los nodos de almacenamiento. No es necesario utilizar esta opción para clientes que solo usan conexiones HTTPS o para clientes que se conectan al servicio Load Balancer (porque puede ["configurar cada punto final del balanceador de carga"](#) para utilizar HTTP o HTTPS).

Ver ["Resumen: Direcciones IP y puertos para conexiones de cliente"](#) para conocer qué puertos utilizan los clientes S3 cuando se conectan a nodos de almacenamiento mediante HTTP o HTTPS.

Seleccionar opciones

Antes de empezar

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

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Configuración de seguridad**.
2. Seleccione la pestaña **Red y objetos**.
3. Para el cifrado de objetos almacenados, utilice la configuración **Ninguno** (predeterminada) si no desea que se cifren los objetos almacenados, o seleccione **AES-128** o **AES-256** para cifrar los objetos almacenados.
4. Opcionalmente, seleccione **Evitar modificación del cliente** si desea evitar que los clientes S3 realicen solicitudes específicas.



Si cambia esta configuración, tomará aproximadamente un minuto para que se aplique la nueva configuración. El valor configurado se almacena en caché para mejorar el rendimiento y la escala.

5. Opcionalmente, seleccione **Habilitar HTTP para conexiones de nodo de almacenamiento** si los clientes se conectan directamente a los nodos de almacenamiento y desea utilizar conexiones HTTP.



Tenga cuidado al habilitar HTTP para una cuadrícula de producción porque las solicitudes se enviarán sin cifrar.

6. Seleccione **Guardar**.

Cambiar la configuración de seguridad de la interfaz

La configuración de seguridad de la interfaz le permite controlar si se cierra la sesión de los usuarios si están inactivos durante más de la cantidad de tiempo especificada y si se incluye un seguimiento de pila en las respuestas de error de API.

Antes de empezar

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

Acerca de esta tarea

La página **Configuración de seguridad** incluye las configuraciones de **Tiempo de espera de inactividad del navegador** y **Seguimiento de la pila de API de administración**.

Tiempo de espera por inactividad del navegador

Indica cuánto tiempo puede estar inactivo el navegador de un usuario antes de que se cierre la sesión. El valor predeterminado es 15 minutos.

El tiempo de espera por inactividad del navegador también está controlado por lo siguiente:

- Un temporizador StorageGRID independiente, no configurable, que se incluye para la seguridad del sistema. El token de autenticación de cada usuario expira 16 horas después de que el usuario inicia sesión. Cuando expira la autenticación de un usuario, ese usuario cierra la sesión automáticamente, incluso si el tiempo de espera de inactividad del navegador está deshabilitado o no se ha alcanzado el valor del tiempo de espera del navegador. Para renovar el token, el usuario deberá volver a iniciar sesión.
- Configuración de tiempo de espera para el proveedor de identidad, asumiendo que el inicio de sesión único (SSO) está habilitado para StorageGRID.

Si SSO está habilitado y el navegador de un usuario expira, el usuario debe volver a ingresar sus

credenciales de SSO para acceder a StorageGRID nuevamente. Ver ["Configurar el inicio de sesión único"](#) .

Seguimiento de la pila de la API de gestión

Controla si se devuelve un seguimiento de pila en las respuestas de error de API de Grid Manager y Tenant Manager.

Esta opción está deshabilitada de forma predeterminada, pero es posible que desee habilitar esta funcionalidad para un entorno de prueba. En general, debe dejar el seguimiento de pila deshabilitado en entornos de producción para evitar revelar detalles internos del software cuando ocurren errores de API.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Configuración de seguridad**.
2. Seleccione la pestaña **Interfaz**.
3. Para cambiar la configuración del tiempo de espera por inactividad del navegador:
 - a. Expandir el acordeón.
 - b. Para cambiar el período de tiempo de espera, especifique un valor entre 60 segundos y 7 días. El tiempo de espera predeterminado es de 15 minutos.
 - c. Para desactivar esta función, desmarque la casilla de verificación.
 - d. Seleccione **Guardar**.

La nueva configuración no afecta a los usuarios que actualmente hayan iniciado sesión. Los usuarios deben iniciar sesión nuevamente o actualizar sus navegadores para que la nueva configuración de tiempo de espera surta efecto.

4. Para cambiar la configuración del seguimiento de la pila de la API de administración:
 - a. Expandir el acordeón.
 - b. Seleccione la casilla de verificación para devolver un seguimiento de la pila en las respuestas de error de API de Grid Manager y Tenant Manager.



Deje el seguimiento de pila deshabilitado en entornos de producción para evitar revelar detalles internos del software cuando se producen errores de API.

- c. Seleccione **Guardar**.

Configurar servidores de administración de claves

¿Qué es un servidor de administración de claves (KMS)?

Un servidor de administración de claves (KMS) es un sistema externo de terceros que proporciona claves de cifrado a los nodos del dispositivo StorageGRID en el sitio StorageGRID asociado mediante el Protocolo de interoperabilidad de administración de claves (KMIP).

StorageGRID solo admite ciertos servidores de administración de claves. Para obtener una lista de productos y versiones compatibles, utilice el ["Herramienta de matriz de interoperabilidad de NetApp \(IMT\)"](#) .

Puede utilizar uno o más servidores de administración de claves para administrar las claves de cifrado de nodo para cualquier nodo del dispositivo StorageGRID que tenga la configuración **Cifrado de nodo** habilitada

durante la instalación. El uso de servidores de administración de claves con estos nodos de dispositivos le permite proteger sus datos incluso si se quita un dispositivo del centro de datos. Una vez cifrados los volúmenes del dispositivo, no podrá acceder a ningún dato del dispositivo a menos que el nodo pueda comunicarse con el KMS.



StorageGRID no crea ni administra las claves externas que se utilizan para cifrar y descifrar los nodos del dispositivo. Si planea utilizar un servidor de administración de claves externo para proteger los datos de StorageGRID , debe comprender cómo configurar ese servidor y cómo administrar las claves de cifrado. La realización de tareas de gestión de claves queda fuera del alcance de estas instrucciones. Si necesita ayuda, consulte la documentación de su servidor de administración de claves o comuníquese con el soporte técnico.

Configuración de KMS y dispositivos

Antes de poder usar un servidor de administración de claves (KMS) para proteger los datos de StorageGRID en los nodos del dispositivo, debe completar dos tareas de configuración: configurar uno o más servidores KMS y habilitar el cifrado de nodos para los nodos del dispositivo. Una vez completadas estas dos tareas de configuración, el proceso de gestión de claves se produce automáticamente.

El diagrama de flujo muestra los pasos de alto nivel para usar un KMS para proteger los datos de StorageGRID en los nodos del dispositivo.

El diagrama de flujo muestra la configuración de KMS y la configuración del dispositivo ocurriendo en paralelo; sin embargo, puede configurar los servidores de administración de claves antes o después de habilitar el cifrado de nodos para los nuevos nodos del dispositivo, según sus requisitos.

Configurar el servidor de administración de claves (KMS)

La configuración de un servidor de administración de claves incluye los siguientes pasos de alto nivel.

Paso	Referirse a
Acceda al software KMS y agregue un cliente para StorageGRID a cada KMS o clúster KMS.	"Configurar StorageGRID como cliente en el KMS"
Obtenga la información requerida para el cliente StorageGRID en el KMS.	"Configurar StorageGRID como cliente en el KMS"
Agregue el KMS al Grid Manager, asígnelo a un solo sitio o a un grupo predeterminado de sitios, cargue los certificados necesarios y guarde la configuración del KMS.	"Agregar un servidor de administración de claves (KMS)"

Configurar el aparato

La configuración de un nodo de dispositivo para el uso de KMS incluye los siguientes pasos de alto nivel.

1. Durante la etapa de configuración de hardware de la instalación del dispositivo, utilice el instalador de dispositivos StorageGRID para habilitar la configuración **Cifrado de nodo** para el dispositivo.



No se puede habilitar la configuración **Cifrado de nodo** después de agregar un dispositivo a la red, y no se puede usar la administración de claves externa para dispositivos que no tengan habilitado el cifrado de nodo.

2. Ejecute el instalador del dispositivo StorageGRID . Durante la instalación, se asigna una clave de cifrado de datos aleatoria (DEK) a cada volumen del dispositivo, de la siguiente manera:
 - Las DEK se utilizan para cifrar los datos en cada volumen. Estas claves se generan mediante el cifrado de disco LUKS (configuración de clave unificada de Linux) en el sistema operativo del dispositivo y no se pueden modificar.
 - Cada DEK individual está encriptado por una clave de encriptación maestra (KEK). La KEK inicial es una clave temporal que cifra las DEK hasta que el dispositivo pueda conectarse al KMS.
3. Agregue el nodo del dispositivo a StorageGRID.

Ver "[Habilitar el cifrado de nodos](#)" Para más detalles.

Proceso de cifrado de gestión de claves (se produce automáticamente)

El cifrado de gestión de claves incluye los siguientes pasos de alto nivel que se realizan automáticamente.

1. Cuando instala un dispositivo que tiene el cifrado de nodo habilitado en la red, StorageGRID determina si existe una configuración de KMS para el sitio que contiene el nuevo nodo.
 - 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, los datos del dispositivo continúan encriptados por la KEK temporal hasta que configure un KMS para el sitio y el dispositivo reciba la configuración del KMS.
2. El dispositivo utiliza la configuración de 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 reemplaza la KEK temporal y ahora se utiliza para cifrar y descifrar las DEK de los volúmenes del dispositivo.



Cualquier dato que exista antes de que el nodo del dispositivo cifrado se conecte al KMS configurado se cifra con una clave temporal. Sin embargo, los volúmenes del dispositivo no deben considerarse protegidos contra la eliminación del centro de datos hasta que la clave temporal sea reemplazada por la clave de cifrado KMS.

4. Si el dispositivo se enciende o se reinicia, se vuelve a conectar al KMS para solicitar la clave. La clave, que se guarda en la memoria volátil, no puede sobrevivir a una pérdida de energía o a un reinicio.

Consideraciones y requisitos para utilizar un servidor de administración de claves

Antes de configurar un servidor de administración de claves externo (KMS), debe comprender las consideraciones y los requisitos.

¿Qué versión de KMIP es compatible?

StorageGRID es compatible con KMIP versión 1.4.

["Especificación del protocolo de interoperabilidad de gestión de claves versión 1.4"](#)

¿Cuáles son las consideraciones de la red?

La configuración del firewall de red debe permitir que cada nodo del dispositivo se comuniquen a través del puerto utilizado para las comunicaciones del Protocolo de interoperabilidad de administración de claves (KMIP). El puerto KMIP predeterminado es 5696.

Debe asegurarse de que cada nodo del dispositivo que utiliza cifrado de nodo tenga acceso a la red del KMS o del clúster KMS que configuró para el sitio.

¿Qué versiones de TLS son compatibles?

Las comunicaciones entre los nodos del dispositivo y el KMS configurado utilizan conexiones TLS seguras. StorageGRID puede admitir el protocolo TLS 1.2 o TLS 1.3 cuando realiza conexiones KMIP a un KMS o un clúster KMS, según lo que admita el KMS y que ["Política de TLS y SSH"](#) estás usando

StorageGRID negocia el protocolo y el cifrado (TLS 1.2) o el conjunto de cifrados (TLS 1.3) con el KMS cuando realiza la conexión. Para ver qué versiones de protocolo y cifrados/conjuntos de cifrados están disponibles, revise la `tlsOutbound` sección de la política TLS y SSH activa de la red (**CONFIGURACIÓN > Seguridad Configuración de seguridad**).

¿Qué dispositivos son compatibles?

Puede utilizar un servidor de administración de claves (KMS) para administrar las claves de cifrado para cualquier dispositivo StorageGRID en su red que tenga habilitada la configuración **Cifrado de nodo**. Esta configuración solo se puede habilitar durante la etapa de configuración de hardware de la instalación del dispositivo mediante el instalador de dispositivos StorageGRID .



No se puede habilitar el cifrado de nodos después de agregar un dispositivo a la red, y no se puede usar la administración de claves externa para dispositivos que no tengan habilitado el cifrado de nodos.

Puede utilizar el KMS configurado para dispositivos StorageGRID y nodos de dispositivos.

No se puede utilizar el KMS configurado para nodos basados en software (que no sean dispositivos), incluidos los siguientes:

- Nodos implementados como máquinas virtuales (VM)
- Nodos implementados dentro de motores de contenedores en hosts Linux

Los nodos implementados en estas otras plataformas pueden usar cifrado fuera de StorageGRID en el nivel de disco o de almacén de datos.

¿Cuándo debo configurar los servidores de administración de claves?

Para una nueva instalación, normalmente debe configurar uno o más servidores de administración de claves en Grid Manager antes de crear inquilinos. Esta orden garantiza que los nodos estén protegidos antes de que se almacenen datos de objetos en ellos.

Puede configurar los servidores de administración de claves en Grid Manager antes o después de instalar los nodos del dispositivo.

¿Cuántos servidores de gestión de claves necesito?

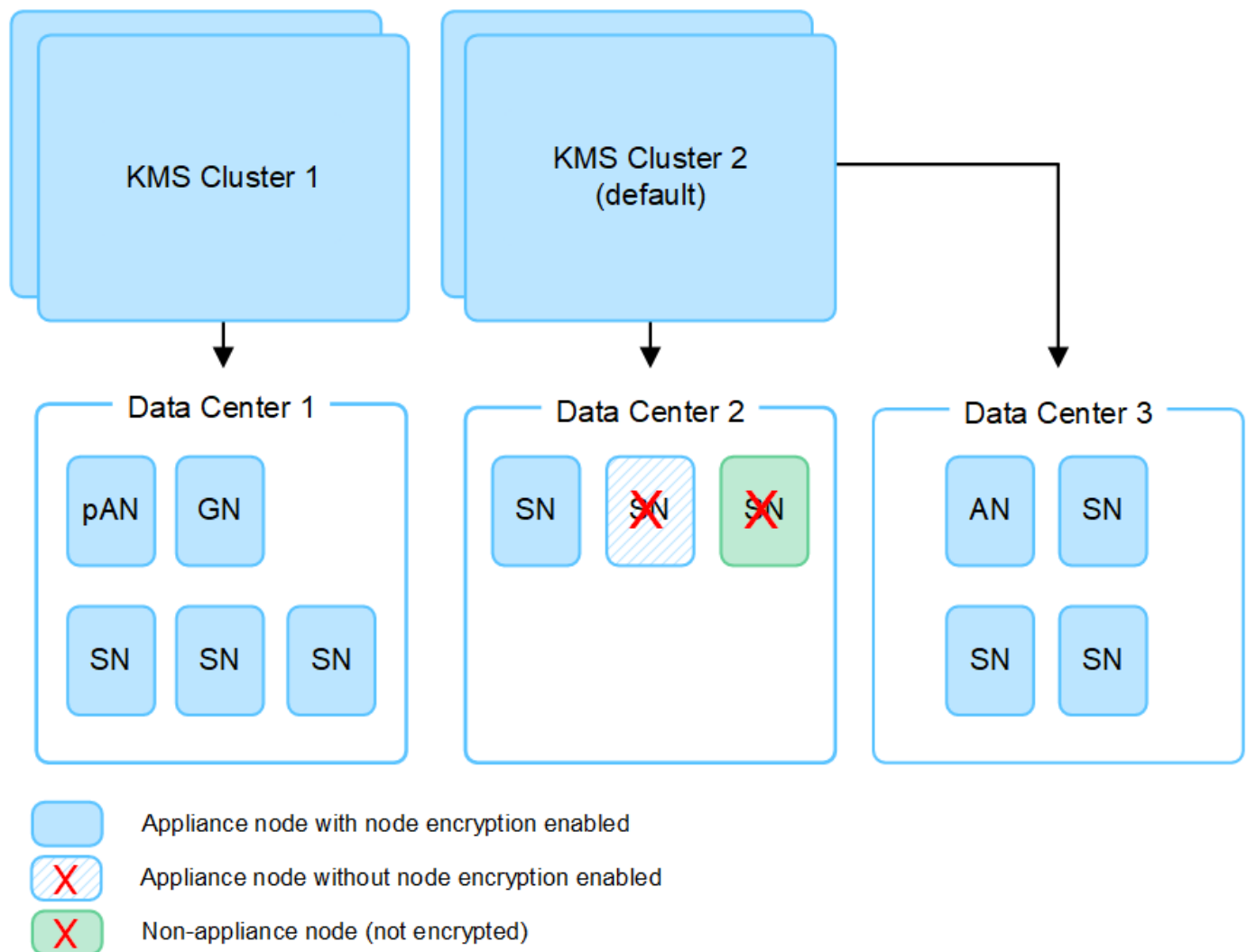
Puede configurar uno o más servidores de administración de claves externos para proporcionar claves de

cifrado a los nodos del dispositivo en su sistema StorageGRID . Cada KMS proporciona una única clave de cifrado a los nodos del dispositivo StorageGRID en un solo sitio o en un grupo de sitios.

StorageGRID admite el uso de clústeres KMS. Cada clúster KMS contiene varios servidores de administración de claves replicados que comparten configuraciones y claves de cifrado. Se recomienda el uso de clústeres KMS para la administración de claves porque mejora las capacidades de conmutación por error de una configuración de alta disponibilidad.

Por ejemplo, supongamos que su sistema StorageGRID tiene tres sitios de centros de datos. Puede configurar un clúster KMS para proporcionar una clave a todos los nodos del dispositivo en el centro de datos 1 y un segundo clúster KMS para proporcionar una clave a todos los nodos del dispositivo en todos los demás sitios. Cuando agrega el segundo clúster KMS, puede configurar un KMS predeterminado para el Centro de datos 2 y el Centro de datos 3.

Tenga en cuenta que no puede usar un KMS para nodos que no sean dispositivos o para ningún nodo de dispositivo que no tuviera habilitada la configuración **Cifrado de nodo** durante la instalación.



¿Qué sucede cuando se gira una llave?

Como práctica recomendada de seguridad, debe realizar periódicamente ["rotar la clave de cifrado"](#) utilizado por cada KMS configurado.

Cuando la nueva versión de la clave esté disponible:

- Se distribuye automáticamente a los nodos del dispositivo cifrado en el sitio o sitios asociados con el KMS. La distribución debe ocurrir dentro de una hora después de que se gira la clave.
- Si el nodo del dispositivo cifrado está fuera de línea cuando se distribuye la nueva versión de la clave, el nodo recibirá la nueva clave tan pronto como se reinicie.
- Si por algún motivo no se puede usar la nueva versión de la clave para cifrar los volúmenes del dispositivo, se activa la alerta **Error en la rotación de la clave de cifrado KMS** para el nodo del dispositivo. Es posible que necesite ponerse en contacto con el soporte técnico para obtener ayuda para resolver esta alerta.

¿Puedo reutilizar un nodo de dispositivo después de haberlo cifrado?

Si necesita instalar un dispositivo cifrado en otro sistema StorageGRID , primero debe dismantelar el nodo de la red para mover los datos del objeto a otro nodo. Luego, puede utilizar el instalador del dispositivo StorageGRID para "[borrar la configuración de KMS](#)". Al borrar la configuración de KMS se deshabilita la configuración de **Cifrado de nodo** y se elimina la asociación entre el nodo del dispositivo y la configuración de KMS para el sitio StorageGRID .



Sin acceso a la clave de cifrado KMS, ya no se puede acceder a los datos que permanecen en el dispositivo y quedan bloqueados de forma permanente.

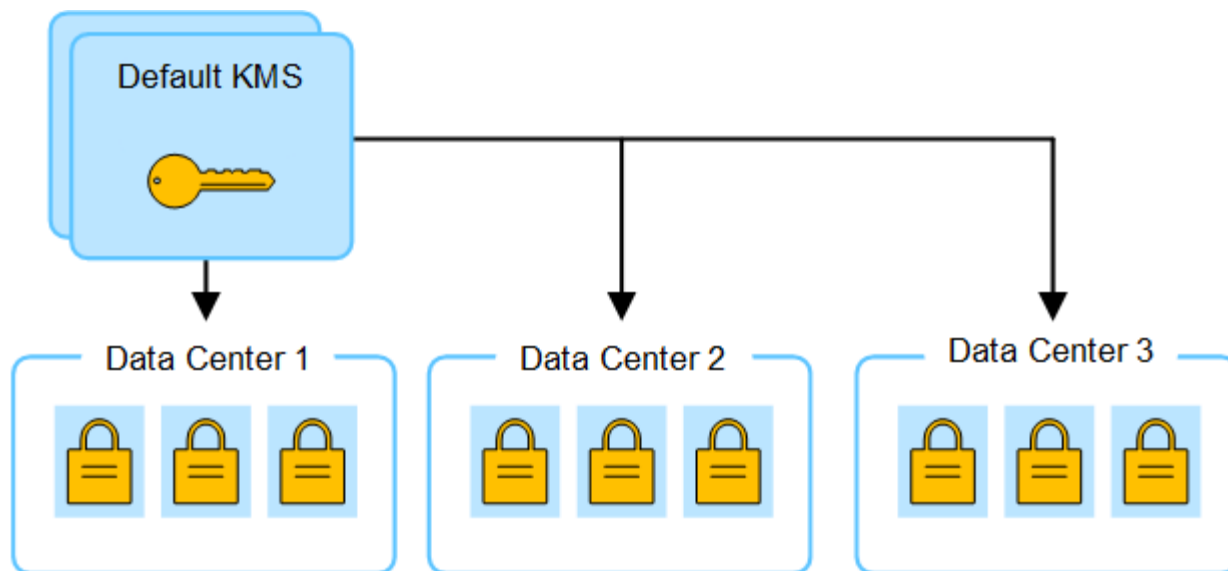
Consideraciones para cambiar el KMS de un sitio

Cada servidor de administración de claves (KMS) o clúster KMS proporciona una clave de cifrado a todos los nodos del dispositivo en un solo sitio o en un grupo de sitios. Si necesita cambiar el KMS que se utiliza para un sitio, es posible que deba copiar la clave de cifrado de un KMS a otro.

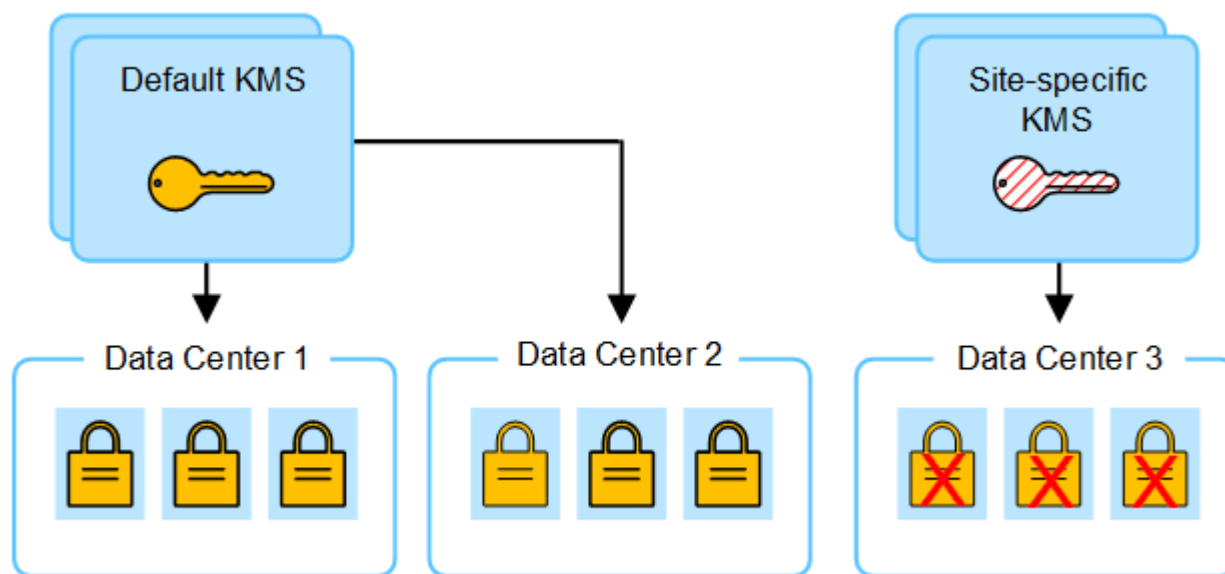
Si cambia el KMS utilizado para un sitio, debe asegurarse de que los nodos del dispositivo previamente cifrados en ese sitio se puedan descifrar usando la clave almacenada en el nuevo KMS. En algunos casos, es posible que necesites copiar la versión actual de la clave de cifrado del KMS original al nuevo KMS. Debe asegurarse de que el KMS tenga la clave correcta para descifrar los nodos del dispositivo cifrados en el sitio.

Por ejemplo:

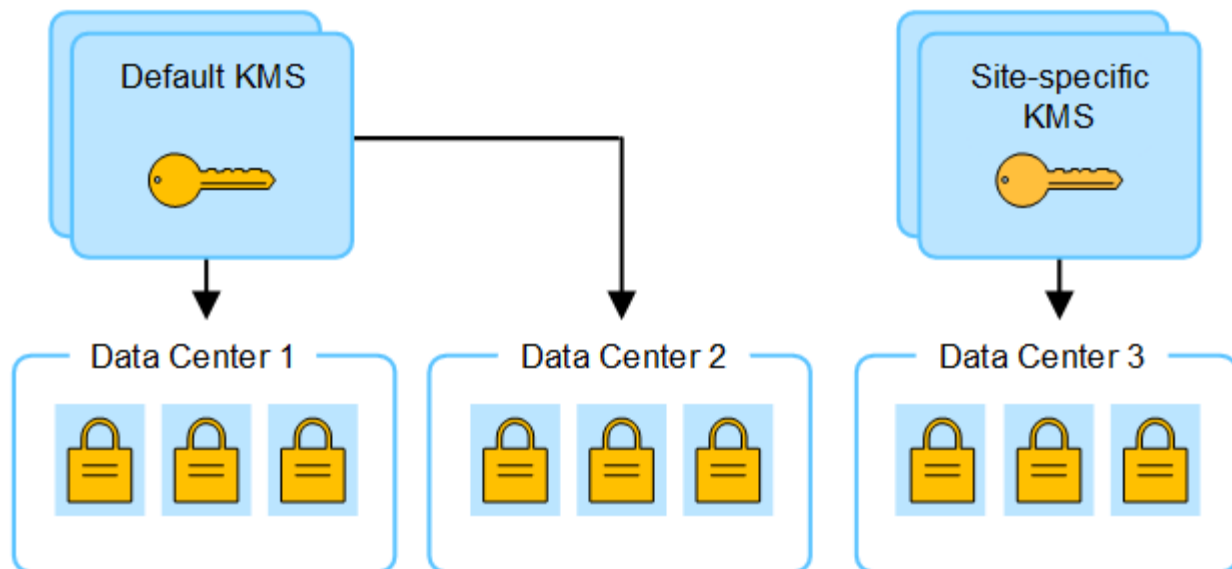
1. Inicialmente, configura un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.
2. Cuando se guarda el KMS, todos los nodos del dispositivo que tienen habilitada la configuración **Cifrado de nodo** se conectan al KMS y solicitan la clave de cifrado. Esta clave se utiliza para cifrar los nodos del dispositivo en todos los sitios. Esta misma clave también debe utilizarse para descifrar dichos dispositivos.



3. Decide agregar un KMS específico del sitio para un sitio (Centro de datos 3 en la figura). Sin embargo, debido a que los nodos del dispositivo ya están cifrados, se produce un error de validación cuando intenta guardar la configuración del 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, copie la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. (Técnicamente, se copia la clave original a una nueva clave con el mismo alias. (La clave original se convierte en una versión anterior de la nueva clave). El KMS específico del sitio ahora tiene la clave correcta para descifrar los nodos del dispositivo en el Centro de datos 3, por lo que se puede guardar en StorageGRID.



Casos de uso para cambiar el KMS que se utiliza para un sitio

La tabla resume los pasos necesarios para los casos más comunes de cambio del KMS de un sitio.

Caso de uso para cambiar el KMS de un sitio	Pasos necesarios
Tiene una o más entradas KMS específicas del sitio y desea utilizar una de ellas como KMS predeterminado.	Editar 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 ahora se utilizará como KMS predeterminado. Se aplicará a cualquier sitio que no tenga un KMS dedicado. "Editar un servidor de administración de claves (KMS)"
Tienes un KMS predeterminado y agregas un nuevo sitio en una expansión. No desea utilizar el KMS predeterminado para el nuevo sitio.	1. Si los nodos del dispositivo en el nuevo sitio ya fueron cifrados por el KMS predeterminado, use el software KMS para copiar la versión actual de la clave de cifrado del KMS predeterminado a un nuevo KMS. 2. Utilizando el Administrador de cuadrícula, agregue el nuevo KMS y seleccione el sitio. "Agregar un servidor de administración de claves (KMS)"
Desea que el KMS de un sitio utilice un servidor diferente.	1. Si los nodos del dispositivo en el sitio ya han sido cifrados por el KMS existente, utilice el software KMS para copiar la versión actual de la clave de cifrado del KMS existente al nuevo KMS. 2. Utilizando el Administrador de cuadrícula, edite la configuración KMS existente e ingrese el nuevo nombre de host o dirección IP. "Agregar un servidor de administración de claves (KMS)"

Configurar StorageGRID como cliente en el KMS

Debe configurar StorageGRID como cliente para cada servidor de administración de claves externo o clúster KMS antes de poder agregar el KMS a StorageGRID.



Estas instrucciones se aplican a Thales CipherTrust Manager y Hashicorp Vault. Para obtener una lista de productos y versiones compatibles, utilice el ["Herramienta de matriz de interoperabilidad de NetApp \(IMT\)"](#).

Pasos

1. Desde el software KMS, cree un cliente StorageGRID para cada KMS o clúster KMS que planee utilizar.

Cada KMS administra una única clave de cifrado para los nodos de dispositivos StorageGRID en un solo sitio o en un grupo de sitios.

2. Cree una clave utilizando uno de los dos métodos siguientes:
 - Utilice la página de administración de claves de su producto KMS. Cree una clave de cifrado AES para cada KMS o clúster KMS.

La clave de cifrado debe tener 2048 bits o más y debe ser exportable.

- Haga que StorageGRID cree la clave. Se le avisará cuando realice la prueba y guarde después ["cargando certificados de cliente"](#).

3. Registre la siguiente información para cada KMS o clúster KMS.

Necesita esta información cuando agrega 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 en el KMS.

4. Para cada KMS o clúster KMS, obtenga un certificado de servidor firmado por una autoridad de certificación (CA) o un paquete de certificados que contenga cada uno de los archivos de certificado de CA codificados en PEM, concatenados en el orden de la cadena de certificados.

El certificado del servidor permite que el KMS externo se autentique en StorageGRID.

- El certificado debe utilizar el formato X.509 codificado en Base-64 de correo de privacidad mejorada (PEM).
- El campo Nombre alternativo del sujeto (SAN) en 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 ingresar los mismos FQDN o direcciones IP en el campo **Nombre de host**.

- El certificado del servidor debe coincidir con el certificado utilizado por la interfaz KMIP del KMS, que normalmente utiliza el puerto 5696.

5. Obtenga el certificado de cliente público emitido a StorageGRID por el KMS externo y la clave privada para el certificado de cliente.

El certificado de cliente permite que StorageGRID se autentique ante el KMS.

Agregar un servidor de administración de claves (KMS)

Utilice el asistente del servidor de administración de claves StorageGRID para agregar cada KMS o clúster KMS.

Antes de empezar

- Usted ha revisado el ["Consideraciones y requisitos para utilizar un servidor de administración de claves"](#) .
- Tienes ["configuró StorageGRID como cliente en el KMS"](#) y tiene la información requerida para cada KMS o clúster KMS.
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .

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 aplique a todos los sitios no administrados por otro KMS. Si crea primero el KMS predeterminado, todos los dispositivos con nodos cifrados en la red se cifrarán con el KMS predeterminado. Si más adelante desea crear un KMS específico del sitio, primero debe copiar la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. Ver ["Consideraciones para cambiar el KMS de un sitio"](#) Para más detalles.

Paso 1: Detalles del KMS

En el Paso 1 (Detalles de KMS) del asistente Agregar un servidor de administración de claves, debe proporcionar detalles sobre el KMS o el clúster de KMS.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Servidor de administración de claves**.

Aparece la página del servidor de administración de claves con la pestaña Detalles de configuración seleccionada.

2. Seleccione **Crear**.

Aparece el paso 1 (detalles de KMS) del asistente Agregar un servidor de administración de claves.

3. Ingrese la siguiente información para el KMS y el cliente StorageGRID que configuró en ese KMS.

Campo	Descripción
Nombre KMS	Un nombre descriptivo para ayudarlo a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de la clave	El alias de clave exacto para el cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. Nota: Si no ha creado una clave con su producto KMS, se le solicitará que StorageGRID cree la clave.

Campo	Descripción
Administra claves para	El sitio StorageGRID que se asociará con este KMS. Si es posible, debe configurar cualquier servidor de administración de claves específico del sitio antes de configurar un KMS predeterminado que se aplique a todos los sitios no administrados por otro KMS. • Seleccione un sitio si este KMS administrará claves de cifrado para los nodos del dispositivo 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 cuando guarde la configuración de KMS si selecciona un sitio que anteriormente fue cifrado por el KMS predeterminado pero no proporcionó la versión actual de la clave de cifrado original al nuevo KMS.
Puerto	El puerto que utiliza el servidor KMS para las comunicaciones del Protocolo de interoperabilidad de administración de claves (KMIP). El valor predeterminado es 5696, que es el puerto estándar KMIP.
Nombre de host	El nombre de dominio completo o la dirección IP para el KMS. Nota: El campo Nombre alternativo del sujeto (SAN) del certificado del servidor debe incluir el FQDN o la dirección IP que ingrese aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

4. Si está configurando un clúster KMS, seleccione **Agregar otro nombre de host** para agregar un nombre de host para cada servidor en el clúster.
5. Seleccione **Continuar**.

Paso 2: Cargar el certificado del servidor

En el paso 2 (Cargar certificado de servidor) del asistente Agregar un servidor de administración de claves, cargue el certificado de servidor (o paquete de certificados) para el KMS. El certificado del servidor permite que el KMS externo se autentique en StorageGRID.

Pasos

1. Desde el **Paso 2 (Cargar certificado de servidor)**, busque la ubicación del certificado de servidor o paquete de certificados guardado.
2. Subir el archivo del certificado.

Aparecen los metadatos del certificado del servidor.



Si cargó un paquete de certificados, los metadatos de cada certificado aparecen en su propia pestaña.

3. Seleccione **Continuar**.

Paso 3: Cargar certificados de cliente

En el paso 3 (Cargar certificados de cliente) del asistente Agregar un servidor de administración de claves, cargue el certificado de cliente y la clave privada del certificado de cliente. El certificado de cliente permite que StorageGRID se autentique ante el KMS.

Pasos

1. Desde el **Paso 3 (Cargar certificados de cliente)**, busque la ubicación del certificado de cliente.
2. Subir el archivo del certificado del cliente.

Aparecen los metadatos del certificado del cliente.

3. Busque la ubicación de la clave privada para el certificado del cliente.
4. Sube el archivo de clave privada.
5. Seleccione **Probar y guardar**.

Si no existe una clave, se le solicitará que StorageGRID cree una.

Se prueban las conexiones entre el servidor de administración de claves y los nodos del dispositivo. Si todas las conexiones son válidas y se encuentra la clave correcta en el KMS, el nuevo servidor de administración de claves se agrega a la tabla en la página Servidor de administración de claves.



Inmediatamente después de agregar un KMS, el estado del certificado en la página del Servidor de administración de claves aparece como Desconocido. StorageGRID podría tardar hasta 30 minutos en obtener el estado real de cada certificado. Debe actualizar su navegador web para ver el estado actual.

6. Si aparece un mensaje de error al seleccionar **Probar y guardar**, revise los detalles del mensaje y luego seleccione **Aceptar**.

Por ejemplo, es posible que reciba un error 422: Entidad no procesable si falla una prueba de conexión.

7. Si necesita guardar la configuración actual sin probar la conexión externa, seleccione **Forzar guardado**.



Al seleccionar **Forzar guardado** 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 del dispositivo que tengan el cifrado de nodo habilitado en el sitio afectado. Podría perder el acceso a sus 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.

Se guarda la configuración del KMS pero no se prueba la conexión al KMS.

Administrar un KMS

Administrar un servidor de administración de claves (KMS) implica ver o editar detalles, administrar certificados, ver nodos cifrados y eliminar un KMS cuando ya no es

necesario.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["permiso de acceso requerido"](#) .

Ver detalles de KMS

Puede ver información sobre cada servidor de administración de claves (KMS) en su sistema StorageGRID , incluidos los detalles de la clave y el estado actual de los certificados del servidor y del cliente.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Servidor de administración de claves**.

Aparece la página del servidor de administración de claves y muestra la siguiente información:

- La pestaña Detalles de configuración enumera todos los servidores de administración de claves que están configurados.
 - La pestaña Nodos cifrados enumera todos los nodos que tienen el cifrado de nodo habilitado.
2. Para ver los detalles de un KMS específico y realizar operaciones en ese KMS, seleccione el nombre del KMS. La página de detalles del KMS enumera la siguiente información:

Campo	Descripción
Administra claves para	El sitio StorageGRID asociado con el KMS. Este campo muestra el nombre de un sitio StorageGRID específico o Sitios no administrados por otro KMS (KMS predeterminado) .
Nombre de host	El nombre de dominio completo o la dirección IP del KMS. Si hay un clúster de dos servidores de administración de claves, se enumeran el nombre de dominio completo o la dirección IP de ambos servidores. Si hay más de dos servidores de administración de claves en un clúster, se incluye el nombre de dominio completo o la dirección IP del primer KMS junto con la cantidad de servidores de administración 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 en un clúster, seleccione un KMS y seleccione Editar o Acciones > Editar .

3. Seleccione una pestaña en la página de detalles de KMS para ver la siguiente información:

Pestaña	Campo	Descripción
Detalles clave	Nombre de la clave	El alias de clave para el cliente StorageGRID en el KMS.

Pestaña	Campo	Descripción
UID de clave	El identificador único de la última versión de la clave.	Última modificación
La fecha y hora de la última versión de la clave.	Certificado de servidor	Metadatos
Los metadatos del certificado, como el número de serie, la fecha y hora de vencimiento y el PEM del certificado.	Certificado PEM	El contenido del archivo PEM (correo con privacidad mejorada) del certificado.
Certificado de cliente	Metadatos	Los metadatos del certificado, como el número de serie, la fecha y hora de vencimiento y el PEM del certificado.

4. Con la frecuencia que requieran las prácticas de seguridad de su organización, seleccione **Rotar clave** o utilice el software KMS para crear una nueva versión de la clave.

Cuando la rotación de clave es exitosa, se actualizan los campos UID de clave y Última modificación.



Si rota la clave de cifrado utilizando el software KMS, rótelea desde la última versión utilizada de la clave a una nueva versión de la misma clave. No gire a una clave completamente diferente.

Nunca intente rotar una clave cambiando el nombre de la clave (alias) para el KMS. StorageGRID requiere que todas las versiones de clave utilizadas anteriormente (así como cualquier versión futura) sean accesibles desde el KMS con el mismo alias de clave. Si cambia el alias de clave de un KMS configurado, es posible que StorageGRID no pueda descifrar sus datos.

Administrar certificados

Aborde rápidamente cualquier problema con el certificado del servidor o del cliente. Si es posible, reemplace los certificados antes de que caduquen.



Debe abordar cualquier problema de certificado lo antes posible para mantener el acceso a los datos.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Servidor de administración de claves**.
2. En la tabla, observe el valor de vencimiento del certificado para cada KMS.
3. Si la expiración del certificado para cualquier KMS es desconocida, espere hasta 30 minutos y luego actualice su navegador web.
4. Si la columna Vencimiento del certificado indica que un certificado ha vencido o está próximo a vencer,

seleccione el KMS para ir a la página de detalles del KMS.

- a. Seleccione **Certificado de servidor** y verifique el valor del campo "Vence el".
 - b. Para reemplazar el certificado, seleccione **Editar certificado** para cargar un nuevo certificado.
 - c. Repita estos subpasos y seleccione **Certificado de cliente** en lugar de Certificado de servidor.
5. Cuando se activan las alertas **Expiración del certificado de CA de KMS**, **Expiración del certificado de cliente de KMS** y **Expiración del certificado de servidor de KMS**, tenga en cuenta la descripción de cada alerta y realice las acciones recomendadas.

StorageGRID podría tardar hasta 30 minutos en obtener actualizaciones sobre la expiración del certificado. Actualice su navegador web para ver los valores actuales.



Si obtiene un estado de **El estado del certificado del servidor es desconocido**, asegúrese de que su KMS permita obtener un certificado de servidor sin requerir un certificado de cliente.

Ver nodos cifrados

Puede ver información sobre los nodos del dispositivo en su sistema StorageGRID que tienen habilitada la configuración **Cifrado de nodo**.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Servidor de administración de claves**.

Aparece la página del Servidor de administración de claves. La pestaña Detalles de configuración muestra todos los servidores de administración de claves que se han configurado.

2. Desde la parte superior de la página, seleccione la pestaña **Nodos cifrados**.

La pestaña Nodos cifrados enumera los nodos del dispositivo en su sistema StorageGRID que tienen habilitada la configuración **Cifrado de nodo**.

3. Revise la información en la tabla para cada nodo del dispositivo.

Columna	Descripción
Nombre del nodo	El nombre del nodo del dispositivo.
Tipo de nodo	El tipo de nodo: Almacenamiento, Administración o Puerta de enlace.
Sitio	El nombre del sitio StorageGRID donde está instalado el nodo.
Nombre KMS	El nombre descriptivo del KMS utilizado para el nodo. Si no aparece ningún KMS, seleccione la pestaña Detalles de configuración para agregar un KMS. "Agregar un servidor de administración de claves (KMS)"

Columna	Descripción
UID de clave	El identificador único de la clave de cifrado utilizada para cifrar y descifrar datos en el nodo del dispositivo. Para ver un UID de clave completo, seleccione el texto. Un guion (--) 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 los cambios de configuración de KMS. Nota: Actualice su navegador web para ver los nuevos valores.

4. Si la columna Estado indica un problema de KMS, solucione el problema de inmediato.

Durante las operaciones normales de KMS, el estado será **Conectado a KMS**. Si un nodo se desconecta de la red, se muestra el estado de conexión del nodo (Administrativamente inactivo o Desconocido).

Otros mensajes de estado corresponden a alertas de StorageGRID con los mismos nombres:

- La configuración de KMS no se pudo cargar
- Error de conectividad KMS
- No se encontró el nombre de la clave de cifrado KMS
- Error en la rotación de la clave de cifrado KMS
- La clave KMS no pudo descifrar un volumen del dispositivo
- KMS no está configurado

Realice las acciones recomendadas para estas alertas.



Debe abordar cualquier problema de inmediato para garantizar que sus datos estén completamente protegidos.

Editar un KMS

Es posible que necesite editar la configuración de un servidor de administración de claves, por ejemplo, si un certificado está a punto de caducar.

Antes de empezar

- Si planea actualizar el sitio seleccionado para un KMS, ha revisado el ["Consideraciones para cambiar el KMS de un sitio"](#).
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Servidor de administración de claves**.

Aparece la página del servidor de administración de claves y muestra todos los servidores de administración de claves que se han configurado.

2. Seleccione el KMS que desea editar y seleccione **Acciones > Editar**.

También puede editar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Editar** en la página de detalles del KMS.

3. Opcionalmente, actualice los detalles en el **Paso 1 (detalles de KMS)** del asistente Editar un servidor de administración de claves.

Campo	Descripción
Nombre KMS	Un nombre descriptivo para ayudarle a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de la clave	El alias de clave exacto para el 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 la clave si se cambia el nombre del alias en el KMS o si se han copiado todas las versiones de la clave anterior al historial de versiones del nuevo alias.
Administra claves para	Si está editando un KMS específico del sitio y aún no tiene un KMS predeterminado, seleccione opcionalmente Sitios no administrados por otro KMS (KMS predeterminado). Esta selección convierte un KMS específico del sitio en el KMS predeterminado, que se aplicará a todos los sitios que no tengan un KMS dedicado y a cualquier sitio agregado en una expansión. Nota: Si está editando un KMS específico del sitio, no podrá seleccionar otro sitio. Si está editando el KMS predeterminado, no podrá seleccionar un sitio específico.
Puerto	El puerto que utiliza el servidor KMS para las comunicaciones del Protocolo de interoperabilidad de administración de claves (KMIP). El valor predeterminado es 5696, que es el puerto estándar KMIP.
Nombre de host	El nombre de dominio completo o la dirección IP para el KMS. Nota: El campo Nombre alternativo del sujeto (SAN) del certificado del servidor debe incluir el FQDN o la dirección IP que ingrese aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

4. Si está configurando un clúster KMS, seleccione **Agregar otro nombre de host** para agregar un nombre de host para cada servidor en el clúster.
5. Seleccione **Continuar**.

Aparece el paso 2 (Cargar certificado de servidor) del asistente Editar un servidor de administración de claves.

6. Si necesita reemplazar el certificado del servidor, seleccione **Explorar** y cargue el nuevo archivo.

7. Seleccione **Continuar**.

Aparece el paso 3 (Cargar certificados de cliente) del asistente Editar un servidor de administración de claves.

8. Si necesita reemplazar el certificado del cliente y la clave privada del certificado del cliente, seleccione **Explorar** y cargue los nuevos archivos.

9. Seleccione **Probar y guardar**.

Se prueban las conexiones entre el servidor de administración de claves y todos los nodos del dispositivo cifrados en los sitios afectados. Si todas las conexiones de nodo son válidas y se encuentra la clave correcta en el KMS, el servidor de administración de claves se agrega a la tabla en la página Servidor de administración de claves.

10. Si aparece un mensaje de error, revise los detalles del mensaje y seleccione **Aceptar**.

Por ejemplo, es posible que reciba un error 422: Entidad no procesable si el sitio que seleccionó para este KMS ya está administrado por otro KMS o si falló una prueba de conexión.

11. Si necesita guardar la configuración actual antes de resolver los errores de conexión, seleccione **Forzar guardado**.



Al seleccionar **Forzar guardado** 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 del dispositivo que tengan el cifrado de nodo habilitado en el sitio afectado. Podría perder el acceso a sus 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.

Se guarda la configuración del KMS, pero no se prueba la conexión al KMS.

Eliminar un servidor de administración de claves (KMS)

Es posible que en algunos casos desees eliminar un servidor de administración de claves. Por ejemplo, es posible que desees eliminar un KMS específico del sitio si has dado de baja el sitio.

Antes de empezar

- Usted ha revisado el ["Consideraciones y requisitos para utilizar un servidor de administración de claves"](#).
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).

Acerca de esta tarea

Puedes eliminar un KMS en estos casos:

- Puede eliminar un KMS específico del sitio si el sitio se ha dado de baja o si no incluye nodos de dispositivos con cifrado de nodos habilitado.

- Puede eliminar el KMS predeterminado si ya existe un KMS específico del sitio para cada sitio que tenga nodos de dispositivo con cifrado de nodo habilitado.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Servidor de administración de claves**.

Aparece la página del servidor de administración de claves y muestra todos los servidores de administración de claves que se han configurado.

2. Seleccione el KMS que desea eliminar y seleccione **Acciones > Eliminar**.

También puede eliminar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Eliminar** en la página de detalles del KMS.

3. Confirme que lo siguiente es verdadero:

- Está eliminando un KMS específico del sitio para un sitio que no tiene ningún nodo de dispositivo con cifrado de nodo habilitado.
- Está eliminando el KMS predeterminado, pero ya existe un KMS específico del sitio para cada sitio con cifrado de nodo.

4. Seleccione **Sí**.

Se elimina la configuración de KMS.

Administrar la configuración del proxy

Configurar el proxy de almacenamiento

Si utiliza servicios de plataforma o grupos de almacenamiento en la nube, puede configurar un proxy no transparente entre los nodos de almacenamiento y los puntos finales externos de S3. Por ejemplo, es posible que necesite un proxy no transparente para permitir que los mensajes de servicios de la plataforma se envíen a puntos finales externos, como un punto final en Internet.



Las configuraciones del proxy de almacenamiento configuradas no se aplican a los puntos finales de los servicios de la plataforma Kafka.

Antes de empezar

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

Acerca de esta tarea

Puede configurar los ajustes para un único proxy de almacenamiento.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Configuración de proxy**.
2. En la pestaña **Almacenamiento**, seleccione la casilla de verificación **Habilitar proxy de almacenamiento**.
3. Seleccione el protocolo para el proxy de almacenamiento.

4. Introduzca el nombre de host o la dirección IP del servidor proxy.
5. Opcionalmente, ingrese el puerto utilizado para conectarse al servidor proxy.

Deje este campo en blanco para utilizar el puerto predeterminado para el protocolo: 80 para HTTP o 1080 para SOCKS5.

6. Seleccione **Guardar**.

Una vez guardado el proxy de almacenamiento, se pueden configurar y probar nuevos puntos finales para los servicios de la plataforma o los grupos de almacenamiento en la nube.



Los cambios de proxy pueden tardar hasta 10 minutos en surtir efecto.

7. Verifique la configuración de su servidor proxy para asegurarse de que los mensajes relacionados con el servicio de la plataforma de StorageGRID no se bloqueen.
8. Si necesita deshabilitar un proxy de almacenamiento, desmarque la casilla de verificación y seleccione **Guardar**.

Configurar los ajustes del proxy de administración

Si envía paquetes de AutoSupport mediante HTTP o HTTPS, puede configurar un servidor proxy no transparente entre los nodos de administración y el soporte técnico (AutoSupport).

Para obtener más información sobre AutoSupport, consulte ["Configurar AutoSupport"](#).

Antes de empezar

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

Acerca de esta tarea

Puede configurar los ajustes para un solo proxy de administrador.

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Configuración de proxy**.

Aparece la página Configuración de proxy. De forma predeterminada, Almacenamiento está seleccionado en el menú de pestañas.

2. Seleccione la pestaña **Admin**.
3. Seleccione la casilla de verificación **Habilitar 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. Opcionalmente, ingrese un nombre de usuario y una contraseña para el servidor proxy.

Deje estos campos en blanco si su servidor proxy no requiere un nombre de usuario o una contraseña.

7. Seleccione una de las siguientes opciones:

- Si desea proteger la conexión al proxy de administración, seleccione **Verificar certificado de proxy**.

Cargue un paquete de CA para verificar la autenticidad de los certificados SSL presentados por el servidor proxy de administración.



AutoSupport on Demand, E-Series AutoSupport a través de StorageGRID y la determinación de ruta de actualización en la página Actualización de StorageGRID no funcionarán si se verifica un certificado de proxy.

Después de cargar el paquete de CA, aparecen sus metadatos.

- Si no desea validar certificados al comunicarse con el servidor proxy de administración, seleccione **No verificar certificado proxy**.

8. Seleccione **Guardar**.

Una vez guardado el proxy de administración, se configura el servidor proxy entre los nodos de administración y el soporte técnico.



Los cambios de proxy pueden tardar hasta 10 minutos en surtir efecto.

9. Si necesita deshabilitar el proxy de administración, desmarque la casilla **Habilitar proxy de administración** y luego seleccione **Guardar**.

Controlar cortafuegos

Controlar el acceso al firewall externo

Puede abrir o cerrar puertos específicos en el firewall externo.

Puede controlar el acceso a las interfaces de usuario y las API en los nodos de administración de StorageGRID abriendo o cerrando puertos específicos en el firewall externo. Por ejemplo, es posible que desee evitar que los inquilinos puedan conectarse al Grid Manager en el firewall, además de utilizar otros métodos para controlar el acceso al sistema.

Si desea configurar el firewall interno de StorageGRID , consulte ["Configurar el firewall interno"](#) .

Puerto	Descripción	Si el puerto está abierto...
443	Puerto HTTPS predeterminado para nodos de administración	Los navegadores web y los clientes de API de administración pueden acceder al Administrador de Grid, la API de administración de Grid, el Administrador de inquilinos y la API de administración de inquilinos. Nota: El puerto 443 también se utiliza para cierto tráfico interno.

Puerto	Descripción	Si el puerto está abierto...
8443	Puerto de Grid Manager restringido en los nodos de administración	• Los navegadores web y los clientes de API de administración pueden acceder al Administrador de Grid y a la API de administración de Grid mediante HTTPS. • Los navegadores web y los clientes de API de administración no pueden acceder al Administrador de inquilinos ni a la API de administración de inquilinos. • Las solicitudes de contenido interno serán rechazadas.
9443	Puerto de administrador de inquilinos restringido en nodos de administración	• Los navegadores web y los clientes de API de administración pueden acceder al Administrador de inquilinos y a la API de administración de inquilinos mediante HTTPS. • Los navegadores web y los clientes de API de administración no pueden acceder al Administrador de Grid ni a la API de administración de Grid. • Las solicitudes de contenido interno serán rechazadas.



El inicio de sesión único (SSO) no está disponible en los puertos restringidos de Grid Manager o Tenant Manager. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autenticuen con inicio de sesión único.

Información relacionada

- ["Sign in en el Administrador de cuadrícula"](#)
- ["Crear una cuenta de inquilino"](#)
- ["Comunicaciones externas"](#)

Administrar los controles internos del firewall

StorageGRID incluye un firewall interno en cada nodo que mejora la seguridad de su red al permitirle controlar el acceso de la red al nodo. Utilice el firewall para evitar el acceso a la red en todos los puertos excepto aquellos necesarios para su implementación de red específica. Los cambios de configuración que realice en la página de control del Firewall se implementarán en cada nodo.

Utilice las tres pestañas de la página de control de Firewall para personalizar el acceso que necesita para su red.

- **Lista de direcciones privilegiadas:** utilice esta pestaña para permitir el acceso seleccionado a puertos cerrados. Puede agregar direcciones IP o subredes en notación CIDR que puedan acceder a puertos cerrados mediante la pestaña Administrar acceso externo.
- **Administrar acceso externo:** utilice esta pestaña para cerrar puertos que están abiertos de forma

predeterminada o reabrir puertos previamente cerrados.

- **Red de cliente no confiable:** utilice esta pestaña para especificar si un nodo confía en el tráfico entrante de la red de cliente.

La configuración de esta pestaña anula la configuración de la pestaña Administrar acceso externo.

- Un nodo con una red de cliente no confiable solo aceptará conexiones en los puertos de punto final del balanceador de carga configurados en ese nodo (puntos finales globales, de interfaz de nodo y enlazados al tipo de nodo).
- Los puertos finales del equilibrador de carga *son los únicos puertos abiertos* en redes de cliente que no son de confianza, independientemente de la configuración en la pestaña Administrar redes externas.
- Cuando es confiable, todos los puertos abiertos en la pestaña Administrar acceso externo son accesibles, así como también cualquier punto final del balanceador de carga abierto en la red del cliente.



Las configuraciones que realice en una pestaña pueden afectar los cambios de acceso que realice en otra pestaña. Asegúrese de verificar la configuración en todas las pestañas para asegurarse de que su red se comporte de la manera esperada.

Para configurar los controles internos del firewall, consulte ["Configurar los controles del firewall"](#) .

Para obtener más información sobre firewalls externos y seguridad de red, consulte ["Controlar el acceso al firewall externo"](#) .

Lista de direcciones privilegiadas y pestañas para administrar acceso externo

La pestaña Lista de direcciones privilegiadas le permite registrar una o más direcciones IP a las que se les concede acceso a los puertos de la red que están cerrados. La pestaña Administrar acceso externo le permite cerrar el acceso externo a puertos externos seleccionados o a todos los puertos externos abiertos (los puertos externos son puertos a los que pueden acceder los nodos que no pertenecen a la red de manera predeterminada). Estas dos pestañas a menudo se pueden usar juntas para personalizar el acceso de red exacto que necesita permitir para su red.



Las direcciones IP privilegiadas no tienen acceso al puerto de la red interna de forma predeterminada.

Ejemplo 1: Utilizar un host de salto para tareas de mantenimiento

Supongamos que desea utilizar un host de salto (un host con seguridad reforzada) para la administración de la red. Podrías utilizar estos pasos generales:

1. Utilice la pestaña Lista de direcciones privilegiadas para agregar la dirección IP del host de salto.
2. Utilice la pestaña Administrar acceso externo para bloquear todos los puertos.



Agregue la dirección IP privilegiada antes de bloquear los puertos 443 y 8443. Cualquier usuario actualmente conectado a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones privilegiadas.

Después de guardar su configuración, todos los puertos externos en el nodo de administración de su red se bloquearán para todos los hosts excepto el host de salto. Luego, puede utilizar el host de salto para realizar

tareas de mantenimiento en su red de forma más segura.

Ejemplo 2: Bloquear puertos sensibles

Supongamos que desea bloquear puertos sensibles y el servicio en ese puerto (por ejemplo, SSH en el puerto 22). Podrías utilizar los siguientes pasos generales:

1. Utilice la pestaña Lista de direcciones privilegiadas para otorgar acceso solo a los hosts que necesitan acceso al servicio.
2. Utilice la pestaña Administrar acceso externo para bloquear todos los puertos.



Agregue la dirección IP privilegiada antes de bloquear el acceso a cualquier puerto asignado para acceder a Grid Manager y al administrador de inquilinos (los puertos preestablecidos son 443 y 8443). Cualquier usuario actualmente conectado a un puerto bloqueado, incluido usted, perderá el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones privilegiadas.

Después de guardar su configuración, el puerto 22 y el servicio SSH estarán disponibles para los hosts en la lista de direcciones privilegiadas. A todos los demás hosts se les negará el acceso al servicio sin importar de qué interfaz provenga la solicitud.

Ejemplo 3: Deshabilitar el acceso a servicios no utilizados

A nivel de red, podrías deshabilitar algunos servicios que no desees utilizar. Por ejemplo, para bloquear el tráfico del cliente HTTP S3, deberá utilizar el interruptor en la pestaña Administrar acceso externo para bloquear el puerto 18084.

Pestaña Redes de clientes no confiables

Si utiliza una red de cliente, puede ayudar a proteger StorageGRID de ataques hostiles al aceptar tráfico de cliente entrante solo en puntos finales configurados explícitamente.

De forma predeterminada, la red de cliente en cada nodo de la red es *confiable*. Es decir, de forma predeterminada, StorageGRID confía en las conexiones entrantes a cada nodo de la red en todos los ["puertos externos disponibles"](#).

Puede reducir la amenaza de ataques hostiles en su sistema StorageGRID especificando que la red de cliente en cada nodo sea *no confiable*. Si la red de cliente de un nodo no es confiable, el nodo solo acepta conexiones entrantes en puertos configurados explícitamente como puntos finales del balanceador de carga. Ver ["Configurar los puntos finales del balanceador de carga"](#) y ["Configurar los controles del firewall"](#).

Ejemplo 1: El nodo de puerta de enlace solo acepta solicitudes HTTPS S3

Supongamos que desea que un nodo de puerta de enlace rechace todo el tráfico entrante en la red del cliente, excepto las solicitudes HTTPS S3. Realizarías estos pasos generales:

1. Desde ["Puntos finales del balanceador de carga"](#) página, configure un punto final de balanceador de carga para S3 sobre HTTPS en el puerto 443.
2. Desde la página de control de Firewall, seleccione No confiable para especificar que la red de cliente en el nodo de puerta de enlace no es confiable.

Después de guardar su configuración, se descarta todo el tráfico entrante en la red de cliente del nodo de puerta de enlace, excepto las solicitudes HTTPS S3 en el puerto 443 y las solicitudes de eco ICMP (ping).

Ejemplo 2: El nodo de almacenamiento envía solicitudes de servicios de la plataforma S3

Supongamos que desea habilitar el tráfico saliente de servicios de la plataforma S3 desde un nodo de almacenamiento, pero desea evitar cualquier conexión entrante a ese nodo de almacenamiento en la red del cliente. Realizarías este paso general:

- Desde la pestaña Redes de clientes no confiables de la página de control de Firewall, indique que la red de clientes en el nodo de almacenamiento no es confiable.

Después de guardar su configuración, el nodo de almacenamiento ya no acepta tráfico entrante en la red del cliente, pero continúa permitiendo solicitudes salientes a los destinos de servicios de plataforma configurados.

Ejemplo 3: Limitar el acceso a Grid Manager a una subred

Supongamos que desea permitir el acceso a Grid Manager solo en una subred específica. Realizarías los siguientes pasos:

1. Conecte la red de cliente de sus nodos de administración a la subred.
2. Utilice la pestaña Red de cliente no confiable para configurar la red de cliente como no confiable.
3. Cuando crea un punto final de balanceador de carga de interfaz de administración, ingrese el puerto y seleccione la interfaz de administración a la que accederá el puerto.
4. Seleccione **Sí** para Red de cliente no confiable.
5. Utilice la pestaña Administrar acceso externo para bloquear todos los puertos externos (con o sin direcciones IP privilegiadas configuradas para hosts fuera de esa subred).

Después de guardar su configuración, solo los hosts en la subred que especificó podrán acceder al Administrador de Grid. Todos los demás hosts están bloqueados.

Configurar el firewall interno

Puede configurar el firewall de StorageGRID para controlar el acceso de red a puertos específicos en sus nodos de StorageGRID .

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Has revisado la información en ["Administrar los controles del firewall"](#) y ["Pautas para establecer redes"](#) .
- Si desea que un nodo de administración o un nodo de puerta de enlace acepte tráfico entrante solo en puntos finales configurados explícitamente, debe definir los puntos finales del equilibrador de carga.



Al cambiar la configuración de la red del cliente, las conexiones de cliente existentes podrían fallar si no se han configurado los puntos finales del balanceador de carga.

Acerca de esta tarea

StorageGRID incluye un firewall interno en cada nodo que le permite abrir o cerrar algunos de los puertos en los nodos de su red. Puede utilizar las pestañas de control de Firewall para abrir o cerrar puertos que están abiertos de manera predeterminada en la red de cuadrícula, la red de administración y la red de cliente. También puede crear una lista de direcciones IP privilegiadas que pueden acceder a los puertos de la red que están cerrados. Si está utilizando una red de cliente, puede especificar si un nodo confía en el tráfico entrante de la red de cliente y puede configurar el acceso a puertos específicos en la red de cliente.

Limitar la cantidad de puertos abiertos a direcciones IP fuera de su red a solo aquellos que sean absolutamente necesarios mejora la seguridad de su red. Utilice la configuración de cada una de las tres pestañas de control del Firewall para asegurarse de que solo los puertos necesarios estén abiertos.

Para obtener más información sobre el uso de los controles de firewall, incluidos ejemplos, consulte ["Administrar los controles del firewall"](#) .

Para obtener más información sobre firewalls externos y seguridad de red, consulte ["Controlar el acceso al firewall externo"](#) .

Controles de firewall de acceso

Pasos

1. Seleccione **CONFIGURACIÓN > Seguridad > Control de firewall**.

Las tres pestañas de esta página se describen en ["Administrar los controles del firewall"](#) .

2. Seleccione cualquier pestaña para configurar los controles del firewall.

Puede utilizar estas pestañas en cualquier orden. Las configuraciones que establezca en una pestaña no limitan lo que puede hacer en las otras pestañas; sin embargo, los cambios de configuración que realice en una pestaña podrían cambiar el comportamiento de los puertos configurados en otras pestañas.

Lista de direcciones privilegiadas

Utilice la pestaña Lista de direcciones privilegiadas para otorgar a los hosts acceso a puertos que están cerrados de manera predeterminada o cerrados por la configuración de la pestaña Administrar acceso externo.

Las direcciones IP y subredes privilegiadas no tienen acceso a la red interna de forma predeterminada. Además, los puntos finales del balanceador de carga y los puertos adicionales abiertos en la pestaña Lista de direcciones privilegiadas son accesibles incluso si están bloqueados en la pestaña Administrar acceso externo.



Las configuraciones en la pestaña Lista de direcciones privilegiadas no pueden anular las configuraciones en la pestaña Red de cliente no confiable.

Pasos

1. En la pestaña Lista de direcciones privilegiadas, ingrese la dirección o subred IP a la que desea otorgar acceso a los puertos cerrados.
2. Opcionalmente, seleccione **Agregar otra dirección IP o subred en notación CIDR** para agregar clientes privilegiados adicionales.



Agregue la menor cantidad posible de direcciones a la lista privilegiada.

3. Opcionalmente, seleccione ***Permitir que las direcciones IP privilegiadas accedan a los puertos internos de StorageGRID ***. Ver ["Puertos internos de StorageGRID"](#) .



Esta opción elimina algunas protecciones para los servicios internos. Déjelo deshabilitado si es posible.

4. Seleccione **Guardar**.

Gestionar el acceso externo

Cuando se cierra un puerto en la pestaña Administrar acceso externo, ninguna dirección IP que no sea de la red podrá acceder al puerto a menos que agregue la dirección IP a la lista de direcciones privilegiadas. Solo puedes cerrar puertos que estén abiertos de forma predeterminada y solo puedes abrir puertos que hayas cerrado.



Las configuraciones en la pestaña Administrar acceso externo no pueden anular las configuraciones en la pestaña Red de cliente no confiable. Por ejemplo, si un nodo no es confiable, el puerto SSH/22 se bloquea en la red del cliente incluso si está abierto en la pestaña Administrar acceso externo. Las configuraciones en la pestaña Red de cliente no confiable anulan los puertos cerrados (como 443, 8443, 9443) en la red del cliente.

Pasos

1. Seleccione **Administrar acceso externo**. La pestaña muestra una tabla con todos los puertos externos (puertos a los que pueden acceder los nodos que no pertenecen a la red de manera predeterminada) para los nodos de su red.
2. Configure los puertos que desea abrir y cerrar utilizando las siguientes opciones:
 - Utilice el interruptor junto a cada puerto para abrir o cerrar el puerto seleccionado.
 - Seleccione **Abrir todos los puertos mostrados** para abrir todos los puertos enumerados en la tabla.
 - Seleccione **Cerrar todos los puertos mostrados** para cerrar todos los puertos enumerados en la tabla.



Si cierra los puertos 443 o 8443 de Grid Manager, todos los usuarios que estén conectados actualmente en un puerto bloqueado, incluido usted, perderán el acceso a Grid Manager a menos que su dirección IP se haya agregado a la lista de direcciones privilegiadas.



Utilice la barra de desplazamiento en el lado derecho de la tabla para asegurarse de haber visto todos los puertos disponibles. Utilice el campo de búsqueda para encontrar la configuración de cualquier puerto externo ingresando un número de puerto. Puede ingresar un número de puerto parcial. Por ejemplo, si ingresa un **2**, se mostrarán todos los puertos que tengan la cadena "2" como parte de su nombre.

3. Seleccione **Guardar**

Red de clientes no confiables

Si la red de cliente de un nodo no es confiable, el nodo solo acepta tráfico entrante en los puertos configurados como puntos finales del balanceador de carga y, opcionalmente, puertos adicionales que seleccione en esta pestaña. También puede utilizar esta pestaña para especificar la configuración predeterminada para los nuevos nodos agregados en una expansión.



Las conexiones de cliente existentes podrían fallar si no se han configurado los puntos finales del balanceador de carga.

Los cambios de configuración que realice en la pestaña **Red de cliente no confiable** anulan las configuraciones de la pestaña **Administrar acceso externo**.

Pasos

1. Seleccione **Red de cliente no confiable**.
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.
 - **Confiable** (predeterminado): cuando se agrega un nodo en una expansión, su red de cliente es confiable.
 - **No confiable**: cuando se agrega un nodo en una expansión, su red de cliente no es confiable.

Según sea necesario, puede regresar a esta pestaña para cambiar la configuración de un nuevo nodo específico.



Esta configuración no afecta a los nodos existentes en su sistema StorageGRID .

3. Utilice las siguientes opciones para seleccionar los nodos que deben permitir conexiones de clientes solo en puntos finales del balanceador de carga configurados explícitamente o en puertos seleccionados adicionales:
 - Seleccione **No confiar en los nodos mostrados** para agregar todos los nodos que se muestran en la tabla a la lista de Red de clientes no confiables.
 - Seleccione **Confiar en los nodos mostrados** para eliminar todos los nodos que se muestran en la tabla de la lista Red de clientes no confiables.
 - Utilice el interruptor junto a cada nodo para configurar la red del cliente como confiable o no confiable para el nodo seleccionado.

Por ejemplo, puede seleccionar **No confiar en los nodos mostrados** para agregar todos los nodos a la lista de Red de clientes no confiables y luego usar el botón junto a un nodo individual para agregar ese único nodo a la lista de Red de clientes confiables.



Utilice la barra de desplazamiento en el lado derecho de la tabla para asegurarse de haber visto todos los nodos disponibles. Utilice el campo de búsqueda para encontrar la configuración de cualquier nodo ingresando el nombre del nodo. Puede introducir un nombre parcial. Por ejemplo, si ingresa un **GW**, se mostrarán todos los nodos que tengan la cadena "GW" como parte de su nombre.

4. Seleccione **Guardar**.

La nueva configuración del firewall se aplica y se ejecuta de inmediato. Las conexiones de cliente existentes podrían fallar si no se han configurado los puntos finales del balanceador de carga.

Administrar inquilinos

¿Qué son las cuentas de inquilinos?

Una cuenta de inquilino le permite utilizar la API REST de Simple Storage Service (S3) para almacenar y recuperar objetos en un sistema StorageGRID .



Se han eliminado los detalles rápidos de esta versión del sitio de documentación. Ver ["StorageGRID 11.8: Administrar inquilinos"](#) .

Como administrador de la red, usted crea y administra las cuentas de inquilino que los clientes S3 usan para

almacenar y recuperar objetos.

Cada cuenta de inquilino tiene grupos federados o locales, usuarios, depósitos S3 y objetos.

Las cuentas de inquilino se pueden utilizar para segregar objetos almacenados por diferentes entidades. Por ejemplo, se pueden utilizar varias cuentas de inquilino para cualquiera de estos casos de uso:

- **Caso de uso empresarial:** si está administrando un sistema StorageGRID en una aplicación empresarial, es posible que desee segregar el almacenamiento de objetos de la red por los diferentes departamentos de su organización. En este caso, podría crear cuentas de inquilino para el departamento de Marketing, el departamento de Atención al Cliente, el departamento de Recursos Humanos, etc.



Si utiliza el protocolo de cliente S3, puede usar depósitos S3 y políticas de depósitos para segregar objetos entre los departamentos de una empresa. No es necesario utilizar cuentas de inquilino. Consulte las instrucciones para la implementación "[Cubos S3 y políticas de cubos](#)" Para más información.

- **Caso de uso de 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 alquilarán el almacenamiento en su red. En este caso, crearía cuentas de inquilino para la Empresa A, la Empresa B, la Empresa C, etc.

Para obtener más información, consulte "[Utilice una cuenta de inquilino](#)".

¿Cómo creo una cuenta de inquilino?

Utilice el administrador de Grid para crear una cuenta de inquilino. Al crear una cuenta de inquilino, se especifica la siguiente información:

- Información básica que incluye el nombre del inquilino, el tipo de cliente (S3) y la cuota de almacenamiento opcional.
- Permisos para la cuenta de inquilino, como si la cuenta de inquilino puede usar servicios de la plataforma S3, configurar su propia fuente de identidad, usar S3 Select o usar una conexión de federación de red.
- El acceso raíz inicial para el inquilino, en función de si el sistema StorageGRID utiliza grupos y usuarios locales, federación de identidad o inicio de sesión único (SSO).

Además, puede habilitar la configuración de Bloqueo de objetos S3 para el sistema StorageGRID si las cuentas de inquilinos S3 deben cumplir con requisitos reglamentarios. Cuando el bloqueo de objetos S3 está habilitado, todas las cuentas de inquilinos de S3 pueden crear y administrar depósitos compatibles.

¿Para qué se utiliza Tenant Manager?

Después de crear la cuenta de inquilino, los usuarios inquilinos pueden iniciar sesión en el Administrador de inquilinos para realizar tareas como las siguientes:

- Configurar la federación de identidad (a menos que la fuente de identidad se comparta con la red)
- Administrar grupos y usuarios
- Utilice la federación de red para la clonación de cuentas y la replicación entre redes
- Administrar claves de acceso S3
- Crear y administrar depósitos S3
- Utilice los servicios de la plataforma S3

- Utilice S3 Select
- Monitorear el uso del almacenamiento



Si bien los usuarios inquilinos de S3 pueden crear y administrar claves de acceso y depósitos de S3 con el Administrador de inquilinos, deben usar una aplicación cliente de S3 para ingerir y administrar objetos. Ver "[Utilice la API REST de S3](#)" Para más detalles.

Crear una cuenta de inquilino

Debe crear al menos una cuenta de inquilino para controlar el acceso al almacenamiento en su sistema StorageGRID .

Los pasos para crear una cuenta de inquilino varían según 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 inquilino pertenece a un grupo de administradores con permiso de acceso raíz.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)" .
- Tú tienes el "[Permiso de acceso de root o de cuentas de inquilino](#)" .
- Si la cuenta del inquilino utilizará la fuente de identidad que se configuró para Grid Manager y desea otorgar permiso de acceso raíz para la cuenta del inquilino a un grupo federado, debe importar ese grupo federado a Grid Manager. No es necesario asignar ningún permiso de administrador de cuadrícula a este grupo de administradores. Ver "[Administrar grupos de administradores](#)" .
- Si desea permitir que un inquilino de S3 clone datos de cuenta y replique objetos de bucket a otra red mediante una conexión de federación de red:
 - Tienes "[configuró la conexión de la federación de red](#)" .
 - El estado de la conexión es **Conectado**.
 - Tienes permiso de acceso root.
 - Has revisado las consideraciones para "[Gestión de los inquilinos permitidos para la federación de red](#)" .
 - Si la cuenta del inquilino utilizará la fuente de identidad que se configuró para Grid Manager, habrá importado el mismo grupo federado a Grid Manager en ambas redes.

Cuando cree el inquilino, seleccionará este grupo para que tenga el permiso de acceso raíz inicial para las cuentas de inquilino de origen y de destino.



Si este grupo de administración no existe en ambas cuadrículas antes de crear el inquilino, este no se replicará en el destino.

Acceder al asistente

Pasos

1. Seleccione **INQUILINOS**.
2. Seleccione **Crear**.

Introducir detalles

Pasos

1. Introduzca los detalles del inquilino.

Campo	Descripción
Nombre	Un nombre para la cuenta del inquilino. Los nombres de los inquilinos no necesitan ser únicos. Cuando se crea la cuenta de inquilino, recibe un ID de cuenta único de 20 dígitos.
Descripción (opcional)	Una descripción para ayudar a identificar al inquilino. Si está creando un inquilino que utilizará una conexión de federación de red, opcionalmente, utilice este campo para ayudar a identificar cuál es el inquilino de origen y cuál es el inquilino de destino. Por ejemplo, esta descripción para un inquilino creado en la Red 1 también aparecerá para el inquilino replicado en la Red 2: "Este inquilino fue creado en la Red 1".
Tipo de cliente	El tipo de protocolo de cliente que utilizará este inquilino, ya sea S3 o Swift . Nota: La compatibilidad con aplicaciones cliente Swift ha quedado obsoleta y se eliminará en una versión futura.
Cuota de almacenamiento (opcional)	Si desea que este inquilino tenga una cuota de almacenamiento, un valor numérico para la cuota y las unidades.

2. Seleccione **Continuar**.

Seleccionar permisos

Pasos

1. Opcionalmente, seleccione los permisos básicos que desea que tenga este inquilino.



Algunos de estos permisos tienen requisitos adicionales. Para obtener más detalles, seleccione el icono de ayuda para cada permiso.

Permiso	Si se selecciona...
Permitir servicios de plataforma	El inquilino puede utilizar servicios de la plataforma S3 como CloudMirror. Ver "Administrar servicios de plataforma para cuentas de inquilinos de S3" .
Utilice su propia fuente de identidad	El inquilino puede configurar y administrar su propia fuente de identidad para grupos y usuarios federados. Esta opción está deshabilitada si tiene "SSO configurado" para su sistema StorageGRID .

Permiso	Si se selecciona...
Permitir selección de S3	El inquilino puede emitir solicitudes de API S3 SelectObjectContent para filtrar y recuperar datos de objetos. Ver "Administrar S3 Select para cuentas de inquilinos" . Importante: Las solicitudes SelectObjectContent pueden disminuir el rendimiento del balanceador de carga para todos los clientes S3 y todos los inquilinos. Habilite esta función solo cuando sea necesario y solo para inquilinos de confianza.

2. Opcionalmente, seleccione los permisos avanzados que desea que tenga este inquilino.

Permiso	Si se selecciona...
Conexión de federación de red	El inquilino puede utilizar una conexión de federación de red, que: • Hace que este inquilino y todos los grupos de inquilinos y usuarios agregados a la cuenta se clonen desde esta cuadrícula (la <i>cuadrícula de origen</i>) a la otra cuadrícula en la conexión seleccionada (la <i>cuadrícula de destino</i>). • Permite que este inquilino configure la replicación entre redes entre los contenedores correspondientes en cada red. Ver "Gestionar los inquilinos permitidos para la federación de red" .
Bloqueo de objetos S3	Permitir que el inquilino utilice funciones específicas de S3 Object Lock: • Establecer período máximo de retención define durante cuánto tiempo se deben conservar los objetos nuevos agregados a este depósito, a partir del momento en que se ingieren. • Permitir modo de cumplimiento evita que los usuarios sobrescriban o eliminen versiones de objetos protegidos durante el período de retención.

3. Seleccione **Continuar**.

Definir el acceso raíz y crear un inquilino

Pasos

1. Defina el acceso raíz para la cuenta de inquilino, en función de si su sistema StorageGRID utiliza federación de identidad, inicio de sesión único (SSO) o ambos.

Opción	Haz esto
Si la federación de identidad no está habilitada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.

Opción	Haz esto
Si la federación de identidad está habilitada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si tanto la federación de identidad como el inicio de sesión único (SSO) están habilitados	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

2. Seleccione **Crear inquilino**.

Aparece un mensaje de éxito y el nuevo inquilino aparece en la página Inquilinos. Para saber cómo ver los detalles de los inquilinos y monitorear su actividad, consulte ["Supervisar la actividad de los inquilinos"](#).



La aplicación de la configuración de los inquilinos en toda la red podría demorar 15 minutos o más según la conectividad de la red, el estado del nodo y las operaciones de Cassandra.

3. Si seleccionó el permiso **Usar conexión de federación de red** para el inquilino:

- Confirme que se haya replicado un inquilino idéntico en la otra red en la conexión. Los inquilinos de ambas redes tendrán el mismo ID de cuenta de 20 dígitos, nombre, descripción, cuota y permisos.



Si ve el mensaje de error "Inquilino creado sin un clon", consulte las instrucciones en ["Solucionar errores de federación de red"](#).

- Si proporcionó una contraseña de usuario raíz local al definir el acceso raíz, ["cambiar la contraseña del usuario root local"](#) para el inquilino replicado.



Un usuario root local no puede iniciar sesión en Tenant Manager en la red de destino hasta que se cambie la contraseña.

Sign in en el inquilino (opcional)

Según sea necesario, puede iniciar sesión en el nuevo inquilino ahora para completar la configuración, o puede iniciar sesión en el inquilino más tarde. Los pasos para iniciar sesión dependen de si ha iniciado sesión en Grid Manager utilizando el puerto predeterminado (443) o un puerto restringido. Ver ["Controlar el acceso al firewall externo"](#).

Sign in ahora

Si estás usando...	Haz esto...
Puerto 443 y establece una contraseña para el usuario root local	1. Seleccione * Sign in como root*. Al iniciar sesión, aparecen enlaces para configurar depósitos, federación de identidad, grupos y usuarios. 2. Seleccione los enlaces para configurar la cuenta del inquilino. Cada enlace abre la página correspondiente en el Administrador de inquilinos. Para completar la página, consulte la "Instrucciones para usar cuentas de inquilinos".
Puerto 443 y no configuró una contraseña para el usuario root local	Seleccione * Sign in* e ingrese las credenciales de un usuario en el grupo federado de acceso raíz.
Un puerto restringido	1. Seleccionar Finalizar 2. Seleccione Restringido en la tabla de inquilinos para obtener más información sobre cómo acceder a esta cuenta de inquilino. La URL del Administrador de inquilinos tiene este formato: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> ◦ <code>`FQDN_or_Admin_Node_IP`</code> es un nombre de dominio completo o la dirección IP de un nodo de administración ◦ <code>`port`</code> es el puerto exclusivo para inquilinos ◦ <code>`20-digit-account-id`</code> es el ID de cuenta único del inquilino

Sign in más tarde

Si estás usando...	Haz uno de estos...
Puerto 443	• Desde el Administrador de red, seleccione INQUILINOS y seleccione * Sign in* a la derecha del nombre del inquilino. • Introduzca la URL del inquilino en un navegador web: <pre>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</pre> ◦ <code>`FQDN_or_Admin_Node_IP`</code> es un nombre de dominio completo o la dirección IP de un nodo de administración ◦ <code>`20-digit-account-id`</code> es el ID de cuenta único del inquilino

Si estás usando...	Haz uno de estos...
Un puerto restringido	• Desde el Administrador de red, seleccione INQUILINOS y seleccione Restringido. • Introduzca la URL del inquilino en un navegador web: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> ◦ <code>FQDN_or_Admin_Node_IP</code> es un nombre de dominio completo o la dirección IP de un nodo de administración ◦ <code>port</code> Es el puerto restringido solo para inquilinos? ◦ <code>20-digit-account-id</code> es el ID de cuenta único del inquilino

Configurar el inquilino

Siga las instrucciones en ["Utilice una cuenta de inquilino"](#) para administrar grupos de inquilinos y usuarios, claves de acceso S3, buckets, servicios de plataforma, clonación de cuentas y replicación entre redes.

Editar cuenta de inquilino

Puede editar una cuenta de inquilino para cambiar el nombre para mostrar, la cuota de almacenamiento o los permisos del inquilino.



Si un inquilino tiene el permiso **Usar conexión de federación de red**, puede editar los detalles del inquilino desde cualquiera de las redes en la conexión. Sin embargo, cualquier cambio que realice en una cuadrícula de la conexión no se copiará a la otra cuadrícula. Si desea mantener los detalles del inquilino exactamente sincronizados entre las cuadrículas, realice las mismas ediciones en ambas cuadrículas. Ver ["Administrar los inquilinos permitidos para la conexión de la federación de red"](#).

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso de root o de cuentas de inquilino"](#).



La aplicación de la configuración de los inquilinos en toda la red podría demorar 15 minutos o más según la conectividad de la red, el estado del nodo y las operaciones de Cassandra.

Pasos

1. Seleccione **INQUILINOS**.

Tenants

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

[Create](#)
[Export to CSV](#)
[Actions](#)

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

2. Localice la cuenta de inquilino que desea editar.

Utilice el cuadro de búsqueda para buscar un inquilino por nombre o ID de inquilino.

3. Seleccione el inquilino. Puede realizar cualquiera de las siguientes acciones:

- Seleccione la casilla de verificación del inquilino y seleccione **Acciones > Editar**.
- Seleccione el nombre del inquilino para mostrar la página de detalles y seleccione **Editar**.

4. Opcionalmente, cambie los valores de estos campos:

- **Nombre**
- **Descripción**
- **Cuota de almacenamiento**

5. Seleccione **Continuar**.

6. Seleccione o borre los permisos para la cuenta de inquilino.

- Si deshabilita los **Servicios de plataforma** para un inquilino que ya los está usando, los servicios que haya configurado para sus buckets 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 bucket S3, aún podrá almacenar objetos en el bucket, pero ya no se realizarán copias de esos objetos en el bucket S3 externo que ha configurado como punto final. Ver "[Administrar servicios de plataforma para cuentas de inquilinos de S3](#)".
- Cambie la configuración de **Usar fuente de identidad propia** para determinar si la cuenta del inquilino utilizará su propia fuente de identidad o la fuente de identidad que se configuró para Grid Manager.

Si **Utilizar fuente de identidad propia** es:

- Deshabilitado y seleccionado, el inquilino ya ha habilitado su propia fuente de identidad. Un inquilino debe deshabilitar su fuente de identidad antes de poder usar la fuente de identidad que se configuró para Grid Manager.
- Deshabilitado y no seleccionado, SSO está habilitado para el sistema StorageGRID. El inquilino debe utilizar la fuente de identidad que se configuró para Grid Manager.

- Seleccione o desmarque el permiso **Permitir selección S3** según sea necesario. Ver "[Administrar S3 Select para cuentas de inquilinos](#)".
- Para eliminar el permiso **Usar conexión de federación de red**:
 - i. Seleccione la pestaña **Federación de red**.
 - ii. Seleccione **Quitar permiso**.
- Para agregar el permiso **Usar conexión de federación de red**:
 - i. Seleccione la pestaña **Federación de red**.
 - ii. Seleccione la casilla de verificación **Usar conexión de federación de red**.
 - iii. Opcionalmente, seleccione **Clonar usuarios y grupos locales existentes** para clonarlos en la red remota. Si lo desea, puede detener la clonación en curso o volver a intentar la clonación si algunos usuarios o grupos locales no pudieron ser clonados después de que se completó la última operación de clonación.
- Para establecer un período máximo de retención o permitir el modo de cumplimiento:



El bloqueo de objetos S3 debe estar habilitado en la cuadrícula antes de poder usar estas configuraciones.

- i. Seleccione la pestaña **Bloqueo de objeto S3**.
- ii. Para **Establecer período máximo de retención**, ingrese un valor y seleccione el período de tiempo en el menú desplegable.
- iii. Para **Permitir modo de cumplimiento**, seleccione la casilla de verificación.

Cambiar la contraseña del usuario root local del inquilino

Es posible que necesite cambiar la contraseña del usuario raíz local de un inquilino si el usuario raíz no puede acceder a la cuenta.

Antes de empezar

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

Acerca de esta tarea

Si el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID, el usuario raíz local no puede iniciar sesión en la cuenta del inquilino. Para realizar tareas de usuario root, los usuarios deben pertenecer a un grupo federado que tenga permiso de acceso root para el inquilino.

Pasos

1. Seleccione **INQUILINOS**.

Tenants

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

[Create](#)
[Export to CSV](#)
[Actions](#)

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

2. Seleccione la cuenta del inquilino. Puede realizar cualquiera de las siguientes acciones:
 - Seleccione la casilla de verificación del inquilino y seleccione **Acciones** > **Cambiar contraseña root**.
 - Seleccione el nombre del inquilino para mostrar la página de detalles y seleccione **Acciones** > **Cambiar contraseña root**.
3. Introduzca la nueva contraseña para la cuenta del inquilino.
4. Seleccione **Guardar**.

Eliminar cuenta de inquilino

Puede eliminar una cuenta de inquilino si desea eliminar permanentemente el acceso del inquilino al sistema.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#).
- Tienes [permisos de acceso específicos](#).
- Ha eliminado todos los depósitos y objetos S3 asociados con la cuenta del inquilino.
- Si al inquilino se le permite usar una conexión de federación de red, ha revisado las consideraciones para [eliminar un inquilino con el permiso Usar conexión de federación de red](#).

Pasos

1. Seleccione **INQUILINOS**.
2. Localice la cuenta o cuentas de inquilino que desea eliminar.

Utilice el cuadro de búsqueda para buscar un inquilino por nombre o ID de inquilino.
3. Para eliminar varios inquilinos, seleccione las casillas de verificación y seleccione **Acciones** > **Eliminar**.
4. Para eliminar un solo inquilino, realice una de las siguientes acciones:
 - Seleccione la casilla de verificación y seleccione **Acciones** > **Eliminar**.

- Seleccione el nombre del inquilino para mostrar la página de detalles y luego seleccione **Acciones > Eliminar**.

5. Seleccione **Sí**.

Administrar los servicios de la plataforma

¿Qué son los servicios de plataforma?

Los servicios de la plataforma incluyen la replicación de CloudMirror, notificaciones de eventos y el servicio de integración de búsqueda.

Si habilita los servicios de plataforma para las cuentas de inquilinos de S3, debe configurar su red para que los inquilinos puedan acceder a los recursos externos necesarios para usar estos servicios.

Replicación de CloudMirror

El servicio de replicación StorageGRID CloudMirror se utiliza para reflejar objetos específicos de un depósito StorageGRID a un destino externo especificado.

Por ejemplo, puede utilizar la replicación de CloudMirror para reflejar registros de clientes específicos en Amazon S3 y luego aprovechar los servicios de AWS para realizar análisis de sus datos.



La replicación de CloudMirror tiene algunas similitudes y diferencias importantes con la función de replicación entre redes. Para obtener más información, consulte "[Comparar la replicación entre redes y la replicación de CloudMirror](#)".



La replicación de CloudMirror no es compatible si el depósito de origen tiene habilitado el bloqueo de objetos S3.

Notificaciones

Las notificaciones de eventos por bucket se utilizan para enviar notificaciones sobre acciones específicas realizadas en objetos a un clúster externo de Kafka o Amazon Simple Notification Service especificado.

Por ejemplo, puede configurar alertas para que se envíen a los administradores sobre cada objeto agregado a un depósito, donde los objetos representan archivos de registro asociados con un evento crítico del sistema.



Si bien la notificación de eventos se puede configurar en un bucket con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos S3 (incluidos la fecha de retención y el estado de retención legal) de los objetos no se incluirán en los mensajes de notificación.

Servicio de integración de búsquedas

El servicio de integración de búsqueda se utiliza para enviar metadatos de objetos S3 a un índice Elasticsearch específico donde los metadatos se pueden buscar o analizar mediante el servicio externo.

Por ejemplo, puede configurar sus depósitos para enviar metadatos de objetos S3 a un servicio Elasticsearch remoto. Luego, puede usar Elasticsearch para realizar búsquedas en diferentes grupos y realizar análisis sofisticados de patrones presentes en los metadatos de sus objetos.



Si bien la integración de Elasticsearch se puede configurar en un bucket con S3 Object Lock habilitado, los metadatos de S3 Object Lock (incluidos Conservar hasta la fecha y el estado de Retención legal) de los objetos no se incluirán en los mensajes de notificación.

Los servicios de plataforma brindan a los inquilinos la posibilidad de utilizar recursos de almacenamiento externo, servicios de notificación y servicios de búsqueda o análisis con sus datos. Dado que la ubicación de destino de los servicios de la plataforma generalmente es externa a su implementación de StorageGRID, debe decidir si desea permitir que los inquilinos utilicen estos servicios. Si lo hace, debe habilitar el uso de los servicios de la plataforma cuando cree o edite cuentas de inquilinos. También debe configurar su red de manera que los mensajes de servicios de plataforma que generan los inquilinos puedan llegar a sus destinos.

Recomendaciones para el uso de los servicios de la plataforma

Antes de utilizar los servicios de la plataforma, tenga en cuenta las siguientes recomendaciones:

- Si un bucket S3 en el sistema StorageGRID tiene habilitadas tanto la versión como la replicación de CloudMirror, también debe habilitar la versión del bucket S3 para el punto final de destino. Esto permite que la replicación de CloudMirror genere versiones de objetos similares en el punto final.
- No debe utilizar más de 100 inquilinos activos con solicitudes S3 que requieran replicación, notificaciones e integración de búsqueda de CloudMirror. Tener más de 100 inquilinos activos puede generar un rendimiento más lento del cliente S3.
- Las solicitudes a un punto final que no se puedan completar se pondrán en cola hasta un máximo de 500 000 solicitudes. Este límite se comparte equitativamente entre los inquilinos activos. A los nuevos inquilinos se les permite exceder temporalmente este límite de 500.000 para que los inquilinos recién creados no sean penalizados injustamente.

Información relacionada

- ["Administrar los servicios de la plataforma"](#)
- ["Configurar los ajustes del proxy de almacenamiento"](#)
- ["Monitorear StorageGRID"](#)

Red y puertos para servicios de plataforma

Si permite que un inquilino de S3 utilice servicios de plataforma, debe configurar la red para la red a fin de garantizar que los mensajes de servicios de plataforma puedan entregarse a sus destinos.

Puede habilitar los servicios de plataforma para una cuenta de inquilino S3 cuando crea o actualiza la cuenta de inquilino. Si los servicios de plataforma están habilitados, el inquilino puede crear puntos finales que sirvan como destino para la replicación de CloudMirror, notificaciones de eventos o mensajes de integración de búsqueda desde sus depósitos S3. Estos mensajes de servicios de plataforma se envían desde los nodos de almacenamiento que ejecutan el servicio ADC a los puntos finales de destino.

Por ejemplo, los inquilinos pueden configurar los siguientes tipos de puntos finales de destino:

- Un clúster de Elasticsearch alojado localmente
- Una aplicación local que admite la recepción de mensajes de Amazon Simple Notification Service
- Un clúster de Kafka alojado localmente
- Un depósito S3 alojado localmente en la misma instancia o en otra instancia de StorageGRID

- Un punto final externo, como un punto final en Amazon Web Services.

Para garantizar que se puedan entregar los mensajes de servicios de la plataforma, debe configurar la red o las redes que contienen los nodos de almacenamiento de ADC. Debe asegurarse de que los siguientes puertos se puedan usar para enviar mensajes de servicios de plataforma a los puntos finales de destino.

De forma predeterminada, los mensajes de servicios de la plataforma se envían en los siguientes puertos:

- **80**: Para URI de puntos finales que comienzan con http (la mayoría de los puntos finales)
- **443**: Para URI de puntos finales que comienzan con https (la mayoría de los puntos finales)
- **9092**: Para URI de puntos finales que comienzan con http o https (solo puntos finales de Kafka)

Los inquilinos pueden especificar un puerto diferente cuando crean o editan un punto final.



Si se utiliza una implementación de StorageGRID como destino para la replicación de CloudMirror, es posible que se reciban mensajes de replicación en un puerto distinto de 80 o 443. Asegúrese de que el puerto que utiliza la implementación de StorageGRID de destino para S3 esté especificado en el punto final.

Si utiliza un servidor proxy no transparente, también debe ["configurar los ajustes del proxy de almacenamiento"](#) para permitir que se envíen mensajes a puntos finales externos, como un punto final en Internet.

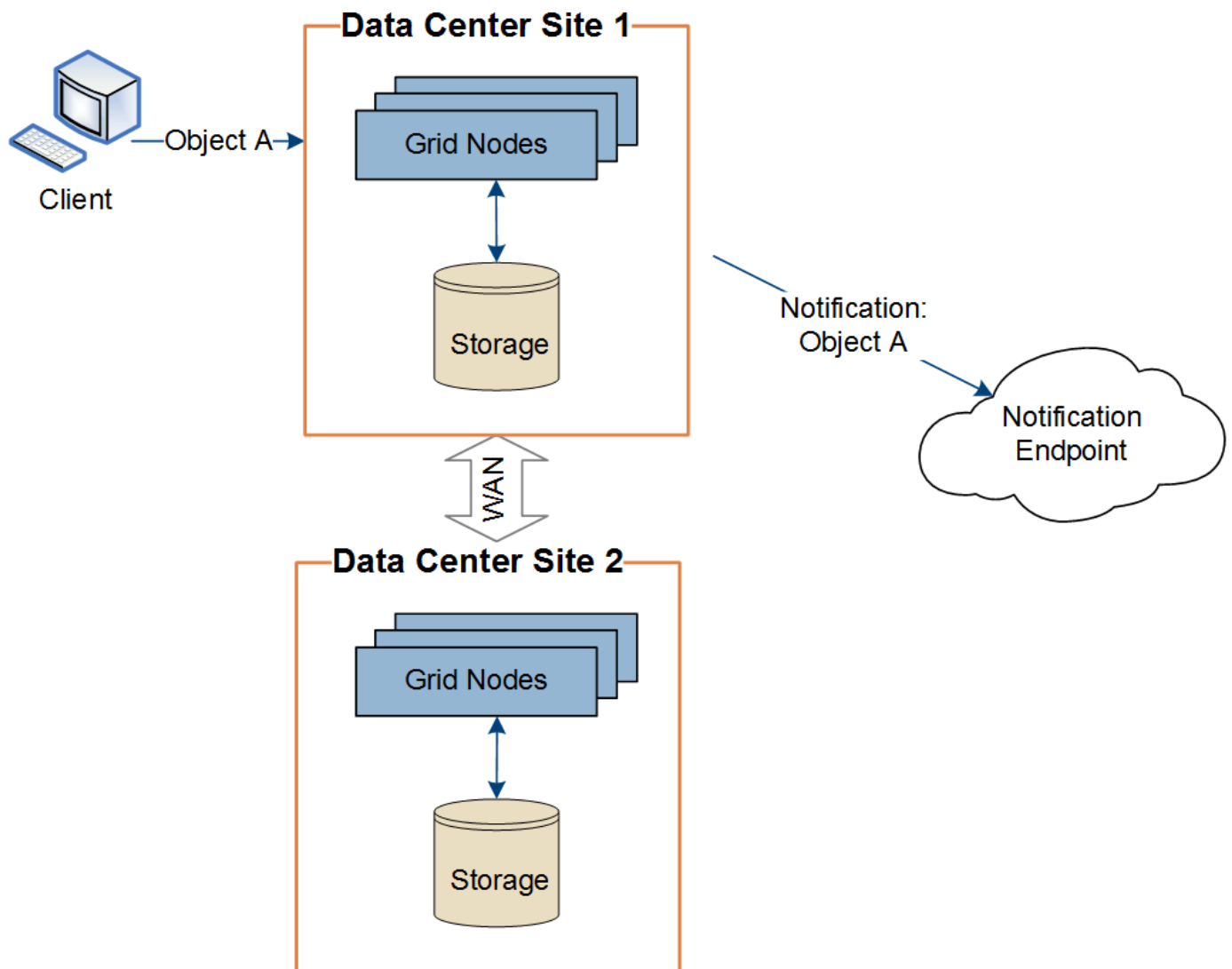
Información relacionada

["Utilice una cuenta de inquilino"](#)

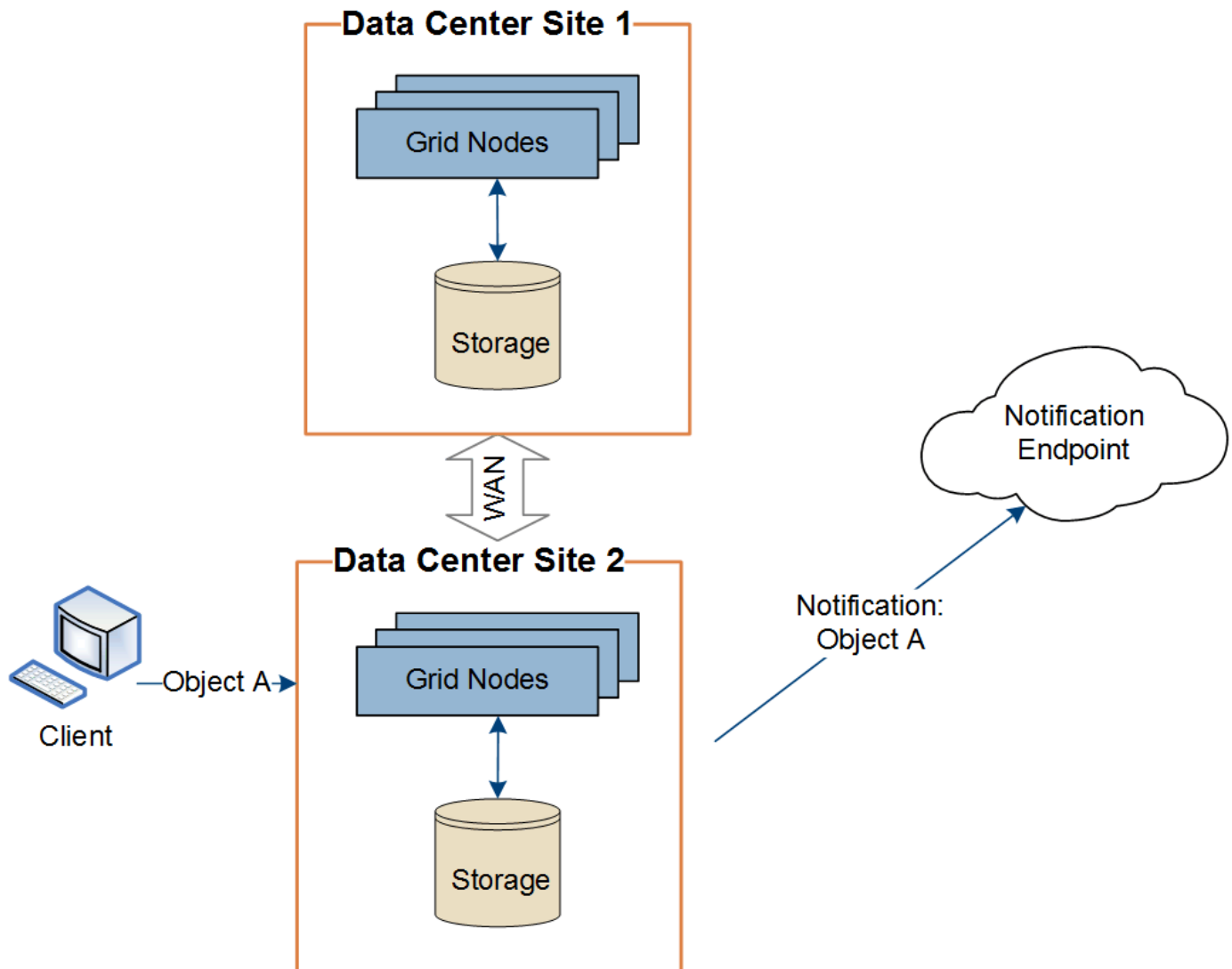
Entrega de mensajes de servicios de plataforma por sitio

Todas las operaciones de servicios de la plataforma se realizan sitio por sitio.

Es decir, si un inquilino utiliza un cliente para realizar una operación de creación de API S3 en un objeto conectándose a un nodo de puerta de enlace en el sitio del centro de datos 1, la notificación sobre esa acción se activa y se envía desde el sitio del centro de datos 1.



Si posteriormente el cliente realiza una operación de eliminación de API S3 en ese mismo objeto desde el sitio del centro de datos 2, la notificación sobre la acción de eliminación se activa y se envía desde el sitio del centro de datos 2.



Asegúrese de que la red en cada sitio esté configurada de manera tal que los mensajes de servicios de la plataforma puedan enviarse a sus destinos.

Solucionar problemas de servicios de la plataforma

Los puntos finales utilizados en los servicios de plataforma son creados y mantenidos por usuarios inquilinos en el Administrador de inquilinos; sin embargo, si un inquilino tiene problemas al configurar o usar los servicios de plataforma, es posible que pueda usar el Administrador de cuadrícula para ayudar a resolver el problema.

Problemas con los nuevos puntos finales

Antes de que un inquilino pueda utilizar los servicios de la plataforma, debe crear uno o más puntos finales mediante el Administrador de inquilinos. Cada punto final representa un destino externo para un servicio de plataforma, como un bucket S3 de StorageGRID, un bucket de Amazon Web Services, un tema de Amazon Simple Notification Service, un tema de Kafka o un clúster de Elasticsearch alojado localmente o en AWS. Cada punto final incluye tanto la ubicación del recurso externo como las credenciales necesarias para acceder a ese recurso.

Cuando un inquilino crea un punto final, el sistema StorageGRID valida que el punto final exista y que se pueda acceder a él utilizando las credenciales especificadas. La conexión al punto final se valida desde un

nodo en cada sitio.

Si falla la validación del punto final, aparecerá un mensaje de error que explica por qué. El usuario inquilino debe resolver el problema y luego intentar crear el punto final nuevamente.



La creación del punto final fallará si los servicios de la plataforma no están habilitados para la cuenta del inquilino.

Problemas con los puntos finales existentes

Si se produce un error cuando StorageGRID intenta acceder a un punto final existente, se muestra un mensaje en el panel 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 inquilinos pueden ir a la página Puntos finales para revisar el mensaje de error más reciente de cada punto final y determinar cuánto tiempo hace que ocurrió el error. La columna **Último error** muestra el mensaje de error más reciente para cada punto final e indica cuánto tiempo hace que ocurrió el error. Errores que incluyen el El icono apareció en los últimos 7 días.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

One or more endpoints have experienced an error. Select the endpoint for more details about the error. Meanwhile, the platform service request will be retried automatically.

5 endpoints Create endpoint

Delete endpoint

☐	Display name	Last error	Type	URI	URN
☐	my-endpoint-2	2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es::mydomain/sveloso/_doc
☐	my-endpoint-3	3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
☐	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
☐	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
☐	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1



Algunos mensajes de error en la columna **Último error** pueden incluir un ID de registro entre paréntesis. Un administrador de red o soporte técnico puede usar esta ID para localizar información más detallada sobre el error en bycast.log.

Problemas relacionados con los servidores proxy

Si ha configurado un "proxy de almacenamiento" Entre los nodos de almacenamiento y los puntos finales del servicio de la plataforma, pueden ocurrir errores si su servicio proxy no permite mensajes de StorageGRID. Para resolver estos problemas, verifique la configuración de su servidor proxy para asegurarse de que los mensajes relacionados con el servicio de la plataforma no estén bloqueados.

Determinar si se ha producido un error

Si se produjo algún error en los puntos finales durante los últimos 7 días, el panel del Administrador de inquilinos mostrará un mensaje de alerta. Puede ir a la página de Puntos finales para ver más detalles sobre el error.

Las operaciones del cliente fallan

Algunos problemas con los servicios de la plataforma podrían provocar que las operaciones del cliente en el bucket S3 fallen. Por ejemplo, las operaciones del cliente S3 fallarán si el servicio de máquina de estado replicada (RSM) interno se detiene o si hay demasiados mensajes de servicios de plataforma en cola para su entrega.

Para comprobar el estado de los servicios:

1. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
2. Seleccione **síto > Nodo de almacenamiento > SSM > Servicios**.

Errores de punto final recuperables e irrecuperables

Una vez creados los puntos finales, pueden producirse errores en las solicitudes de servicio de la plataforma por diversos motivos. Algunos errores se pueden recuperar con la intervención del usuario. Por ejemplo, podrían producirse errores recuperables por las siguientes razones:

- Las credenciales del usuario han sido eliminadas o han expirado.
- El depósito de destino no existe.
- No se puede entregar la notificación.

Si StorageGRID encuentra un error recuperable, se volverá a intentar la solicitud del servicio de la plataforma hasta que tenga éxito.

Otros errores son irrecuperables. Por ejemplo, se produce un error irrecuperable si se elimina el punto final.

Si StorageGRID encuentra un error de punto final irrecuperable:

- En el Administrador de cuadrícula, vaya a **Soporte > Herramientas > Métricas > Grafana > Descripción general de los servicios de plataforma** para ver los detalles del error.
- En el Administrador de inquilinos, vaya a **ALMACENAMIENTO (S3) > Puntos finales de servicios de plataforma** para ver los detalles del error.
- Compruebe el `/var/local/log/bycast-err.log` para errores relacionados. Los nodos de almacenamiento que tienen el servicio ADC contienen este archivo de registro.

No se pueden entregar los mensajes de servicios de la plataforma

Si el destino encuentra un problema que le impide aceptar mensajes de servicios de plataforma, la operación del cliente en el depósito se realiza correctamente, pero el mensaje de servicios de plataforma no se entrega.

Por ejemplo, este error podría ocurrir si las credenciales se actualizan en el destino de tal manera que StorageGRID ya no puede autenticarse en el servicio de destino.

Compruebe si hay alertas relacionadas.

Rendimiento más lento para solicitudes de servicio de la plataforma

El software StorageGRID puede limitar las solicitudes S3 entrantes para un bucket si la velocidad a la que se envían las solicitudes excede la velocidad a la que el punto final de destino puede recibirlas. La limitación solo se produce cuando hay una acumulación de solicitudes en espera de ser enviadas al punto final de destino.

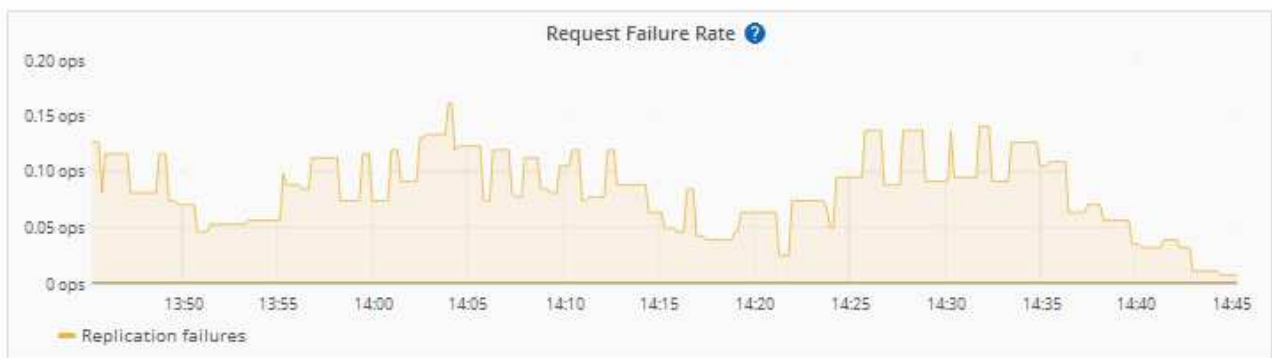
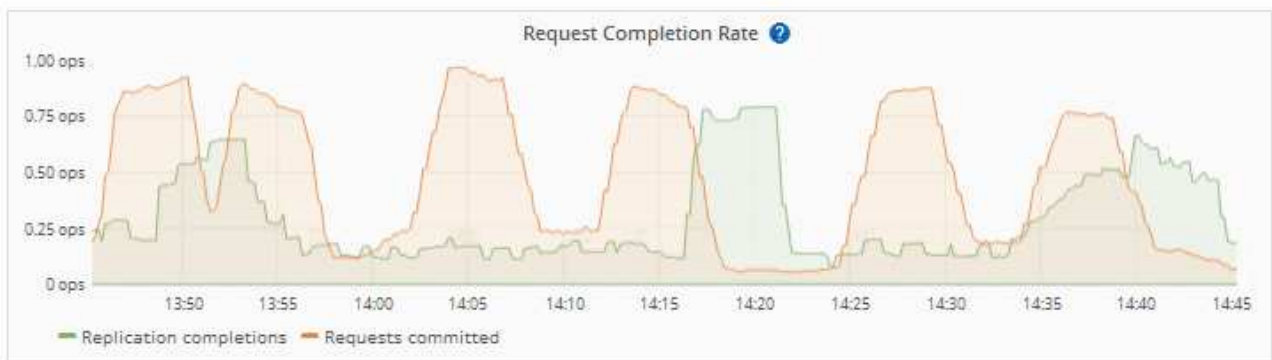
El único efecto visible es que las solicitudes S3 entrantes tardarán más en ejecutarse. Si comienza a detectar un rendimiento significativamente más lento, debe reducir la tasa de ingesta o utilizar un punto final con mayor capacidad. Si la acumulación de solicitudes continúa creciendo, las operaciones S3 del cliente (como las solicitudes PUT) eventualmente fallarán.

Es más probable que las solicitudes de CloudMirror se vean afectadas por el rendimiento del punto final de destino porque estas solicitudes generalmente implican 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 fallas de solicitudes para los servicios de la plataforma:

1. Seleccione **NODOS**.
2. Seleccione **site > Servicios de plataforma**.
3. Vea el gráfico de tasa de error 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 muy pocos 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 puntos finales.

Para resolver esta alerta, determine qué nodos de almacenamiento en el sitio incluyen el servicio RSM. (El servicio RSM está presente en los nodos de almacenamiento que también incluyen el servicio ADC). Luego, asegúrese de que una mayoría simple de esos nodos de almacenamiento estén en ejecución y disponibles.



Si más de un nodo de almacenamiento que contiene el servicio RSM falla en un sitio, perderá todas las solicitudes de servicio de plataforma pendientes para ese sitio.

Guía adicional para la resolución de problemas de los puntos finales de los servicios de la plataforma

Para obtener información adicional, consulte [Usar una cuenta de inquilino](#) > [Solucionar problemas de puntos finales de servicios de la plataforma](#).

Información relacionada

["Solucionar problemas del sistema StorageGRID"](#)

Administrar S3 Select para cuentas de inquilinos

Puede permitir que determinados inquilinos de S3 utilicen 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 habilitar las búsquedas. También reduce el coste y la latencia de la recuperación de datos.

¿Qué es S3 Select?

S3 Select permite a los clientes S3 utilizar 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 características de S3 Select.

Consideraciones y requisitos para el uso de S3 Select

Requisitos de administración de la red

El administrador de la red debe otorgar a los inquilinos la capacidad de selección S3. Seleccione **Permitir selección S3** cuando ["creando un inquilino"](#) o ["editar un inquilino"](#).

Requisitos de formato de objeto

El objeto que desea consultar debe estar en uno de los siguientes formatos:

- **CSV.** Se puede utilizar tal cual o comprimido en archivos GZIP o BZIP2.
- **Parquet.** Requisitos adicionales para los objetos Parquet:
 - S3 Select solo admite la compresión en columnas mediante GZIP o Snappy. S3 Select no admite la compresión de objetos completos para objetos Parquet.
 - S3 Select no admite la salida Parquet. Debe especificar el formato de salida como CSV o JSON.
 - El tamaño máximo del grupo de filas sin comprimir es 512 MB.
 - Debe utilizar los tipos de datos especificados en el esquema del objeto.
 - No se pueden utilizar los tipos lógicos INTERVAL, JSON, LIST, TIME o UUID.

Requisitos del punto final

La solicitud SelectObjectContent debe enviarse a un ["Punto final del balanceador de carga de StorageGRID"](#).

Los nodos de administración y de puerta de enlace utilizados por el punto final deben ser uno de los siguientes:

- Un nodo de dispositivo de servicios
- Un nodo de software basado en VMware
- Un nodo de metal desnudo que ejecuta un kernel con cgroup v2 habilitado

Consideraciones generales

Las consultas no se pueden enviar directamente a los nodos de almacenamiento.



Las solicitudes de SelectObjectContent pueden disminuir el rendimiento del equilibrador de carga para todos los clientes S3 y todos los inquilinos. Habilite esta función solo cuando sea necesario y solo para inquilinos de confianza.

Ver el ["Instrucciones para utilizar S3 Select"](#) .

Para ver ["Gráficos de Grafana"](#) Para seleccionar operaciones a lo largo del tiempo, seleccione **SOPORTE > Herramientas > Métricas** en el Administrador de cuadrícula.

Configurar conexiones de cliente

Configurar conexiones de cliente S3

Como administrador de la red, usted administra las opciones de configuración que controlan cómo las aplicaciones cliente S3 se conectan a su sistema StorageGRID para almacenar y recuperar datos.



Se han eliminado los detalles rápidos de esta versión del sitio de documentación. Ver ["StorageGRID 11.8: Configurar conexiones de cliente S3 y Swift"](#) .

Tareas de configuración

1. Realice tareas previas requeridas en StorageGRID, según cómo la aplicación cliente se conectará a StorageGRID.

Tareas requeridas

Debes obtener:

- Direcciones IP
- Nombres de dominio
- Certificado SSL

Tareas opcionales

Opcionalmente, configure:

- Federación de identidades
- SSO

1. Utilice StorageGRID para obtener los valores que la aplicación necesita para conectarse a la red. Puede utilizar el asistente de configuración de S3 o configurar cada entidad StorageGRID manualmente. +

Utilice el asistente de configuración de S3

Siga los pasos del asistente de configuración de S3.

Configurar manualmente

1. Crear un grupo de alta disponibilidad
2. Crear un punto final del balanceador de carga
3. Crear una cuenta de inquilino
4. Crear bucket y claves de acceso
5. Configurar reglas y políticas de ILM

1. Utilice la aplicación S3 para completar la conexión a StorageGRID. Cree entradas DNS para asociar direcciones IP a cualquier nombre de dominio que planee utilizar.

Según sea necesario, realice configuraciones adicionales de la aplicación.

2. Realice tareas continuas en la aplicación y en StorageGRID para administrar y monitorear el almacenamiento de objetos a lo largo del tiempo.

Información necesaria para adjuntar StorageGRID a una aplicación cliente

Antes de poder conectar StorageGRID a una aplicación cliente S3, debe realizar pasos de configuración en StorageGRID y obtener cierto valor.

¿Qué valores necesito?

La siguiente tabla muestra los valores que debe configurar en StorageGRID y dónde la aplicación S3 y el servidor DNS utilizan esos valores.

Valor	Donde se configura el valor	Dónde se utiliza el valor
Direcciones IP virtuales (VIP)	StorageGRID > Grupo de alta disponibilidad	Entrada DNS
Puerto	StorageGRID > Punto final del balanceador de carga	Aplicación cliente
Certificado SSL	StorageGRID > Punto final del balanceador de carga	Aplicación cliente
Nombre del servidor (FQDN)	StorageGRID > Punto final del balanceador de carga	• Aplicación cliente • Entrada DNS
ID de clave de acceso S3 y clave de acceso secreta	StorageGRID > Inquilino y depósito	Aplicación cliente

Valor	Donde se configura el valor	Dónde se utiliza el valor
Nombre del cubo/contenedor	StorageGRID > Inquilino y depósito	Aplicación cliente

¿Cómo obtengo estos valores?

Dependiendo de sus necesidades, puede realizar cualquiera de las siguientes acciones para obtener la información que necesita:

- *Utilice el ["Asistente de configuración de S3"](#) *. El asistente de configuración de S3 le ayuda a configurar rápidamente los valores necesarios en StorageGRID y genera uno o dos archivos que puede usar al configurar la aplicación S3. El asistente lo guía a través de los pasos necesarios y lo ayuda a garantizar que su configuración se ajuste a las mejores prácticas de StorageGRID .



Si está configurando una aplicación S3, se recomienda utilizar el asistente de configuración S3 a menos que sepa que tiene requisitos especiales o que su implementación requerirá una personalización significativa.

- *Utilice el ["Asistente de configuración de FabricPool"](#) *. Similar al asistente de configuración de S3, el asistente de configuración de FabricPool lo ayuda a configurar rápidamente los valores requeridos y genera un archivo que puede usar cuando configura un nivel de nube de FabricPool en ONTAP.



Si planea utilizar StorageGRID como sistema de almacenamiento de objetos para un nivel de nube de FabricPool , se recomienda utilizar el asistente de configuración de FabricPool a menos que sepa que tiene requisitos especiales o que su implementación requerirá una personalización significativa.

- **Configurar elementos manualmente.** Si se conecta a una aplicación S3 y prefiere no utilizar el asistente de configuración S3, puede obtener los valores necesarios realizando la configuración manualmente. Siga estos pasos:
 - a. Configure el grupo de alta disponibilidad (HA) que desea utilizar para la aplicación S3. Ver ["Configurar grupos de alta disponibilidad"](#) .
 - b. Cree el punto final del equilibrador de carga que utilizará la aplicación S3. Ver ["Configurar los puntos finales del balanceador de carga"](#) .
 - c. Cree la cuenta de inquilino que utilizará la aplicación S3. Ver ["Crear una cuenta de inquilino"](#) .
 - d. Para un inquilino S3, inicie sesión en la cuenta del inquilino y genere una ID de clave de acceso y una clave de acceso secreta para cada usuario que accederá a la aplicación. Ver ["Crea tus propias claves de acceso"](#) .
 - e. Cree uno o más depósitos S3 dentro de la cuenta del inquilino. Para S3, consulte ["Crear un depósito S3"](#) .
 - f. Para agregar instrucciones de ubicación específicas para los objetos que pertenecen al nuevo inquilino o contenedor, cree una nueva regla ILM y active una nueva política ILM para usar esa regla. Ver ["Crear regla ILM"](#) y ["Crear una política ILM"](#) .

Seguridad para clientes S3

Las cuentas de inquilino de StorageGRID utilizan aplicaciones cliente S3 para guardar datos de objetos en StorageGRID. Debe revisar las medidas de seguridad implementadas para las aplicaciones cliente.

Resumen

La siguiente lista resume cómo se implementa la seguridad para la API REST de S3:

Seguridad de la conexión

TLS

Autenticación del servidor

Certificado de servidor X.509 firmado por la CA del sistema o certificado de servidor personalizado proporcionado por el administrador

Autenticación de cliente

ID de clave de acceso de la cuenta S3 y clave de acceso secreta

Autorización del cliente

Propiedad del depósito y todas las políticas de control de acceso aplicables

Cómo StorageGRID proporciona seguridad para las aplicaciones cliente

Las aplicaciones cliente S3 pueden conectarse al servicio Load Balancer en nodos de puerta de enlace o nodos de administración o directamente a nodos de almacenamiento.

- Los clientes que se conectan al servicio Load Balancer pueden usar HTTPS o HTTP, según cómo ["configurar el punto final del balanceador de carga"](#).

Se recomienda utilizar HTTPS para proporcionar una comunicación segura cifrada mediante TLS. Debe adjuntar un certificado de seguridad al punto final.

HTTP proporciona una comunicación menos segura y sin cifrar y solo debe usarse para redes que no sean de producción o de prueba.

- Los clientes que se conectan a los nodos de almacenamiento también pueden usar HTTPS o HTTP.

HTTPS es el predeterminado y se recomienda.

HTTP proporciona una comunicación menos segura y sin cifrar, pero puede ser opcional. ["activado"](#) para redes que no sean de producción o de prueba.

- Las comunicaciones entre StorageGRID y el cliente están cifradas mediante TLS.
- Las comunicaciones entre el servicio Load Balancer y los nodos de almacenamiento dentro de la red están cifradas independientemente de si el punto final del balanceador de carga está configurado para aceptar conexiones HTTP o HTTPS.
- Los clientes deben suministrar ["Encabezados de autenticación HTTP"](#) a StorageGRID para realizar operaciones de API REST.

Certificados de seguridad y aplicaciones cliente

En todos los casos, las aplicaciones cliente pueden realizar conexiones TLS utilizando un certificado de servidor personalizado cargado por el administrador de la red o un certificado generado por el sistema StorageGRID :

- Cuando las aplicaciones cliente se conectan al servicio Load Balancer, utilizan el certificado que se configuró para el punto final del balanceador de carga. Cada punto final del equilibrador de carga tiene su propio certificado: un certificado de servidor personalizado cargado por el administrador de la red o un

certificado que el administrador de la red generó en StorageGRID al configurar el punto final.

Ver "[Consideraciones para el equilibrio de carga](#)".

- Cuando las aplicaciones cliente se conectan directamente a un nodo de almacenamiento, utilizan los certificados de servidor generados por el sistema que se generaron para los nodos de almacenamiento cuando se instaló el sistema StorageGRID (que están firmados por la autoridad de certificación del sistema) o un único certificado de servidor personalizado que proporciona un administrador de la red para la red. Ver "[agregar un certificado API S3 personalizado](#)".

Los clientes deben configurarse para confiar en la autoridad de certificación que firmó el certificado que utilizan para establecer conexiones TLS.

Algoritmos de cifrado y hash compatibles con bibliotecas TLS

El sistema StorageGRID admite un conjunto de conjuntos de cifrado que las aplicaciones cliente pueden usar al establecer una sesión TLS. Para configurar cifrados, vaya a **CONFIGURACIÓN > Seguridad > Configuración de seguridad** y seleccione **Políticas TLS y SSH**.

Versiones compatibles de TLS

StorageGRID admite TLS 1.2 y TLS 1.3.



SSLv3 y TLS 1.1 (o versiones anteriores) ya no son compatibles.

Utilice el asistente de configuración de S3

Utilizar el asistente de configuración de S3: Consideraciones y requisitos

Puede utilizar el asistente de configuración de S3 para configurar StorageGRID como el sistema de almacenamiento de objetos para una aplicación S3.

Cuándo utilizar el asistente de configuración de S3

El asistente de configuración de S3 lo guía a través de cada paso de la configuración de StorageGRID para su uso con una aplicación S3. Como parte de completar el asistente, descargará archivos que puede usar para ingresar valores en la aplicación S3. Utilice el asistente para configurar su sistema más rápidamente y asegurarse de que sus configuraciones se ajusten a las mejores prácticas de StorageGRID.

Si tienes el "[Permiso de acceso root](#)" Puede completar el asistente de configuración de S3 cuando comience a utilizar StorageGRID Grid Manager o puede acceder al asistente y completarlo en cualquier momento posterior. Dependiendo de sus requisitos, también puede configurar algunos o todos los elementos necesarios manualmente y luego usar el asistente para reunir los valores que necesita una aplicación S3.

Antes de utilizar el asistente

Antes de utilizar el asistente, confirme que ha completado estos requisitos previos.

Obtener direcciones IP y configurar interfaces VLAN

Si configura un grupo de alta disponibilidad (HA), sabrá a qué nodos se conectará la aplicación S3 y qué red StorageGRID se utilizará. También sabe qué valores ingresar para el CIDR de subred, la dirección IP de puerta de enlace y las direcciones IP virtuales (VIP).

Si planea utilizar una LAN virtual para segregar el tráfico de la aplicación S3, ya ha configurado la interfaz

VLAN. Ver "[Configurar interfaces VLAN](#)".

Configurar la federación de identidades y el SSO

Si planea utilizar la federación de identidad o el inicio de sesión único (SSO) para su sistema StorageGRID, debe habilitar estas funciones. También sabe qué grupo federado debe tener acceso raíz para la cuenta de inquilino que utilizará la aplicación S3. Ver "[Utilizar la federación de identidades](#)" y "[Configurar el inicio de sesión único](#)".

Obtener y configurar nombres de dominio

Sabe qué nombre de dominio completo (FQDN) utilizar para StorageGRID. Las entradas del servidor de nombres de dominio (DNS) asignarán este FQDN a las direcciones IP virtuales (VIP) del grupo de alta disponibilidad que cree mediante el asistente.

Si planea utilizar solicitudes alojadas virtuales de estilo S3, debe tener "[nombres de dominio de punto final S3 configurados](#)". Se recomienda utilizar solicitudes de estilo alojado virtual.

Revisar los requisitos del balanceador de carga y del certificado de seguridad

Si planea utilizar el balanceador de carga StorageGRID, ha revisado las consideraciones generales para el balanceo de carga. Tienes los certificados que cargarás o los valores que necesitas para generar un certificado.

Si planea utilizar un punto final de balanceador de carga externo (de terceros), debe tener el nombre de dominio completo (FQDN), el puerto y el certificado para ese balanceador de carga.

Configurar cualquier conexión de federación de red

Si desea permitir que el inquilino de S3 clone datos de cuenta y replique objetos de bucket a otra red mediante una conexión de federación de red, confirme lo siguiente antes de iniciar el asistente:

- Tienes "[configuró la conexión de la federación de red](#)".
- El estado de la conexión es **Conectado**.
- Tienes permiso de acceso root.

Acceda y complete el asistente de configuración de S3

Puede utilizar el asistente de configuración de S3 para configurar StorageGRID para su uso con una aplicación S3. El asistente de configuración proporciona los valores que la aplicación necesita para acceder a un depósito StorageGRID y guardar objetos.

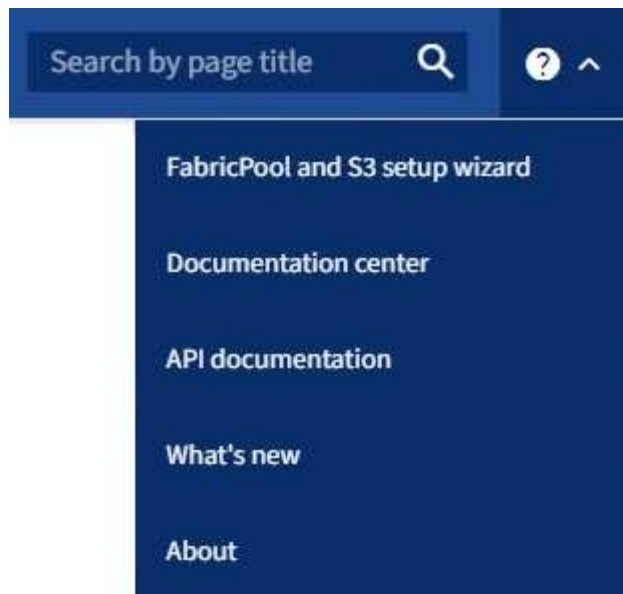
Antes de empezar

- Tú tienes el "[Permiso de acceso root](#)".
- Usted ha revisado el "[Consideraciones y requisitos](#)" para utilizar el asistente.

Acceder al asistente

Pasos

1. Sign in en Grid Manager usando un "[navegador web compatible](#)".
2. Si aparece el banner **Asistente de configuración de FabricPool y S3** en el panel, seleccione el enlace en el banner. Si el banner ya no aparece, seleccione el ícono de ayuda en la barra de encabezado en el Administrador de cuadrícula y seleccione **Asistente de configuración de FabricPool y S3**.



3. En la sección de aplicación S3 de la página del asistente de configuración de FabricPool y S3, seleccione **Configurar ahora**.

Paso 1 de 6: Configurar el grupo de alta disponibilidad

Un grupo de alta disponibilidad es una colección de nodos que contienen cada uno el servicio StorageGRID Load Balancer. Un grupo de alta disponibilidad puede contener nodos de puerta de enlace, nodos de administración o ambos.

Puede utilizar un grupo HA para ayudar a mantener disponibles las conexiones de datos S3. Si la interfaz activa en el grupo HA falla, una interfaz de respaldo puede administrar la carga de trabajo con poco impacto en las operaciones de S3.

Para obtener más detalles sobre esta tarea, consulte ["Administrar grupos de alta disponibilidad"](#).

Pasos

1. Si planea utilizar un balanceador de carga externo, no necesita crear un grupo de alta disponibilidad. Seleccione **Omitir este paso** y vaya a [Paso 2 de 6: Configurar el punto final del balanceador de carga](#).
2. Para utilizar el equilibrador de carga StorageGRID, puede crear un nuevo grupo de HA o utilizar un grupo de HA existente.

Crear un grupo de alta disponibilidad

- Para crear un nuevo grupo de HA, seleccione **Crear grupo de HA**.
- Para el paso **Ingresar detalles**, complete los siguientes campos.

Campo	Descripción
Nombre del grupo HA	Un nombre para mostrar único para este grupo HA.
Descripción (opcional)	La descripción de este grupo HA.

- Para el paso **Agregar interfaces**, seleccione las interfaces de nodo que desea utilizar en este grupo de HA.

Utilice los encabezados de columna para ordenar las filas o ingrese un término de búsqueda para localizar interfaces más rápidamente.

Puede seleccionar uno o más nodos, pero solo puede seleccionar una interfaz para cada nodo.

- Para el paso **Priorizar interfaces**, determine la interfaz principal y cualquier interfaz de respaldo para este grupo de HA.

Arrastre filas para cambiar los valores en la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra una falla.

Si el grupo HA incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se mueven a la primera interfaz de respaldo en el orden de prioridad. Si esa interfaz falla, las direcciones VIP pasan a la siguiente interfaz de respaldo, y así sucesivamente. Cuando se resuelven las fallas, las direcciones VIP vuelven a la interfaz de mayor prioridad disponible.

- Para el paso **Ingresar direcciones IP**, complete los siguientes campos.

Campo	Descripción
CIDR de subred	La dirección de la subred VIP en notación CIDR: una dirección IPv4 seguida de una barra 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 .
Dirección IP de la puerta de enlace (opcional)	Si las direcciones IP de S3 utilizadas para acceder a StorageGRID no están en la misma subred que las direcciones VIP de StorageGRID , ingrese la dirección IP de la puerta de enlace local VIP de StorageGRID . La dirección IP de la puerta de enlace local debe estar dentro de la subred VIP.

Campo	Descripción
Dirección IP virtual	Ingrese al menos una y no más de diez direcciones VIP para la interfaz activa en el grupo HA. Todas las direcciones VIP deben estar dentro de la subred VIP. Al menos una dirección debe ser IPv4. Opcionalmente, puede especificar direcciones IPv4 e IPv6 adicionales.

f. Seleccione **Crear grupo HA** y luego seleccione **Finalizar** para regresar al asistente de configuración de S3.

g. Seleccione **Continuar** para ir al paso del balanceador de carga.

Utilizar el grupo HA existente

a. Para utilizar un grupo de HA existente, seleccione el nombre del grupo de HA en **Seleccionar un grupo de HA**.

b. Seleccione **Continuar** para ir al paso del balanceador de carga.

Paso 2 de 6: Configurar el punto final del balanceador de carga

StorageGRID utiliza un equilibrador de carga para administrar la carga de trabajo de las aplicaciones cliente. El equilibrio de carga maximiza la velocidad y la capacidad de conexión en múltiples nodos de almacenamiento.

Puede utilizar el servicio StorageGRID Load Balancer, que existe en todos los nodos de puerta de enlace y de administración, o puede conectarse a un balanceador de carga externo (de terceros). Se recomienda utilizar el balanceador de carga StorageGRID .

Para obtener más detalles sobre esta tarea, consulte ["Consideraciones para el equilibrio de carga"](#) .

Para utilizar el servicio StorageGRID Load Balancer, seleccione la pestaña * StorageGRID load balancer* y luego cree o seleccione el punto final del balanceador de carga que desee utilizar. Para utilizar un balanceador de carga externo, seleccione la pestaña **Balanceador de carga externo** y proporcione detalles sobre el sistema que ya ha configurado.

Crear punto final

Pasos

1. Para crear un punto final de balanceador de carga, seleccione **Crear punto final**.
2. Para el paso **Ingresar detalles del punto final**, complete los siguientes campos.

Campo	Descripción
Nombre	Un nombre descriptivo para el punto final.
Puerto	El puerto StorageGRID que desea utilizar para equilibrar la carga. Este campo tiene como valor predeterminado 10433 para el primer punto final que cree, pero puede ingresar cualquier puerto externo no utilizado. Si ingresa 80 o 443, el punto final se configura solo en los nodos de puerta de enlace, porque estos puertos están reservados en los nodos de administración. Nota: No se permiten los puertos utilizados por otros servicios de red. Ver el "Referencia del puerto de red".
Tipo de cliente	Debe ser S3 .
Protocolo de red	Seleccione HTTPS. Nota: Se admite la comunicación con StorageGRID sin cifrado TLS, pero no se recomienda.

3. Para el paso **Seleccionar modo de enlace**, especifique el modo de enlace. El modo de enlace controla cómo se accede al punto final utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final utilizando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice la configuración Global (predeterminada) a menos que necesite restringir la accesibilidad de este punto final.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o FQDN correspondiente) de un grupo de HA para acceder a este punto final. Todos los puntos finales con este modo de enlace pueden usar el mismo número de puerto, siempre que los grupos de HA que seleccione para los puntos finales no se superpongan.
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.

Modo	Descripción
Tipo de nodo	Según el tipo de nodo que seleccione, los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este punto final.

4. Para el paso de acceso de inquilino, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (predeterminado)	Todas las cuentas de inquilinos pueden usar este punto final para acceder a sus depósitos.
Permitir inquilinos seleccionados	Solo las cuentas de inquilinos seleccionadas pueden usar este punto final para acceder a sus depósitos.
Bloquear inquilinos seleccionados	Las cuentas de inquilinos seleccionadas no pueden usar este punto final para acceder a sus depósitos. Todos los demás inquilinos pueden utilizar este punto final.

5. Para el paso **Adjuntar certificado**, seleccione una de las siguientes opciones:

Campo	Descripción
Subir certificado (recomendado)	Utilice esta opción para cargar un certificado de servidor firmado por una CA, una clave privada de certificado y un paquete de CA opcional.
Generar certificado	Utilice esta opción para generar un certificado autofirmado. Ver "Configurar los puntos finales del balanceador de carga" para obtener detalles de qué ingresar.
Utilice el certificado StorageGRID S3	Utilice esta opción solo si ya ha cargado o generado una versión personalizada del certificado global de StorageGRID . Ver "Configurar certificados de API S3" Para más detalles.

6. Seleccione **Finalizar** para regresar al asistente de configuración de S3.

7. Seleccione **Continuar** para ir al paso de inquilino y depósito.



Los cambios en un certificado de punto final pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Utilice el punto final del balanceador de carga existente

Pasos

1. Para utilizar un punto final existente, seleccione su nombre en **Seleccionar un punto final del balanceador de carga**.
2. Seleccione **Continuar** para ir al paso de inquilino y depósito.

Utilice un balanceador de carga externo

Pasos

1. Para utilizar un balanceador de carga externo, complete los siguientes campos.

Campo	Descripción
Nombre de dominio completo (FQDN)	El nombre de dominio completo (FQDN) del balanceador de carga externo.
Puerto	El número de puerto que utilizará la aplicación S3 para conectarse al balanceador de carga externo.
Certificado	Copie el certificado del servidor para el balanceador de carga externo y péguelo en este campo.

2. Seleccione **Continuar** para ir al paso de inquilino y depósito.

Paso 3 de 6: Crear inquilino y depósito

Un inquilino es una entidad que puede utilizar aplicaciones S3 para almacenar y recuperar objetos en StorageGRID. Cada inquilino tiene sus propios usuarios, claves de acceso, depósitos, objetos y un conjunto específico de capacidades.

Un bucket es un contenedor que se utiliza para almacenar objetos y metadatos de objetos de un inquilino. Aunque los inquilinos pueden tener muchos grupos, el asistente le ayuda a crear un inquilino y un grupo de la forma más rápida y sencilla. Si necesita agregar depósitos o configurar opciones más adelante, puede utilizar el Administrador de inquilinos.

Para obtener más detalles sobre esta tarea, consulte ["Crear una cuenta de inquilino"](#) y ["Crear un depósito S3"](#).

Pasos

1. Introduzca un nombre para la cuenta de inquilino.

Los nombres de los inquilinos no necesitan ser únicos. Cuando se crea la cuenta de inquilino, recibe un ID de cuenta numérico único.

2. Defina el acceso raíz para la cuenta de inquilino, en función de si su sistema StorageGRID utiliza ["federación de identidades"](#), ["inicio de sesión único \(SSO\)"](#), o ambos.

Opción	Haz esto
Si la federación de identidad no está habilitada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si la federación de identidad está habilitada	a. Seleccione un grupo federado existente para tener "Permiso de acceso root" para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.

Opción	Haz esto
Si tanto la federación de identidad como el inicio de sesión único (SSO) están habilitados	Seleccione un grupo federado existente para tener " Permiso de acceso root " para el inquilino. Ningún usuario local puede iniciar sesión.

- Si desea que el asistente cree la ID de clave de acceso y la clave de acceso secreta para el usuario raíz, seleccione **Crear clave de acceso S3 del usuario raíz automáticamente**.

Seleccione esta opción si el único usuario del inquilino será el usuario raíz. Si otros usuarios utilizarán este inquilino, "[utilizar el Administrador de inquilinos](#)" para configurar claves y permisos.

- Si desea crear un depósito para este inquilino ahora, seleccione **Crear depósito para este inquilino**.



Si el Bloqueo de objetos S3 está habilitado para la cuadrícula, el depósito creado en este paso no tendrá el Bloqueo de objetos S3 habilitado. Si necesita utilizar un depósito de bloqueo de objetos S3 para esta aplicación S3, no seleccione crear un depósito ahora. En su lugar, utilice el Administrador de inquilinos para "[crear el cubo](#)" más tarde.

- Introduzca el nombre del depósito que utilizará la aplicación S3. Por ejemplo, `s3-bucket`.

No puedes cambiar el nombre del depósito después de crearlo.

- Seleccione la **Región** para este bucket.

Utilice la región predeterminada (`us-east-1`) a menos que espere utilizar ILM en el futuro para filtrar objetos según la región del depósito.

- Seleccione **Crear y continuar**.

Paso 4 de 6: Descargar datos

En el paso de descarga de datos, puede descargar uno o dos archivos para guardar los detalles de lo que acaba de configurar.

Pasos

- Si seleccionó **Crear clave de acceso S3 de usuario raíz automáticamente**, realice una o ambas de las siguientes acciones:
 - Seleccione **Descargar claves de acceso** para descargar una `.csv` archivo que contiene el nombre de la cuenta del inquilino, el ID de la clave de acceso y la clave de acceso secreta.
 - Seleccione el icono de copia () para copiar el ID de la clave de acceso y la clave de acceso secreta al portapapeles.
- Seleccione **Descargar valores de configuración** para descargar un `.txt` archivo que contiene las configuraciones para el punto final del balanceador de carga, el inquilino, el depósito y el usuario raíz.
- Guarde esta información en un lugar seguro.



No cierre esta página hasta que haya copiado ambas claves de acceso. Las claves no estarán disponibles después de cerrar esta página. Asegúrese de guardar esta información en una ubicación segura porque puede usarse para obtener datos de su sistema StorageGRID.

4. Si se le solicita, seleccione la casilla de verificación para confirmar que ha descargado o copiado las claves.
5. Seleccione **Continuar** para ir al paso de reglas y políticas de ILM.

Paso 5 de 6: Revisar la regla y la política de ILM para S3

Las reglas de administración del ciclo de vida de la información (ILM) controlan la ubicación, la duración y el comportamiento de ingesta de todos los objetos en su sistema StorageGRID . La política ILM incluida con StorageGRID realiza dos copias replicadas de todos los objetos. Esta política estará vigente hasta que active al menos una nueva política.

Pasos

1. Revise la información proporcionada en la página.
2. Si desea agregar instrucciones específicas para los objetos que pertenecen al nuevo inquilino o depósito, cree una nueva regla y una nueva política. Ver "[Crear regla ILM](#)" y "[Utilice las políticas de ILM](#)".
3. Seleccione **He revisado estos pasos y entiendo lo que necesito hacer**.
4. Seleccione la casilla de verificación para indicar que comprende qué hacer a continuación.
5. Seleccione **Continuar** para ir a **Resumen**.

Paso 6 de 6: Revisar el resumen

Pasos

1. Revise el resumen.
2. Tome nota de los detalles en los próximos pasos, que describen la configuración adicional que podría ser necesaria antes de conectarse al cliente S3. Por ejemplo, si selecciona * Sign in como root*, accederá al Administrador de inquilinos, donde podrá agregar usuarios inquilinos, crear depósitos adicionales y actualizar la configuración de los depósitos.
3. Seleccione **Finalizar**.
4. Configure la aplicación utilizando el archivo que descargó de StorageGRID o los valores que obtuvo manualmente.

Administrar grupos de alta disponibilidad

¿Qué son los grupos de alta disponibilidad (HA)?

Los grupos de alta disponibilidad (HA) proporcionan conexiones de datos de alta disponibilidad para clientes S3 y conexiones de alta disponibilidad para Grid Manager y Tenant Manager.

Puede agrupar las interfaces de red de varios nodos de administración y de puerta de enlace en un grupo de alta disponibilidad (HA). Si la interfaz activa en el grupo HA falla, una interfaz de respaldo puede administrar la carga de trabajo.

Cada grupo HA proporciona acceso a los servicios compartidos en los nodos seleccionados.

- Los grupos de alta disponibilidad que incluyen nodos de puerta de enlace, nodos de administración o ambos proporcionan conexiones de datos de alta disponibilidad para clientes S3.
- Los grupos de HA que incluyen solo nodos de administración proporcionan conexiones de alta disponibilidad al Administrador de red y al Administrador de inquilinos.

- Un grupo de alta disponibilidad que incluye solo dispositivos de servicios y nodos de software basados en VMware puede proporcionar conexiones de alta disponibilidad para ["Inquilinos de S3 que utilizan S3 Select"](#) . Se recomiendan grupos HA cuando se utiliza S3 Select, pero no son obligatorios.

¿Cómo se crea un grupo HA?

1. Selecciona una interfaz de red para uno o más nodos de administración o nodos de puerta de enlace. Puede utilizar 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 se puede agregar una interfaz a un grupo HA si tiene una dirección IP asignada por DHCP.

2. Debe especificar una interfaz para que sea la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra una falla.
3. Usted determina el orden de prioridad para cualquier interfaz de respaldo.
4. Asigna de una a diez direcciones IP virtuales (VIP) al grupo. Las aplicaciones clientes pueden usar cualquiera de estas direcciones VIP para conectarse a StorageGRID.

Para obtener instrucciones, consulte ["Configurar grupos de alta disponibilidad"](#) .

¿Qué es la interfaz activa?

Durante el funcionamiento normal, todas las direcciones VIP del grupo HA se agregan a la interfaz principal, que es la primera interfaz en el orden de prioridad. Mientras la interfaz principal permanezca disponible, se utilizará cuando los clientes se conecten a cualquier dirección VIP del grupo. Es decir, durante el funcionamiento normal, la interfaz principal es la interfaz "activa" para el grupo.

De manera similar, durante el funcionamiento normal, cualquier interfaz de menor prioridad para el grupo HA actúa como interfaz de "respaldo". Estas interfaces de respaldo no se utilizan a menos que la interfaz principal (actualmente activa) deje de estar disponible.

Ver el estado actual del grupo HA de un nodo

Para ver si un nodo está asignado a un grupo de alta disponibilidad y determinar su estado actual, seleccione **NODOS > nodo**.

Si la pestaña **Descripción general** incluye una entrada para **Grupos de HA**, el nodo se asigna a los grupos de HA enumerados. El valor después del nombre del grupo es el estado actual del nodo en el grupo HA:

- **Activo:** El grupo HA está alojado actualmente en este nodo.
- **Copia de seguridad:** El grupo HA no está utilizando actualmente este nodo; esta es 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 detuvo manualmente.
- **Error:** El grupo HA no se puede alojar en este nodo debido a uno o más de los siguientes motivos:
 - 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 caído.

En este ejemplo, el nodo de administración principal se ha agregado a dos grupos de alta disponibilidad. Este nodo es actualmente la interfaz activa para el grupo de clientes de administración y una interfaz de respaldo para el grupo de clientes de FabricPool .

DC1-ADM1 (Primary Admin Node)

Overview

Hardware

Network

Storage

Load balancer

Tasks

Node information

Name:

DC1-ADM1

Type:

Primary Admin Node

ID:

ce00d9c8-8a79-4742-bdef-c9c658db5315

Connection state:

Connected

Software version:

11.6.0 (build 20211207.1804.614bc17)

HA groups:

Admin clients (Active)

FabricPool clients (Backup)

IP addresses:

172.16.1.225 - eth0 (Grid Network)

10.224.1.225 - eth1 (Admin Network)

47.47.0.2, 47.47.1.225 - eth2 (Client Network)

Show additional IP addresses

¿Qué sucede cuando falla la interfaz activa?

La interfaz que actualmente aloja 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 esa interfaz falla, las direcciones VIP pasan a la siguiente interfaz de respaldo disponible, y así sucesivamente.

La conmutación por error se puede activar por cualquiera de estos motivos:

- El nodo en el que está configurada la interfaz deja de funcionar.
- El nodo en el que está configurada la interfaz pierde conectividad con todos los demás nodos durante al menos 2 minutos.
- La interfaz activa deja de funcionar.
- El servicio Load Balancer se detiene.
- El servicio de Alta Disponibilidad se detiene.



Es posible que la conmutación por error no se active por fallas de red externas al nodo que aloja la interfaz activa. De manera similar, la conmutación por error no es activada por los servicios del Administrador de red o del Administrador de inquilinos.

El proceso de conmutación por error generalmente toma sólo unos segundos y es lo suficientemente rápido como para que las aplicaciones cliente experimenten poco impacto y puedan confiar en los comportamientos de reintento normales para continuar la operación.

Cuando se resuelve la falla y vuelve a estar disponible una interfaz de mayor prioridad, las direcciones VIP se mueven automáticamente a la interfaz de mayor prioridad que esté disponible.

¿Cómo se utilizan los grupos HA?

Puede utilizar grupos de alta disponibilidad (HA) para proporcionar conexiones de alta disponibilidad a StorageGRID para datos de objetos y para uso administrativo.

- Un grupo HA puede proporcionar conexiones administrativas de alta disponibilidad al administrador de red o al administrador de inquilinos.
- Un grupo HA puede proporcionar conexiones de datos de alta disponibilidad para clientes S3.
- Un grupo HA que contiene solo una interfaz le permite proporcionar muchas direcciones VIP y configurar explícitamente direcciones IPv6.

Un grupo de alta disponibilidad solo puede proporcionar alta disponibilidad si todos los nodos incluidos en el grupo brindan los mismos servicios. Al crear un grupo de alta disponibilidad, agregue interfaces de los tipos de nodos que brindan los servicios que necesita.

- **Nodos de administración:** incluye el servicio Load Balancer y habilita el acceso al Grid Manager o al Tenant Manager.
- **Nodos de puerta de enlace:** incluye el servicio Load Balancer.

Propósito del grupo HA	Agregue nodos de este tipo al grupo HA
Acceso al Administrador de Red	• Nodo de administración principal (Principal) • Nodos de administración no principales 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 únicamente al administrador de inquilinos	• Nodos de administración primarios o no primarios
Acceso de cliente S3: servicio Load Balancer	• Nodos de administración • Nodos de puerta de enlace
Acceso de cliente S3 para " S3 Seleccionar "	• Servicios de electrodomésticos • Nodos de software basados en VMware Nota: Se recomiendan grupos HA cuando se utiliza S3 Select, pero no son obligatorios.

Limitaciones del uso de grupos de alta disponibilidad con Grid Manager o Tenant Manager

Si falla un servicio de Grid Manager o Tenant Manager, no se activa la conmutación por error del grupo HA.

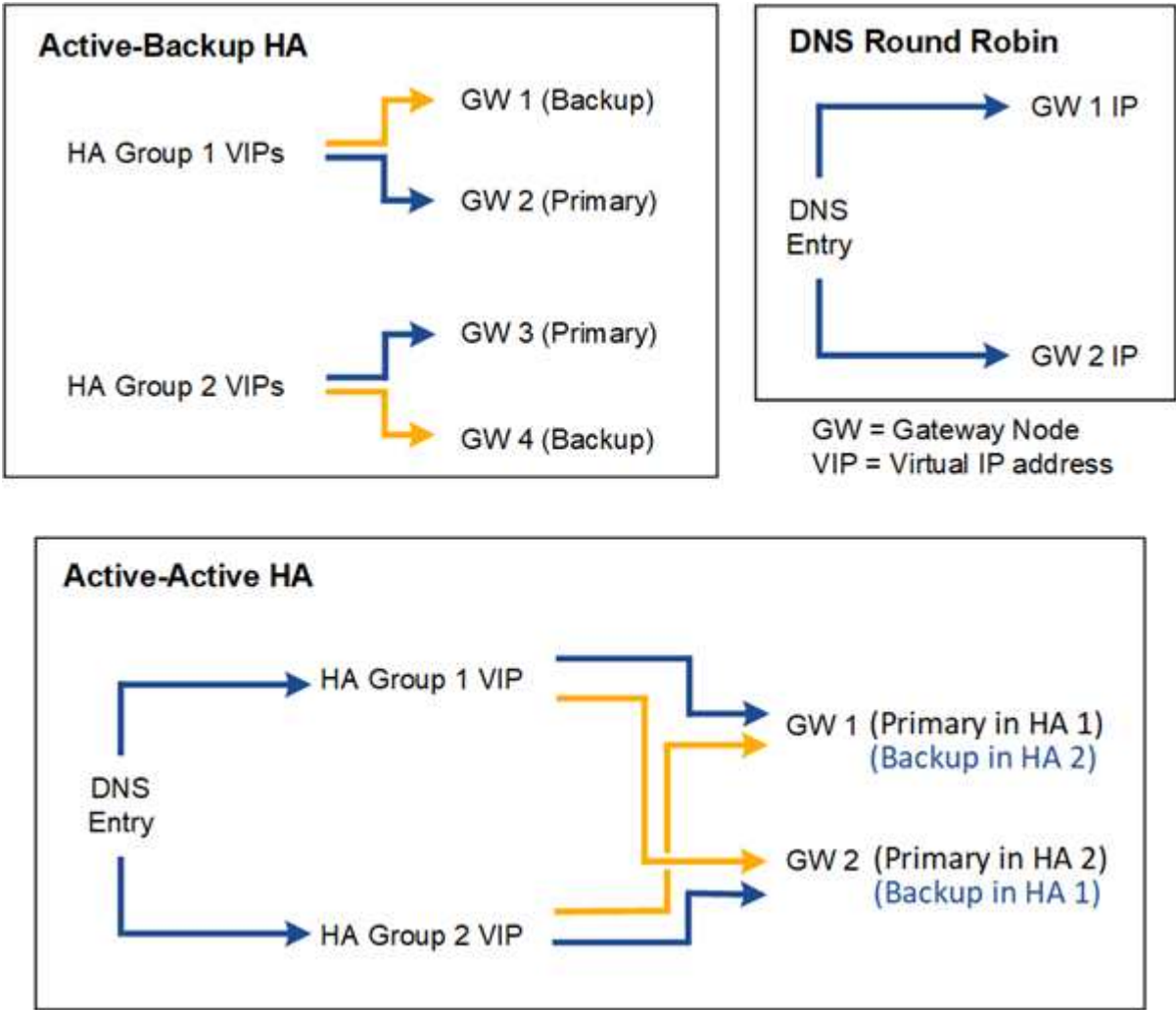
Si ha iniciado sesión en Grid Manager o Tenant Manager cuando se produce una conmutación por error, cerrará la sesión y deberá iniciar sesión nuevamente para reanudar su tarea.

Algunos procedimientos de mantenimiento no se pueden realizar cuando el nodo de administración principal no está disponible. Durante la conmutación por error, puede utilizar el Administrador de cuadrícula para supervisar su sistema StorageGRID .

Opciones de configuración para grupos de alta disponibilidad

Los siguientes diagramas proporcionan ejemplos de diferentes formas en las que se pueden configurar grupos de HA. Cada opción tiene ventajas y desventajas.

En los diagramas, el azul indica la interfaz principal en el grupo HA y el amarillo indica la interfaz de respaldo en el grupo HA.



La tabla resume los beneficios de cada configuración de HA que se muestra en el diagrama.

Configuración	Ventajas	Desventajas
Alta disponibilidad de respaldo activo	• Administrado por StorageGRID sin dependencias externas. • Conmutación por error rápida.	• Solo un nodo en un grupo HA está activo. Al menos un nodo por grupo HA estará inactivo.

Configuración	Ventajas	Desventajas
DNS Round Robin	• Aumento del rendimiento agregado. • No hay hosts inactivos.	• Conmutación por error lenta, que podría depender del comportamiento del cliente. • Requiere configuración de hardware fuera de StorageGRID. • Necesita un control de salud implementado por el cliente.
HA activo-activo	• El tráfico se distribuye entre varios grupos de alta disponibilidad. • Alto rendimiento agregado que escala con la cantidad de grupos de HA. • Conmutación por error rápida.	• Más complejo de configurar. • Requiere configuración de hardware fuera de StorageGRID. • Necesita un control de salud implementado por el cliente.

Configurar grupos de alta disponibilidad

Puede configurar grupos de alta disponibilidad (HA) para proporcionar acceso de alta disponibilidad a los servicios en los nodos de administración o los nodos de puerta de enlace.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .
- Si planea utilizar una interfaz VLAN en un grupo HA, habrá creado la interfaz VLAN. Ver ["Configurar interfaces VLAN"](#) .
- Si planea utilizar una interfaz de acceso para un nodo en un grupo de alta disponibilidad, ha creado la interfaz:
 - **Red Hat Enterprise Linux (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Ubuntu o Debian (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Linux (después de instalar el nodo):** ["Linux: Agregar interfaces troncales o de acceso a un nodo"](#)
 - **VMware (después de instalar el nodo):** ["VMware: Agregar interfaces troncales o de acceso a un nodo"](#)

Crear un grupo de alta disponibilidad

Cuando se crea un grupo de alta disponibilidad, se selecciona una o más interfaces y se organizan en orden de prioridad. Luego, asigna una o más direcciones VIP al grupo.

Una interfaz debe ser para que un nodo de puerta de enlace o un nodo de administración se incluya en un grupo de alta disponibilidad. Un grupo de HA solo puede usar una interfaz para un nodo determinado; sin embargo, se pueden usar otras interfaces para el mismo nodo en otros grupos de HA.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad**.
2. Seleccione **Crear**.

Introduzca detalles para el grupo HA

Pasos

1. Proporcione un nombre único para el grupo HA.
2. Opcionalmente, ingrese una descripción para el grupo HA.
3. Seleccione **Continuar**.

Agregar interfaces al grupo HA

Pasos

1. Seleccione una o más interfaces para agregar a este grupo de HA.

Utilice los encabezados de columna para ordenar las filas o ingrese un término de búsqueda para localizar interfaces más rápidamente.

Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.

?

Total interface count: 4

	Node	Interface	Site	IPv4 subnet	Node type
☐	DC1-ADM1-104-96	eth0	DC1	10.96.104.0/22	Primary Admin Node
☐	DC1-ADM1-104-96	eth2	DC1	—	Primary Admin Node
☐	DC2-ADM1-104-103	eth0	DC2	10.96.104.0/22	Admin Node
☐	DC2-ADM1-104-103	eth2	DC2	—	Admin Node

0 interfaces selected



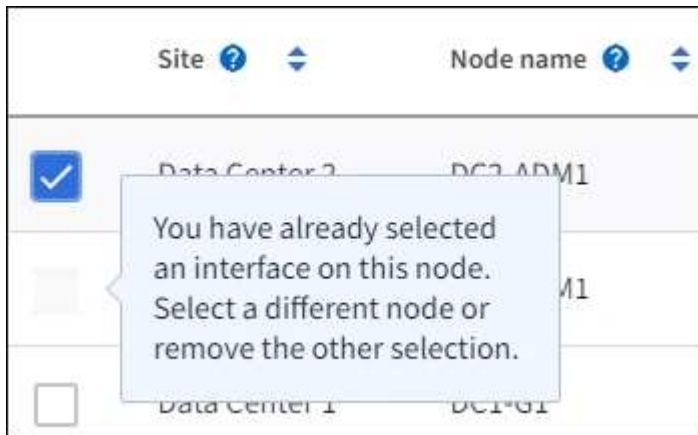
Después de crear una interfaz VLAN, espere hasta 5 minutos para que la nueva interfaz aparezca en la tabla.

Directrices para la selección de interfaces

- Debes seleccionar al menos una interfaz.
- Puede seleccionar solo una interfaz para un nodo.
- Si el grupo HA es para la protección de HA de los servicios del nodo de administración, que incluyen el administrador de red y el administrador de inquilinos, seleccione interfaces solo en los nodos de administración.
- Si el grupo HA es para la protección de HA del tráfico del cliente S3, seleccione interfaces en los

nodos de administración, los nodos de puerta de enlace o ambos.

- Si selecciona interfaces en diferentes tipos de nodos, aparece una nota informativa. Se le recuerda que si se produce una conmutación por error, es posible que los servicios proporcionados por el nodo previamente activo no estén disponibles en el nuevo nodo activo. Por ejemplo, un nodo de puerta de enlace de respaldo no puede brindar protección de alta disponibilidad a los servicios del nodo de administración. De manera similar, un nodo de administración de respaldo no puede realizar todos los procedimientos de mantenimiento que el nodo de administración principal puede proporcionar.
- Si no puede seleccionar una interfaz, su casilla de verificación estará deshabilitada. La información sobre herramientas proporciona más información.



- No puede seleccionar una interfaz si su valor de subred o puerta de enlace entra en conflicto con otra interfaz seleccionada.
- No puede seleccionar una interfaz configurada si no tiene una dirección IP estática.

2. Seleccione **Continuar**.

Determinar el orden de prioridad

Si el grupo HA incluye más de una interfaz, puede determinar cuál es la interfaz principal y cuáles son las interfaces de respaldo (conmutación por error). Si la interfaz principal falla, las direcciones VIP se mueven a la interfaz de mayor prioridad que esté disponible. Si esa interfaz falla, las direcciones VIP pasan a la siguiente interfaz de mayor prioridad que esté disponible, y así sucesivamente.

Pasos

1. Arrastre filas en la columna **Orden de prioridad** para determinar la interfaz principal y cualquier interfaz de respaldo.

La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra una falla.

Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order ?	Node	Interface ?	Node type ?
1 (Primary interface)	⬆ DC1-ADM1-104-96	eth2	Primary Admin Node
2	⬆ DC2-ADM1-104-103	eth2	Admin Node



Si el grupo HA proporciona acceso al Administrador de red, debe seleccionar una interfaz en el Nodo de administración principal para que sea la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

2. Seleccione **Continuar**.

Introduzca direcciones IP

Pasos

1. En el campo **Subred CIDR**, especifique la subred VIP en notación CIDR: una dirección IPv4 seguida de una barra 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.



Si utiliza un prefijo de 32 bits, la dirección de red VIP también sirve 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.

[Add another IP address](#)

- De manera opcional, si algún cliente administrativo o inquilino de S3 accederá a estas direcciones VIP desde una subred diferente, ingrese la **dirección IP de puerta de enlace**. La dirección de la puerta de enlace debe estar dentro de la subred VIP.

Los usuarios clientes y administradores utilizarán esta puerta de enlace para acceder a las direcciones IP virtuales.

- Ingrese al menos una y no más de diez direcciones VIP para la interfaz activa en el grupo HA. Todas las direcciones VIP deben estar dentro de la subred VIP y todas estarán activas al mismo tiempo en la interfaz activa.

Debe proporcionar al menos una dirección IPv4. Opcionalmente, puede especificar direcciones IPv4 e IPv6 adicionales.

- Seleccione **Crear grupo HA** y seleccione **Finalizar**.

Se crea el grupo HA y ahora puede utilizar las direcciones IP virtuales configuradas.

Próximos pasos

Si va a utilizar este grupo HA para equilibrar la carga, cree un punto final del equilibrador de carga para determinar el puerto y el protocolo de red y para adjuntar los certificados necesarios. Ver ["Configurar los puntos finales del balanceador de carga"](#).

Editar un grupo de alta disponibilidad

Puede editar un grupo de alta disponibilidad (HA) para cambiar su nombre y descripción, agregar o eliminar interfaces, cambiar el orden de prioridad o agregar o actualizar direcciones IP virtuales.

Por ejemplo, es posible que necesite editar un grupo de alta disponibilidad si desea eliminar el nodo asociado

con una interfaz seleccionada en un procedimiento de desmantelamiento de 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 verificación del grupo HA 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 de HA** para actualizar el nombre o la descripción del grupo, agregar o eliminar interfaces, cambiar el orden de prioridad o agregar o eliminar direcciones VIP.
4. Si seleccionó **Editar dirección IP virtual**:
 - a. Actualice las direcciones IP virtuales para el grupo HA.
 - b. Seleccione **Guardar**.
 - c. Seleccione **Finalizar**.
5. Si seleccionó **Editar grupo HA**:
 - a. Opcionalmente, actualice el nombre o la descripción del grupo.
 - b. Opcionalmente, seleccione o desmarque las casillas de verificación para agregar o eliminar interfaces.



Si el grupo HA proporciona acceso al Administrador de red, debe seleccionar una interfaz en el Nodo de administración principal para que sea la interfaz principal. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal

- c. Opcionalmente, arrastre filas para cambiar el orden de prioridad de la interfaz principal y cualquier interfaz de respaldo para este grupo de HA.
- d. Opcionalmente, actualice las direcciones IP virtuales.
- e. Seleccione **Guardar** y luego seleccione **Finalizar**.

Eliminar un grupo de alta disponibilidad

Puede eliminar uno o más grupos de alta disponibilidad (HA) a la vez.



No se puede eliminar un grupo de alta disponibilidad si está vinculado a un punto final del equilibrador de carga. Para eliminar un grupo de HA, debe quitarlo de todos los puntos finales del balanceador de carga que lo utilicen.

Para evitar interrupciones del cliente, actualice cualquier aplicación cliente S3 afectada antes de eliminar un grupo de alta disponibilidad. Actualice cada cliente para conectarse utilizando otra dirección IP, por ejemplo, la dirección IP virtual de un grupo de HA diferente o la dirección IP que se configuró para una interfaz durante la instalación.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad**.
2. Revise la columna **Puntos finales del balanceador de carga** para cada grupo de HA que desee eliminar. Si se enumeran puntos finales del balanceador de carga:

- a. Vaya a **CONFIGURACIÓN > Red > Puntos finales del balanceador de carga**.
 - b. Seleccione la casilla de verificación para el punto final.
 - c. Seleccione **Acciones > Editar modo de enlace de punto final**.
 - d. Actualice el modo de enlace para eliminar el grupo HA.
 - e. Seleccione **Guardar cambios**.
3. Si no se enumeran puntos finales del balanceador de carga, seleccione la casilla de verificación para cada grupo de alta disponibilidad que desee eliminar.
 4. Seleccione **Acciones > Eliminar grupo HA**.
 5. Revise el mensaje y seleccione **Eliminar grupo HA** para confirmar su selección.

Se eliminan todos los grupos HA que seleccionó. Aparece un banner de éxito verde en la página de grupos de alta disponibilidad.

Gestionar el equilibrio de carga

Consideraciones para el equilibrio de carga

Puede utilizar el equilibrio de carga para gestionar cargas de trabajo de ingesta y recuperación de clientes S3.

¿Qué es el equilibrio de carga?

Cuando una aplicación cliente guarda o recupera datos de un sistema StorageGRID, StorageGRID utiliza un equilibrador de carga para administrar la carga de trabajo de ingesta y recuperación. El equilibrio de carga maximiza la velocidad y la capacidad de conexión al distribuir la carga de trabajo entre múltiples nodos de almacenamiento.

El servicio StorageGRID Load Balancer está instalado en todos los nodos de administración y en todos los nodos de puerta de enlace y proporciona equilibrio de carga de capa 7. Realiza la terminación de seguridad de la capa de transporte (TLS) de las solicitudes de los clientes, inspecciona las solicitudes y establece nuevas conexiones seguras con los nodos de almacenamiento.

El servicio Load Balancer en cada nodo funciona de forma independiente al reenviar el tráfico del cliente a los nodos de almacenamiento. A través de un proceso de ponderación, el servicio Load Balancer dirige más solicitudes a los nodos de almacenamiento con mayor disponibilidad de CPU.



Si bien el servicio StorageGRID Load Balancer es el mecanismo de equilibrio de carga recomendado, es posible que desee integrar un equilibrador de carga de terceros. Para obtener más información, comuníquese con su representante de cuenta de NetApp o consulte ["TR-4626: Balanceadores de carga globales y de terceros de StorageGRID"](#).

¿Cuántos nodos de equilibrio de carga necesito?

Como práctica recomendada general, cada sitio en su sistema StorageGRID debe incluir dos o más nodos con el servicio Load Balancer. Por ejemplo, un sitio puede incluir dos nodos de puerta de enlace o un nodo de administración y un nodo de puerta de enlace. Asegúrese de que haya una infraestructura de red, hardware o virtualización adecuada para cada nodo de equilibrio de carga, independientemente de que utilice dispositivos de servicios, nodos físicos o nodos basados en máquinas virtuales (VM).

¿Qué es un punto final de balanceador de carga?

Un punto final del balanceador de carga define el puerto y el protocolo de red (HTTPS o HTTP) que las solicitudes de aplicaciones cliente entrantes y salientes utilizarán para acceder a aquellos nodos que contienen el servicio del balanceador de carga. El punto final también define el tipo de cliente (S3), el modo de enlace y, opcionalmente, una lista de inquilinos permitidos o bloqueados.

Para crear un punto final del balanceador de carga, seleccione **CONFIGURACIÓN > Red > Puntos finales del balanceador de carga** o complete el asistente de configuración de FabricPool y S3. Para obtener instrucciones:

- ["Configurar los puntos finales del balanceador de carga"](#)
- ["Utilice el asistente de configuración de S3"](#)
- ["Utilice el asistente de configuración de FabricPool"](#)

Consideraciones para el puerto

El puerto para un punto final del balanceador de carga tiene como valor predeterminado 10433 para el primer punto final que cree, pero puede especificar cualquier puerto externo no utilizado entre 1 y 65535. Si usa el puerto 80 o 443, el punto final utilizará el servicio Load Balancer solo en los nodos de puerta de enlace. Estos puertos están reservados en los nodos de administración. Si utiliza el mismo puerto para más de un punto final, debe especificar un modo de enlace diferente para cada punto final.

No se permiten puertos utilizados por otros servicios de la red. Ver el ["Referencia del puerto de red"](#).

Consideraciones para el protocolo de red

En la mayoría de los casos, las conexiones entre las aplicaciones cliente y StorageGRID deben utilizar el cifrado de seguridad de la capa de transporte (TLS). Se admite la conexión a StorageGRID sin cifrado TLS, pero no se recomienda, especialmente en entornos de producción. Al seleccionar el protocolo de red para el punto final del balanceador de carga StorageGRID, debe seleccionar **HTTPS**.

Consideraciones sobre los certificados de punto final del equilibrador de carga

Si selecciona **HTTPS** como protocolo de red para el punto final del balanceador de carga, deberá proporcionar un certificado de seguridad. Puede utilizar cualquiera de estas tres opciones al crear el punto final del equilibrador de carga:

- **Subir un certificado firmado (recomendado).** Este certificado puede estar firmado por una autoridad de certificación (CA) privada o de confianza pública. La mejor práctica es utilizar un certificado de servidor CA de confianza pública para proteger la conexión. A diferencia de los certificados generados, los certificados firmados por una CA se pueden rotar sin interrupciones, lo que puede ayudar a evitar problemas de vencimiento.

Debe obtener los siguientes archivos antes de crear el punto final del equilibrador de carga:

- El archivo de certificado de servidor personalizado.
- El archivo de clave privada del certificado de servidor personalizado.
- Opcionalmente, un paquete CA de los certificados de cada autoridad de certificación emisora intermedia.
- **Generar un certificado autofirmado.**
- **Utilice el certificado global StorageGRID S3.** Debe cargar o generar una versión personalizada de este

certificado antes de poder seleccionarlo para el punto final del balanceador de carga. Ver ["Configurar certificados de API S3"](#).

¿Qué valores necesito?

Para crear el certificado, debe conocer todos los nombres de dominio y direcciones IP que las aplicaciones cliente S3 usarán para acceder al punto final.

La entrada **DN del sujeto** (nombre distinguido) del certificado debe incluir el nombre de dominio completo que la aplicación cliente utilizará para StorageGRID. Por ejemplo:

```
Subject DN:  
/C=Country/ST=State/O=Company, Inc./CN=s3.storagegrid.example.com
```

Según sea necesario, el certificado puede usar caracteres comodín para representar los nombres de dominio completos de todos los nodos de administración y nodos de puerta de enlace que ejecutan el servicio Load Balancer. Por ejemplo, `*.storagegrid.example.com` utiliza el comodín `*` para representar `adm1.storagegrid.example.com` y `gn1.storagegrid.example.com`.

Si planea utilizar solicitudes alojadas virtuales de estilo S3, el certificado también debe incluir una entrada **Nombre alternativo** para cada una. ["Nombre de dominio del punto final S3"](#) que haya configurado, incluidos los nombres comodín. Por ejemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```



Si utiliza comodines para los nombres de dominio, revise la ["Pautas de refuerzo para certificados de servidor"](#).

También debe definir una entrada DNS para cada nombre en el certificado de seguridad.

¿Cómo gestiono los certificados que expiran?



Si el certificado utilizado para proteger la conexión entre la aplicación S3 y StorageGRID caduca, la aplicación podría perder temporalmente el acceso a StorageGRID.

Para evitar problemas de vencimiento de certificados, siga estas prácticas recomendadas:

- Supervise atentamente cualquier alerta que advierta sobre fechas de vencimiento de certificados próximas, como las alertas **Vencimiento del certificado del punto final del equilibrador de carga** y **Vencimiento del certificado del servidor global para la API de S3**.
- Mantenga siempre sincronizadas las versiones del certificado de StorageGRID y de la aplicación S3. Si reemplaza o renueva el certificado utilizado para un punto final del balanceador de carga, debe reemplazar o renovar el certificado equivalente utilizado por la aplicación S3.
- Utilice un certificado CA firmado públicamente. Si utiliza un certificado firmado por una CA, puede reemplazar certificados que estén próximos a vencer sin interrupciones.
- Si ha generado un certificado StorageGRID autofirmado y dicho certificado está a punto de caducar, debe reemplazarlo manualmente tanto en StorageGRID como en la aplicación S3 antes de que caduque el certificado existente.

Consideraciones para el modo de enlace

El modo de enlace le permite controlar qué direcciones IP se pueden usar para acceder a un punto final del balanceador de carga. Si un punto final utiliza un modo de enlace, las aplicaciones cliente solo pueden acceder al punto final si usan una dirección IP permitida o su nombre de dominio completo (FQDN) correspondiente. Las aplicaciones cliente que utilicen cualquier otra dirección IP o FQDN no pueden acceder al punto final.

Puede especificar cualquiera de los siguientes modos de enlace:

- **Global** (predeterminado): Las aplicaciones cliente pueden acceder al punto final utilizando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice esta configuración a menos que necesite restringir la accesibilidad de un punto final.
- **IP virtuales de grupos HA**. Las aplicaciones cliente deben utilizar una dirección IP virtual (o FQDN correspondiente) de un grupo de alta disponibilidad.
- **Interfaces de nodo**. Los clientes deben utilizar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas.
- **Tipo de nodo**. Según el tipo de nodo que seleccione, los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o FQDN correspondiente) de cualquier nodo de puerta de enlace.

Consideraciones para el acceso de los inquilinos

El acceso de inquilinos es una función de seguridad opcional que le permite controlar qué cuentas de inquilinos de StorageGRID pueden usar un punto final del balanceador de carga para acceder a sus buckets. Puede permitir que todos los inquilinos accedan a un punto final (predeterminado) o puede especificar una lista de inquilinos permitidos o bloqueados para cada punto final.

Puede utilizar esta función para proporcionar un mejor aislamiento de seguridad entre los inquilinos y sus puntos finales. Por ejemplo, puede utilizar esta función para garantizar que los materiales altamente clasificados o de alto secreto propiedad de un inquilino permanezcan completamente inaccesibles para los demás inquilinos.



A los efectos del control de acceso, el inquilino se determina a partir de las claves de acceso utilizadas en la solicitud del cliente; si no se proporcionan claves de acceso como parte de la solicitud (como en el caso del acceso anónimo), se utiliza el propietario del depósito para determinar el inquilino.

Ejemplo de acceso de inquilinos

Para comprender cómo funciona esta característica de seguridad, considere el siguiente ejemplo:

1. Ha creado dos puntos finales de equilibrador de carga, de la siguiente manera:
 - Punto final **público**: utiliza el puerto 10443 y permite el acceso a todos los inquilinos.
 - Punto final **alto secreto**: utiliza el puerto 10444 y permite el acceso únicamente al inquilino **alto secreto**. Todos los demás inquilinos tienen bloqueado el acceso a este punto final.
2. El `top-secret.pdf` está en un cubo propiedad del inquilino **alto secreto**.

Para acceder a la `top-secret.pdf`, un usuario en el inquilino **Top secret** puede emitir una solicitud GET a `https://w.x.y.z:10444/top-secret.pdf`. Debido a que a este inquilino se le permite usar el punto

final 10444, el usuario puede acceder al objeto. Sin embargo, si un usuario que pertenece a otro inquilino emite la misma solicitud a la misma URL, recibirá inmediatamente un mensaje de acceso denegado. Se deniega el acceso incluso si las credenciales y la firma son válidas.

Disponibilidad de CPU

El servicio Load Balancer en cada nodo de administración y nodo de puerta de enlace funciona de forma independiente al reenviar tráfico S3 a los nodos de almacenamiento. A través de un proceso de ponderación, el servicio Load Balancer dirige más solicitudes a los nodos de almacenamiento con mayor disponibilidad de CPU. La información de carga de la CPU del nodo se actualiza cada pocos minutos, pero la ponderación podría actualizarse con mayor frecuencia. A todos los nodos de almacenamiento se les asigna un valor de peso base mínimo, incluso si un nodo informa una utilización del 100 % o no informa su utilización.

En algunos casos, la información sobre la disponibilidad de la CPU se limita al sitio donde se encuentra el servicio Load Balancer.

Configurar los puntos finales del balanceador de carga

Los puntos finales del balanceador de carga determinan los puertos y los protocolos de red que los clientes S3 pueden usar cuando se conectan al balanceador de carga StorageGRID en los nodos de puerta de enlace y de administración. También puede utilizar puntos finales para acceder al Administrador de red, al Administrador de inquilinos o a ambos.



Se han eliminado los detalles rápidos de esta versión del sitio de documentación. Ver ["Configurar conexiones de cliente S3 y Swift"](#).

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).
- Usted ha revisado el ["Consideraciones para el equilibrio de carga"](#).
- Si anteriormente reasignó un puerto que desea utilizar para el punto final del balanceador de carga, debe ["Se eliminó la reasignación del puerto"](#).
- Ha creado todos los grupos de alta disponibilidad (HA) que planea utilizar. Se recomiendan los grupos HA, pero no son obligatorios. Ver ["Administrar grupos de alta disponibilidad"](#).
- Si el punto final del balanceador de carga será utilizado por ["Inquilinos de S3 para S3 Select"](#), no debe utilizar las direcciones IP o FQDN de ningún nodo físico. Solo se permiten dispositivos de servicios y nodos de software basados en VMware para los puntos finales del equilibrador de carga utilizados para S3 Select.
- Ha configurado todas las interfaces VLAN que planea utilizar. Ver ["Configurar interfaces VLAN"](#).
- Si está creando un punto final HTTPS (recomendado), tiene la información del certificado del servidor.



Los cambios en un certificado de punto final pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

- Para cargar un certificado, necesita el certificado del servidor, la clave privada del certificado y, opcionalmente, un paquete de CA.
- Para generar un certificado, necesita todos los nombres de dominio y direcciones IP que los clientes S3 usarán para acceder al punto final. También debes conocer el tema (Nombre Distinguido).

- Si desea utilizar el certificado API S3 de StorageGRID (que también se puede usar para conexiones directas a nodos de almacenamiento), ya ha reemplazado el certificado predeterminado con un certificado personalizado firmado por una autoridad de certificación externa. Ver "[Configurar certificados de API S3](#)".

Crear un punto final de balanceador de carga

Cada punto final del balanceador de carga del cliente S3 especifica un puerto, un tipo de cliente (S3) y un protocolo de red (HTTP o HTTPS). Los puntos finales del balanceador de carga de la interfaz de administración especifican un puerto, un tipo de interfaz y una red de cliente no confiable.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Puntos finales del balanceador de carga**.
2. Para crear un punto final para un cliente S3 o Swift, seleccione la pestaña **Cliente S3 o Swift**.
3. Para crear un punto final para acceder al Administrador de red, al Administrador de inquilinos o a ambos, seleccione la pestaña **Interfaz de administración**.
4. Seleccione **Crear**.

Ingrese los detalles del punto final

Pasos

1. Seleccione las instrucciones adecuadas para ingresar detalles para el tipo de punto final que desea crear.

Cliente S3 o Swift

Campo	Descripción
Nombre	Un nombre descriptivo para el punto final, que aparecerá en la tabla de la página Puntos finales del balanceador de carga.
Puerto	El puerto StorageGRID que desea utilizar para equilibrar la carga. Este campo tiene como valor predeterminado 10433 para el primer punto final que cree, pero puede ingresar cualquier puerto externo no utilizado del 1 al 65535. Si ingresa 80 o 8443, el punto final se configura solo en los nodos de puerta de enlace, a menos que haya liberado el puerto 8443. Luego, puede usar el puerto 8443 como punto final S3, y el puerto se configurará tanto en los nodos de puerta de enlace como en los de administración.
Tipo de cliente	El tipo de aplicación cliente que utilizará este punto final, ya sea S3 o Swift .
Protocolo de red	El protocolo de red que utilizarán los clientes cuando se conecten a este punto final. • Seleccione HTTPS para una comunicación segura y cifrada con TLS (recomendado). Debe adjuntar un certificado de seguridad antes de poder guardar el punto final. • Seleccione HTTP para una comunicación menos segura y sin cifrar. Utilice HTTP únicamente para una cuadrícula que no sea de producción.

Interfaz de gestión

Campo	Descripción
Nombre	Un nombre descriptivo para el punto final, que aparecerá en la tabla de la página Puntos finales del balanceador de carga.
Puerto	El puerto StorageGRID que desea utilizar para acceder al Administrador de Grid, al Administrador de inquilinos o a ambos. • Administrador de red: 8443 • Gerente de inquilinos: 9443 • Tanto el administrador de la red como el administrador de inquilinos: 443 Nota: Puede utilizar estos puertos preestablecidos u otros puertos disponibles.
Tipo de interfaz	Seleccione el botón de opción para la interfaz StorageGRID a la que accederá mediante este punto final.

Campo	Descripción
Red de clientes no confiables	Seleccione Sí si este punto final debe ser accesible para redes de clientes que no son de confianza. De lo contrario, seleccione No. Cuando selecciona Sí, el puerto se abre en todas las redes de cliente que no son de confianza. Nota: Solo puede configurar un puerto para que esté abierto o cerrado para redes de clientes que no sean de confianza cuando crea el punto final del balanceador de carga.

1. Seleccione **Continuar**.

Seleccionar un modo de enlace

Pasos

1. Seleccione un modo de enlace para el punto final para controlar cómo se accede a él utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Algunos modos de enlace están disponibles para puntos finales de cliente o puntos finales de interfaz de administración. Aquí se enumeran todos los modos para ambos tipos de puntos finales.

Modo	Descripción
Global (predeterminado para puntos finales del cliente)	Los clientes pueden acceder al punto final utilizando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice la configuración Global a menos que necesite restringir la accesibilidad de este punto final.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o FQDN correspondiente) de un grupo de HA para acceder a este punto final. Todos los puntos finales con este modo de enlace pueden usar el mismo número de puerto, siempre que los grupos de HA que seleccione para los puntos finales no se superpongan.
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.
Tipo de nodo (solo puntos finales del cliente)	Según el tipo de nodo que seleccione, los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este punto final.

Modo	Descripción
Todos los nodos de administración (predeterminado para los puntos finales de la interfaz de administración)	Los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración para acceder a este punto final.

Si más de un punto final usa el mismo puerto, StorageGRID usa este orden de prioridad para decidir qué punto final usar: **IP virtuales de grupos de alta disponibilidad** > **Interfaces de nodo** > **Tipo de nodo** > **Global**.

Si está creando puntos finales de interfaz de administración, solo se permiten nodos de administración.

2. Si seleccionó **IP virtuales de grupos de HA**, seleccione uno o más grupos de HA.

Si está creando puntos finales de interfaz de administración, seleccione VIP asociados únicamente con nodos de administración.

3. Si seleccionó **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 punto final.
4. Si seleccionó **Tipo de nodo**, seleccione Nodos de administración, que incluye tanto el nodo de administración principal como cualquier nodo de administración no principal, o Nodos de puerta de enlace.

Controlar el acceso de los inquilinos



Un punto final de interfaz de administración puede controlar el acceso de los inquilinos solo cuando el punto final tiene la [Tipo de interfaz del administrador de inquilinos](#).

Pasos

1. Para el paso **Acceso de inquilino**, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (predeterminado)	Todas las cuentas de inquilinos pueden usar este punto final para acceder a sus depósitos. Debe seleccionar esta opción si aún no ha creado ninguna cuenta de inquilino. Después de agregar cuentas de inquilino, puede editar el punto final del balanceador de carga para permitir o bloquear cuentas específicas.
Permitir inquilinos seleccionados	Solo las cuentas de inquilinos seleccionadas pueden usar este punto final para acceder a sus depósitos.
Bloquear inquilinos seleccionados	Las cuentas de inquilinos seleccionadas no pueden usar este punto final para acceder a sus depósitos. Todos los demás inquilinos pueden utilizar este punto final.

2. Si está creando un punto final **HTTP**, no necesita adjuntar un certificado. Seleccione **Crear** para agregar el

nuevo punto final del balanceador de carga. Luego, ve a [Después de terminar](#) . De lo contrario, seleccione **Continuar** para adjuntar el certificado.

Adjuntar certificado

Pasos

1. Si está creando un punto final **HTTPS**, seleccione el tipo de certificado de seguridad que desea adjuntar al punto final.

El certificado protege las conexiones entre los clientes S3 y el servicio Load Balancer en los nodos de administración o de puerta de enlace.

- **Subir 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 el certificado StorageGRID S3.** Seleccione esta opción si desea utilizar el certificado API S3 global, que también se puede usar para conexiones directas a nodos de almacenamiento.

No puede seleccionar esta opción a menos que haya reemplazado el certificado API S3 predeterminado, que está firmado por la CA de la red, con un certificado personalizado firmado por una autoridad de certificación externa. Ver "[Configurar certificados de API S3](#)".

- **Utilizar certificado de interfaz de administración.** Seleccione esta opción si desea utilizar el certificado de interfaz de administración global, que también se puede utilizar para conexiones directas a los nodos de administración.
2. Si no está utilizando el certificado StorageGRID S3, cargue o genere el certificado.

Subir certificado

a. Seleccione **Subir certificado**.

b. Cargue los archivos de certificado de servidor necesarios:

- **Certificado de servidor:** el archivo de certificado de servidor personalizado en codificación PEM.
- **Clave privada del certificado:** El archivo de clave privada del certificado del servidor personalizado(`.key`).



Las claves privadas EC deben tener 224 bits o más. Las claves privadas RSA deben tener 2048 bits o más.

- **Paquete CA:** un único archivo opcional que contiene los certificados de cada autoridad de certificación (CA) emisora intermedia. El archivo debe contener cada uno de los archivos de certificado CA codificados en PEM, concatenados en el orden de la cadena de certificados.

c. Expande **Detalles del certificado** para ver los metadatos de cada certificado que hayas cargado. Si cargó un paquete de CA opcional, cada certificado se muestra 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 del 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 CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

d. Seleccione **Crear**. + Se crea el punto final del equilibrador de carga. El certificado personalizado se utiliza para todas las nuevas conexiones posteriores entre los clientes S3 o la interfaz de administración y el punto final.

Generar certificado

a. Seleccione **Generar certificado**.

b. Especifique la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o más nombres de dominio completos para incluir en el certificado. Utilice un * como comodín para representar varios nombres de dominio.
Propiedad intelectual	Una o más direcciones IP para incluir en el certificado.
Asunto (opcional)	Sujeto X.509 o nombre distinguido (DN) del propietario del certificado. Si no se ingresa ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o dirección IP como nombre común del sujeto (CN).

Campo	Descripción
Días válidos	Número de días después de su creación que expira el certificado.
Agregar extensiones de uso de claves	Si se selecciona (predeterminado y recomendado), las extensiones de uso de clave y uso de clave extendido se agregan al certificado generado. Estas extensiones definen el propósito de la clave contenida en el certificado. Nota: Deje esta casilla de verificación seleccionada a menos que experimente problemas de conexión con clientes más antiguos cuando los certificados incluyan estas extensiones.

c. Seleccione **Generar**.

d. Seleccione **Detalles del certificado** para ver los metadatos del certificado generado.

- Seleccione **Descargar certificado** para guardar el archivo del certificado.

Especifique el nombre del archivo del 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 y pegarlo en otro lugar.

e. Seleccione **Crear**.

Se crea el punto final del equilibrador de carga. El certificado personalizado se utiliza para todas las nuevas conexiones posteriores entre los clientes S3 o la interfaz de administración y este punto final.

Después de terminar

Pasos

1. Si utiliza un DNS, asegúrese de que el DNS incluya un registro para asociar el nombre de dominio completo (FQDN) de StorageGRID a cada dirección IP que los clientes usarán para realizar conexiones.

La dirección IP que ingrese en el registro DNS depende de si está utilizando un grupo HA de nodos de equilibrio de carga:

- Si ha configurado un grupo de alta disponibilidad, los clientes se conectarán a las direcciones IP virtuales de ese grupo de alta disponibilidad.
- Si no utiliza un grupo de alta disponibilidad, los clientes se conectarán al servicio StorageGRID Load Balancer mediante la dirección IP de un nodo de puerta de enlace o de administración.

También debe asegurarse de que el registro DNS haga referencia a todos los nombres de dominio de punto final requeridos, incluidos todos los nombres comodín.

2. Proporcionar a los clientes S3 la información necesaria para conectarse al punto final:

- Número de puerto
- Nombre de dominio completo o dirección IP
- Cualquier detalle del certificado requerido

Ver y editar puntos finales del balanceador de carga

Puede ver los detalles de los puntos finales del balanceador de carga existentes, incluidos los metadatos del certificado para un punto final seguro. Puede cambiar ciertas configuraciones para un punto final.

- Para ver información básica de todos los puntos finales del balanceador de carga, revise las tablas en la página Puntos finales del balanceador de carga.
- Para ver todos los detalles sobre un punto final específico, incluidos los metadatos del certificado, seleccione el nombre del punto final en la tabla. La información mostrada varía según el tipo de punto final y cómo esté configurado.

S3 load balancer endpoint

Port:	10443
Client type:	S3
Network protocol:	HTTPS
Binding mode:	Global
Endpoint ID:	3d02c126-9437-478c-8b24-08384401d3cb

[Remove](#)

Binding mode

Certificate

Tenant access (2 allowed)

You can select a different binding mode or change IP addresses for the current binding mode.

[Edit binding mode](#)

Binding mode: Global

 This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.

- Para editar un punto final, utilice el menú **Acciones** en la página Puntos finales del balanceador de carga.



Si pierde el acceso a Grid Manager mientras edita el puerto de un punto final de la interfaz de administración, actualice la URL y el puerto para recuperar el acceso.



Después de editar un punto final, es posible que deba esperar hasta 15 minutos para que los cambios se apliquen a todos los nodos.

Tarea	Menú de acciones	Página de detalles
Editar el nombre del punto final	a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar nombre del punto final. c. Introduzca el nuevo nombre. d. Seleccione Guardar.	a. Seleccione el nombre del punto final para mostrar los detalles. b. Seleccione el icono de edición . c. Introduzca el nuevo nombre. d. Seleccione Guardar.
Editar el puerto del punto final	a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar puerto de punto final. c. Introduzca un número de puerto válido. d. Seleccione Guardar.	<i>n / A</i>
Editar el modo de enlace del punto final	a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar modo de enlace de punto final. c. Actualice el modo de enlace según sea necesario. d. Seleccione Guardar cambios.	a. Seleccione el nombre del punto final para mostrar los detalles. b. Seleccione Editar modo de enlace. c. Actualice el modo de enlace según sea necesario. d. Seleccione Guardar cambios.
Editar el certificado del punto final	a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar certificado de punto final. c. Cargue o genere un nuevo certificado personalizado o comience a utilizar el certificado S3 global, según sea necesario. d. Seleccione Guardar cambios.	a. Seleccione el nombre del punto final para mostrar los detalles. b. Seleccione la pestaña Certificado. c. Seleccione Editar certificado. d. Cargue o genere un nuevo certificado personalizado o comience a utilizar el certificado S3 global, según sea necesario. e. Seleccione Guardar cambios.

Tarea	Menú de acciones	Página de detalles
Editar el acceso de los inquilinos	a. Seleccione la casilla de verificación para el punto final. b. Seleccione Acciones > Editar acceso de inquilino . c. Elija una opción de acceso diferente, seleccione o elimine inquilinos de la lista, o haga ambas cosas. d. Seleccione Guardar cambios .	a. Seleccione el nombre del punto final para mostrar los detalles. b. Seleccione la pestaña Acceso de inquilinos . c. Seleccione Editar acceso de inquilino . d. Elija una opción de acceso diferente, seleccione o elimine inquilinos de la lista, o haga ambas cosas. e. Seleccione Guardar cambios .

Eliminar puntos finales del balanceador de carga

Puede eliminar uno o más puntos finales mediante el menú **Acciones**, o puede eliminar un solo punto final desde la página de detalles.



Para evitar interrupciones del cliente, actualice cualquier aplicación cliente S3 afectada antes de eliminar un punto final del balanceador de carga. Actualice cada cliente para conectarse usando un puerto asignado a otro punto final del balanceador de carga. Asegúrese de actualizar también cualquier información del certificado requerida.



Si pierde el acceso a Grid Manager mientras elimina un punto final de la interfaz de administración, actualice la URL.

- Para eliminar uno o más puntos finales:
 - Desde la página Balanceador de carga, seleccione la casilla de verificación para cada punto final que desee eliminar.
 - Seleccione **Acciones > Eliminar**.
 - Seleccione **Aceptar**.
- Para eliminar un punto final de la página de detalles:
 - Desde la página Balanceador de carga, seleccione el nombre del punto final.
 - Seleccione **Eliminar** en la página de detalles.
 - Seleccione **Aceptar**.

Configurar nombres de dominio de puntos finales S3

Para admitir solicitudes de estilo alojado virtualmente S3, debe usar Grid Manager para configurar la lista de nombres de dominio de puntos finales S3 a los que se conectan los clientes S3.



No se admite el uso de una dirección IP para un nombre de dominio de punto final. Las versiones futuras evitarán esta configuración.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Ha confirmado que no hay ninguna actualización de la red en curso.



No realice ningún cambio en la configuración del nombre de dominio cuando haya una actualización de la red en curso.

Acerca de esta tarea

Para permitir que los clientes utilicen nombres de dominio de punto final S3, debe realizar todo lo siguiente:

- Utilice Grid Manager para agregar los nombres de dominio del punto final S3 al sistema StorageGRID .
- Asegúrese de que el ["Certificado que el cliente utiliza para conexiones HTTPS a StorageGRID"](#) Está firmado para todos los nombres de dominio que requiera el cliente.

Por ejemplo, si el punto final es `s3.company.com` , debe asegurarse de que el certificado utilizado para las conexiones HTTPS incluya el `s3.company.com` punto final y el nombre alternativo del sujeto (SAN) comodín del punto final: `*.s3.company.com` .

- Configurar el servidor DNS utilizado por el cliente. Incluya registros DNS para las direcciones IP que los clientes usan para realizar conexiones y asegúrese de que los registros hagan referencia a todos los nombres de dominio de punto final S3 requeridos, incluidos todos los nombres comodín.



Los clientes pueden conectarse a StorageGRID utilizando la dirección IP de un nodo de puerta de enlace, un nodo de administración o un nodo de almacenamiento, o conectándose a la dirección IP virtual de un grupo de alta disponibilidad. Debe comprender cómo se conectan las aplicaciones cliente a la red para incluir las direcciones IP correctas en los registros DNS.

Los clientes que utilizan conexiones HTTPS (recomendadas) a la red pueden usar cualquiera de estos certificados:

- Los clientes que se conectan a un punto final del equilibrador de carga pueden usar un certificado personalizado para ese punto final. Cada punto final del equilibrador de carga se puede configurar para reconocer diferentes nombres de dominio de punto final S3.
- Los clientes que se conectan a un punto final del balanceador de carga o directamente a un nodo de almacenamiento pueden personalizar el certificado API S3 global para incluir todos los nombres de dominio de punto final S3 requeridos.



Si no agrega nombres de dominio de punto final S3 y la lista está vacía, se deshabilita la compatibilidad con solicitudes de estilo alojado virtualmente S3.

Agregar un nombre de dominio de punto final S3

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Nombres de dominio de punto final S3**.
2. Introduzca el nombre de dominio en el campo **Nombre de dominio 1**. Seleccione **Agregar otro nombre de dominio** para agregar más nombres de dominio.
3. Seleccione **Guardar**.

4. Asegúrese de que los certificados de servidor que utilizan los clientes coincidan con los nombres de dominio de punto final S3 requeridos.
 - Si los clientes se conectan a un punto final del balanceador de carga que utiliza su propio certificado, ["Actualizar el certificado asociado con el punto final"](#) .
 - Si los clientes se conectan a un punto final del balanceador de carga que utiliza el certificado de API S3 global o directamente a los nodos de almacenamiento, ["actualizar el certificado API global de S3"](#) .
5. Agregue los registros DNS necesarios para garantizar que se puedan resolver las solicitudes de nombre de dominio del punto final.

Resultado

Ahora, cuando los clientes utilizan el punto final `bucket.s3.company.com` , el servidor DNS se resuelve en el punto final correcto y el certificado autentica el punto final como se esperaba.

Cambiar el nombre de un dominio de punto final S3

Si cambia un nombre utilizado por aplicaciones S3, las solicitudes de estilo alojado virtualmente fallarán.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Nombres de dominio de punto final S3**.
2. Seleccione el campo de nombre de dominio que desea editar y realice los cambios necesarios.
3. Seleccione **Guardar**.
4. Seleccione **Sí** para confirmar su cambio.

Eliminar un nombre de dominio de punto final S3

Si elimina un nombre utilizado por aplicaciones S3, las solicitudes de estilo alojado virtualmente fallarán.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Nombres de dominio de punto final S3**.
2. Seleccione el icono de eliminar  junto al nombre de dominio.
3. Seleccione **Sí** para confirmar la eliminación.

Información relacionada

- ["Utilice la API REST de S3"](#)
- ["Ver direcciones IP"](#)
- ["Configurar grupos de alta disponibilidad"](#)

Resumen: Direcciones IP y puertos para conexiones de cliente

Para almacenar o recuperar objetos, las aplicaciones cliente S3 se conectan al servicio Load Balancer, que está incluido en todos los nodos de administración y nodos de puerta de enlace, o al servicio Local Distribution Router (LDR), que está incluido en todos los nodos de almacenamiento.

Las aplicaciones cliente pueden conectarse a StorageGRID utilizando la dirección IP de un nodo de la red y el número de puerto del servicio en ese nodo. Opcionalmente, puede crear grupos de alta disponibilidad (HA) de nodos de equilibrio de carga para proporcionar conexiones de alta disponibilidad que utilicen direcciones IP virtuales (VIP). Si desea conectarse a StorageGRID utilizando un nombre de dominio completo (FQDN) en

lugar de una dirección IP o VIP, puede configurar entradas DNS.

Esta tabla resume las diferentes formas en que los clientes pueden conectarse a StorageGRID y las direcciones IP y los puertos que se utilizan para cada tipo de conexión. Si ya ha creado puntos finales de equilibrador de carga y grupos de alta disponibilidad (HA), consulte [Dónde encontrar direcciones IP](#) para localizar estos valores en el Administrador de cuadrícula.

Donde se establece la conexión	Servicio al que se conecta el cliente	Dirección IP	Puerto
Grupo HA	Balanceador de carga	Dirección IP virtual de un grupo de alta disponibilidad	Puerto asignado al punto final del balanceador de carga
Nodo de administración	Balanceador de carga	Dirección IP del nodo de administración	Puerto asignado al punto final del balanceador de carga
Nodo de puerta de enlace	Balanceador de carga	Dirección IP del nodo de enlace	Puerto asignado al punto final del balanceador de carga
Nodo de almacenamiento	LDR	Dirección IP del nodo de almacenamiento	Puertos S3 predeterminados: • HTTPS: 18082 • HTTP: 18084

URL de ejemplo

Para conectar una aplicación cliente al punto final del balanceador de carga de un grupo de alta disponibilidad 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 HA es 192.0.2.5 y el número de puerto del punto final del balanceador de carga es 10443, entonces una aplicación podría usar la siguiente URL para conectarse a StorageGRID:

`https://192.0.2.5:10443`

Dónde encontrar direcciones IP

1. Sign in en Grid Manager usando un ["navegador web compatible"](#).
2. Para encontrar la dirección IP de un nodo de la red:
 - a. Seleccione **NODOS**.
 - b. Seleccione el nodo de administración, el nodo de puerta de enlace o el nodo de almacenamiento al que desea conectarse.
 - c. Seleccione la pestaña **Descripción general**.
 - d. En la sección Información del nodo, anote las direcciones IP del nodo.

- e. Seleccione **Mostrar más** para ver las direcciones IPv6 y las asignaciones de interfaces.

Puede establecer conexiones desde aplicaciones cliente a cualquiera de las direcciones IP de la lista:

- **eth0**: Red de cuadrícula
- **eth1**: Red de administración (opcional)
- **eth2**: Red de cliente (opcional)



Si está viendo un nodo de administración o un nodo de puerta de enlace y es el nodo activo en un grupo de alta disponibilidad, la dirección IP virtual del grupo de alta disponibilidad se muestra en eth2.

3. Para encontrar la dirección IP virtual de un grupo de alta disponibilidad:
 - a. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad**.
 - b. En la tabla, anote la dirección IP virtual del grupo HA.
4. Para encontrar el número de puerto de un punto final del balanceador de carga:
 - a. Seleccione **CONFIGURACIÓN > Red > Puntos finales del balanceador de carga**.
 - b. Anote el número de puerto del punto final que desea utilizar.



Si el número de puerto es 80 o 443, el punto final se configura solo en los nodos de puerta de enlace, porque esos puertos están reservados en los nodos de administración. Todos los demás puertos se configuran tanto en los nodos de puerta de enlace como en los nodos de administración.

- c. Seleccione el nombre del punto final de la tabla.
- d. Confirme que el **Tipo de cliente** (S3) coincida con la aplicación cliente que utilizará el punto final.

Administrar redes y conexiones

Configurar los ajustes de red

Puede configurar varias configuraciones de red desde Grid Manager para ajustar el funcionamiento de su sistema StorageGRID .

Configurar interfaces VLAN

Puede [crear interfaces de LAN virtual \(VLAN\)](#) para aislar y particionar el tráfico para garantizar la seguridad, la flexibilidad y el rendimiento. Cada interfaz VLAN está asociada con una o más interfaces principales en los nodos de administración y los nodos de puerta de enlace. Puede usar interfaces VLAN en grupos de alta disponibilidad y en puntos finales del balanceador de carga para segregar el tráfico de clientes o administradores por aplicación o inquilino.

Políticas de clasificación de tráfico

Puedes utilizar [políticas de clasificación de tráfico](#) para identificar y gestionar diferentes tipos de tráfico de red, incluido el tráfico relacionado con buckets, inquilinos, subredes de clientes o puntos finales de balanceador de carga específicos. Estas políticas pueden ayudar a limitar y monitorear el tráfico.

Directrices para redes StorageGRID

Puede utilizar Grid Manager para configurar y administrar redes y conexiones de StorageGRID .

Ver "[Configurar conexiones de cliente S3](#)" para aprender cómo conectar clientes S3.

Redes StorageGRID predeterminadas

De forma predeterminada, StorageGRID admite tres interfaces de red por nodo de red, lo que le permite configurar la red para cada nodo de red individual para que coincida con sus requisitos de seguridad y acceso.

Para obtener más información sobre la topología de red, consulte "[Pautas para establecer redes](#)".

Red de cuadrícula

Requerido. La red Grid se utiliza para todo el tráfico interno de StorageGRID . Proporciona conectividad entre todos los nodos de la red, en todos los sitios y subredes.

Red de administración

Opcional. La red de administración normalmente se utiliza para la administración y el mantenimiento del sistema. También se puede utilizar para acceder al protocolo de cliente. La red de administración normalmente es una red privada y no necesita ser enrutable entre sitios.

Red de clientes

Opcional. La red de cliente es una red abierta que normalmente se utiliza para proporcionar acceso a aplicaciones de cliente S3, de modo que la red de cuadrícula se puede aislar y proteger. La red del cliente puede comunicarse con cualquier subred accesible a través de la puerta de enlace local.

Pautas

- Cada nodo 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 red no puede tener más de una interfaz en una red.
- Se admite una única puerta de enlace por red y por nodo de la red, y debe estar en la misma subred que el nodo. Puede implementar un enrutamiento más complejo en la puerta de enlace, si es necesario.
- En cada nodo, cada red se asigna a una interfaz de red específica.

Red	Nombre de la interfaz
Red	eth0
Administrador (opcional)	eth1
Cliente (opcional)	eth2

- Si el nodo está conectado a un dispositivo StorageGRID , se utilizan puertos específicos para cada red. Para obtener más detalles, consulte las instrucciones de instalación de su aparato.
- La ruta predeterminada se genera automáticamente, por nodo. Si eth2 está habilitado, entonces 0.0.0.0/0

usa la red del cliente en eth2. Si eth2 no está habilitado, entonces 0.0.0.0/0 usa la red Grid en eth0.

- La red del cliente no estará operativa hasta que el nodo de la red se haya unido a la red.
- La red de administración se puede configurar durante la implementación del nodo de la red para permitir el acceso a la interfaz de usuario de instalación antes de que la red esté completamente instalada.

Interfaces opcionales

Opcionalmente, puede agregar interfaces adicionales a un nodo. Por ejemplo, es posible que desee agregar una interfaz troncal a un nodo de administración o de puerta de enlace, para poder usar ["Interfaces VLAN"](#) para segregar el tráfico perteneciente a diferentes aplicaciones o inquilinos. O bien, es posible que desee agregar una interfaz de acceso para usar en un ["grupo de alta disponibilidad \(HA\)"](#).

Para agregar interfaces troncales o de acceso, consulte lo siguiente:

- **VMware (después de instalar el nodo):** ["VMware: Agregar interfaces troncales o de acceso a un nodo"](#)
 - **Red Hat Enterprise Linux (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Ubuntu o Debian (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **RHEL, Ubuntu o Debian (después de instalar el nodo):** ["Linux: Agregar interfaces troncales o de acceso a un nodo"](#)

Ver direcciones IP

Puede ver la dirección IP de cada nodo de la red en su sistema StorageGRID. Luego puede utilizar esta dirección IP para iniciar sesión en el nodo de la red en la línea de comando y realizar varios procedimientos de mantenimiento.

Antes de empezar

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

Acerca de esta tarea

Para obtener información sobre cómo cambiar direcciones IP, consulte ["Configurar direcciones IP"](#).

Pasos

1. Seleccione **NODOS > nodo de cuadrícula > Descripción general**.
2. Seleccione **Mostrar más** a la derecha del título Direcciones IP.

Las direcciones IP de ese nodo de la red se enumeran en una tabla.

[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state:  Connected

Storage used:

Object data		7%	?
Object metadata		5%	?

Software version: 11.6.0 (build 20210915.1941.afce2d9)

IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

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

Alerts

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

Configurar interfaces VLAN

Puede crear interfaces de LAN virtual (VLAN) en nodos de administración y nodos de puerta de enlace y usarlas en grupos de alta disponibilidad y puntos finales de equilibrador de carga para aislar y particionar el tráfico para lograr seguridad, flexibilidad y rendimiento. Los nodos seleccionados en el grupo HA pueden usar las interfaces VLAN para compartir hasta 10 direcciones IP virtuales, de modo que si un nodo deja de funcionar, otro nodo se hace cargo del tráfico hacia y desde las direcciones IP virtuales.

Consideraciones para las interfaces VLAN

- Para crear una interfaz VLAN, ingrese una ID de VLAN y elija una interfaz principal en uno o más nodos.
- Se debe configurar una interfaz principal como interfaz troncal en el conmutador.

- Una interfaz principal puede ser la red de cuadrícula (eth0), la red de cliente (eth2) o una interfaz troncal adicional para la máquina virtual o el host físico (por ejemplo, ens256).
- Para cada interfaz VLAN, puede seleccionar solo una interfaz principal para un nodo determinado. Por ejemplo, no puede utilizar la interfaz de red de cuadrícula y 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 VLAN es para el tráfico del nodo de administración, que incluye el tráfico relacionado con el administrador de red y el administrador de inquilinos, seleccione interfaces solo en los nodos de administración.
- Si la interfaz VLAN es para el tráfico del cliente S3, seleccione interfaces en los nodos de administración o en los nodos de puerta de enlace.
- Si necesita agregar interfaces troncales, consulte lo siguiente para obtener más detalles:
 - **VMware (después de instalar el nodo):** ["VMware: Agregar interfaces troncales o de acceso a un nodo"](#)
 - **RHEL (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Ubuntu o Debian (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **RHEL, Ubuntu o Debian (después de instalar el nodo):** ["Linux: Agregar interfaces troncales o de acceso a un nodo"](#)

Crear una interfaz VLAN

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).
- Se ha configurado una interfaz troncal en la red y se ha conectado al nodo VM o Linux. Conoces el nombre de la interfaz troncal.
- Conoces el ID de la VLAN que estás configurando.

Acerca de esta tarea

Es posible que su administrador de red haya configurado una o más interfaces troncales y una o más VLAN para segregar el tráfico de cliente o administrador que pertenece a diferentes aplicaciones o inquilinos. Cada VLAN se identifica mediante una etiqueta o ID numérico. Por ejemplo, su red podría usar VLAN 100 para el tráfico de FabricPool y VLAN 200 para una aplicación de archivo.

Puede utilizar Grid Manager para crear interfaces VLAN que permitan a los clientes acceder a StorageGRID en una VLAN específica. Cuando crea interfaces VLAN, especifica el ID de VLAN y selecciona interfaces principales (troncales) en uno o más nodos.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Interfaces VLAN**.
2. Seleccione **Crear**.

Introduzca detalles para las interfaces VLAN

Pasos

1. Especifique el ID de la VLAN en su red. Puede ingresar cualquier valor entre 1 y 4094.

Los ID de VLAN no necesitan ser únicos. Por ejemplo, puede utilizar el ID de VLAN 200 para el tráfico de administrador en un sitio y el mismo ID 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 el mismo ID no pueden compartir la misma interfaz en un nodo. Si especifica un ID que ya se ha utilizado, aparecerá un mensaje.

2. Opcionalmente, ingrese una breve descripción para la interfaz VLAN.
3. Seleccione **Continuar**.

Seleccionar interfaces principales

La tabla enumera las interfaces disponibles para todos los nodos de administración y nodos de puerta de enlace en cada sitio de su red. Las interfaces de red de administración (eth1) no se pueden usar como interfaces principales y no se muestran.

Pasos

1. Seleccione una o más interfaces principales para conectar 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 administración.

Parent interfaces

Select one or more parent interfaces for this VLAN interface. You can only select one parent interface on each node for each VLAN interface.

	Site ?	Node name ?	Interface ?	Description ?	Node type ?	Attached VLANs ?
☐	Data Center 2	DC2-ADM1	eth0	Grid Network	Non-primary Admin	—
☒	Data Center 2	DC2-ADM1	eth2	Client Network	Non-primary Admin	—
☐	Data Center 1	DC1-G1	eth0	Grid Network	Gateway	—
☒	Data Center 1	DC1-G1	eth2	Client Network	Gateway	—
☐	Data Center 1	DC1-ADM1	eth0	Grid Network	Primary Admin	—

2 interfaces are selected.

[Previous](#)[Continue](#)

2. Seleccione **Continuar**.

Confirmar la configuración

Pasos

1. Revise la configuración y realice los cambios necesarios.
 - Si necesita cambiar la ID o la descripción de la VLAN, seleccione **Ingresar detalles de VLAN** en la parte superior de la página.

- Si necesita cambiar una interfaz principal, seleccione **Elegir interfaces principales** en la parte superior de la página o seleccione **Anterior**.
- Si necesita eliminar 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 se incluya en la tabla **Interfaces de red** del nodo (**NODES > parent interface node > Network**).

Editar una interfaz VLAN

Al editar una interfaz VLAN, puede realizar los siguientes tipos de cambios:

- Cambiar la ID o descripción de la VLAN.
- Agregar o eliminar interfaces principales.

Por ejemplo, es posible que desee eliminar una interfaz principal de una interfaz VLAN si planea dismantelar el nodo asociado.

Tenga en cuenta lo siguiente:

- No se puede cambiar una ID de VLAN si la interfaz de VLAN se utiliza en un grupo de alta disponibilidad.
- No se puede eliminar una interfaz principal si dicha interfaz principal se utiliza en un grupo de alta disponibilidad.

Por ejemplo, supongamos que VLAN 200 está conectada a las interfaces principales de los nodos A y B. Si un grupo HA usa la interfaz VLAN 200 para el nodo A y la interfaz eth2 para el nodo B, puede eliminar la interfaz principal no utilizada para el nodo B, pero no puede eliminar la interfaz principal utilizada para el nodo A.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Interfaces VLAN**.
2. Seleccione la casilla de verificación de la interfaz VLAN que desea editar. Luego, seleccione **Acciones > Editar**.
3. Opcionalmente, actualice el ID de VLAN o la descripción. Luego, seleccione **Continuar**.

No se puede actualizar una ID de VLAN si la VLAN se utiliza en un grupo de alta disponibilidad.

4. Opcionalmente, seleccione o desmarque las casillas de verificación para agregar interfaces principales o eliminar interfaces no utilizadas. Luego, seleccione **Continuar**.
5. Revise la configuración y realice los cambios necesarios.
6. Seleccione **Guardar**.

Eliminar una interfaz VLAN

Puede eliminar una o más interfaces VLAN.

No se puede eliminar una interfaz VLAN si actualmente se utiliza en un grupo HA. Debe eliminar la interfaz VLAN del grupo HA antes de poder eliminarla.

Para evitar interrupciones en el tráfico de clientes, considere realizar una de las siguientes acciones:

- Agregue una nueva interfaz VLAN al grupo HA antes de eliminar esta interfaz VLAN.
- Cree un nuevo grupo HA que no utilice esta interfaz VLAN.
- Si la interfaz VLAN que desea eliminar es actualmente la interfaz activa, edite el grupo HA. Mueva la interfaz VLAN que desea eliminar al final de la lista de prioridades. Espere hasta que se establezca la comunicación en la nueva interfaz principal y luego elimine la interfaz anterior del grupo HA. Por último, elimine la interfaz VLAN en ese nodo.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Interfaces VLAN**.
2. Seleccione la casilla de verificación para cada interfaz VLAN que desee eliminar. Luego, seleccione **Acciones > Eliminar**.
3. Seleccione **Sí** para confirmar su selección.

Se eliminarán todas las interfaces VLAN que seleccionó. Aparece un banner de éxito verde en la página de interfaces VLAN.

Administrar políticas de clasificación de tráfico

¿Qué son las políticas de clasificación de tráfico?

Las políticas de clasificación de tráfico le permiten identificar y monitorear diferentes tipos de tráfico de red. Estas políticas pueden ayudar a limitar y monitorear el tráfico para mejorar sus ofertas de calidad de servicio (QoS).

Las políticas de clasificación de tráfico se aplican a los puntos finales en el servicio StorageGRID Load Balancer para los nodos de puerta de enlace y los nodos de administración. Para crear políticas de clasificación de tráfico, es necesario que ya haya creado puntos finales del balanceador de carga.

Reglas de coincidencia

Cada política de clasificación de tráfico contiene una o más reglas de coincidencia para identificar el tráfico de red relacionado con una o más de las siguientes entidades:

- Cubos
- Subred
- Arrendatario
- Puntos finales del balanceador de carga

StorageGRID monitorea el tráfico que coincide con cualquier regla dentro de la política según los objetivos de la regla. Cualquier tráfico que coincida con alguna regla de una política es manejado por esa política. Por el contrario, puedes establecer reglas para que coincidan con todo el tráfico excepto una entidad específica.

Limitación del tráfico

Opcionalmente, puede agregar los siguientes tipos de límites a una política:

- Ancho de banda agregado
- Ancho de banda por solicitud
- Solicitudes concurrentes

- Tarifa de solicitud

Los valores límite se aplican según cada equilibrador de carga. Si el tráfico se distribuye simultáneamente entre varios balanceadores de carga, las velocidades 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 al mismo tiempo. Los límites de ancho de banda agregados pueden imponer un impacto menor adicional en el rendimiento del tráfico no limitado.

Para límites de ancho de banda agregados o por solicitud, las solicitudes entran o salen a la velocidad que usted establezca. StorageGRID solo puede aplicar una velocidad, por lo que la coincidencia de política más específica, por tipo de comparador, es la que se aplica. El ancho de banda consumido por la solicitud no se tiene en cuenta para otras políticas de coincidencia menos específicas que contienen políticas de límite de ancho de banda agregado. Para todos los demás tipos de límites, las solicitudes de los clientes se retrasan 250 milisegundos y reciben una respuesta 503 Slow Down para las solicitudes que exceden cualquier límite de política coincidente.

En el Administrador de cuadrícula, puede ver gráficos de tráfico y verificar que las políticas estén aplicando los límites de tráfico esperados.

Utilice políticas de clasificación de tráfico con SLA

Puede utilizar políticas de clasificación de tráfico junto con límites de capacidad y protección de datos para aplicar acuerdos de nivel de servicio (SLA) que proporcionen detalles específicos sobre la capacidad, la protección de datos y el rendimiento.

El siguiente ejemplo muestra tres niveles de un SLA. Puede crear políticas de clasificación de tráfico para lograr los objetivos de rendimiento de cada nivel de SLA.

Nivel de servicio	Capacidad	Protección de datos	Máximo rendimiento permitido	Costo
Oro	Se permite 1 PB de almacenamiento	3 copia la regla ILM	25 K solicitudes/seg Ancho de banda de 5 GB/seg (40 Gbps)	\$\$\$ por mes
Plata	Se permiten 250 TB de almacenamiento	2 copia la regla ILM	10 K solicitudes/seg 1,25 GB/seg (10 Gbps) de ancho de banda	\$\$ por mes
Bronce	Se permiten 100 TB de almacenamiento	2 copia la regla ILM	5 K solicitudes/seg 1 GB/seg (8 Gbps) de ancho de banda	\$ por mes

Crear políticas de clasificación de tráfico

Puede crear políticas de clasificación de tráfico si desea monitorear y, opcionalmente, limitar el tráfico de red por depósito, expresión regular de depósito, CIDR, punto final del balanceador de carga o inquilino. Opcionalmente, puede establecer límites para una política en función del ancho de banda, la cantidad de solicitudes simultáneas o la tasa de solicitudes.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .
- Ha creado todos los puntos finales del balanceador de carga que desea que coincidan.
- Has creado todos los inquilinos que quieres emparejar.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Red** > **Clasificación de tráfico**.
2. Seleccione **Crear**.
3. Ingrese un nombre y una descripción (opcional) para la política y seleccione **Continuar**.

Por ejemplo, describa a qué se aplica esta política de clasificación de tráfico y qué limitará.

4. Seleccione **Agregar regla** y especifique los siguientes detalles para crear una o más reglas coincidentes para la política. Cualquier política que cree debe tener al menos una regla coincidente. Seleccione **Continuar**.

Campo	Descripción
Tipo	Seleccione los tipos de tráfico a los que se aplica la regla de coincidencia. Los tipos de tráfico son bucket, regex de bucket, CIDR, punto final del equilibrador de carga e inquilino.

Campo	Descripción
Valor de coincidencia	Introduzca el valor que coincida con el tipo seleccionado. • Cubo: Ingrese uno o más nombres de cubo. • Expresión regular de depósito: ingrese una o más expresiones regulares utilizadas para hacer coincidir un conjunto de nombres de depósito. La expresión regular no está anclada. Utilice el ancla ^ para que coincida al principio del nombre del depósito, y utilice el ancla \$ para que coincida al final del nombre. La coincidencia de expresiones regulares admite un subconjunto de la sintaxis PCRE (expresión regular compatible con Perl). • CIDR: ingrese una o más subredes IPv4, en notación CIDR, que coincidan con la subred deseada. • Punto final del equilibrador de carga: seleccione un nombre de punto final. Estos son los puntos finales del balanceador de carga que definió en el "Configurar los puntos finales del balanceador de carga". • Inquilino: la coincidencia de inquilinos utiliza el ID de la clave de acceso. Si la solicitud no contiene un ID de clave de acceso (por ejemplo, acceso anónimo), se utiliza la propiedad del depósito al que se accede para determinar el inquilino.
Partido inverso	Si desea hacer coincidir todo el tráfico de la red <i>excepto</i> el tráfico consistente con el Tipo y el Valor de coincidencia que acaba de definir, seleccione la casilla de verificación Coincidencia inversa. De lo contrario, deje la casilla de verificación sin marcar. Por ejemplo, si desea que esta política se aplique a todos los puntos finales del balanceador de carga excepto uno, especifique el punto final del balanceador de carga que se excluirá y seleccione Coincidencia inversa. Para una política que contiene varios comparadores donde al menos uno es un comparador inverso, tenga cuidado de no crear una política que coincida con todas las solicitudes.

5. Opcionalmente, seleccione **Agregar un límite** y seleccione los siguientes detalles para agregar uno o más límites para controlar el tráfico de red que coincide con una regla.



StorageGRID recopila métricas incluso si no agrega ningún límite, para que pueda comprender las tendencias de tráfico.

Campo	Descripción
Tipo	El tipo de límite que desea aplicar al tráfico de red que coincide con la regla. Por ejemplo, puede limitar el ancho de banda o la velocidad de solicitud. Nota: 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 al mismo tiempo. Cuando se utiliza el ancho de banda agregado, el ancho de banda por solicitud no está disponible. Por el contrario, cuando se utiliza el ancho de banda por solicitud, el ancho de banda agregado no está disponible. Los límites de ancho de banda agregados pueden imponer un impacto menor adicional en el rendimiento del tráfico no limitado. Para los límites de ancho de banda, StorageGRID aplica la política que mejor coincide con el tipo de límite establecido. Por ejemplo, si tiene una política que limita el tráfico en una sola dirección, entonces el tráfico en la dirección opuesta será ilimitado, incluso si hay tráfico que coincida con políticas adicionales que tienen límites de ancho de banda. StorageGRID implementa las "mejores" coincidencias para los límites de ancho de banda en el siguiente orden: • Dirección IP exacta (máscara /32) • Nombre exacto del depósito • Expresión regular de cubo • Arrendatario • Punto final • Coincidencias CIDR no exactas (no /32) • Coincidencias inversas
Se aplica a	Si este límite se aplica a solicitudes de lectura del cliente (GET o HEAD) o solicitudes de escritura (PUT, POST o DELETE).
Valor	El valor al que se limitará el tráfico de red, según la unidad que seleccione. Por ejemplo, ingrese 10 y seleccione MiB/s para evitar que el tráfico de red que coincide con esta regla supere los 10 MiB/s. Nota: Dependiendo de la configuración de las unidades, las unidades disponibles serán binarias (por ejemplo, GiB) o decimales (por ejemplo, GB). Para cambiar la configuración de las unidades, seleccione el menú desplegable de usuario en la parte superior derecha del Administrador de cuadrícula, luego seleccione Preferencias de usuario.
Unidad	La unidad que describe el valor ingresado.

Por ejemplo, si desea crear un límite de ancho de banda de 40 GB/s para un nivel de SLA, cree dos límites de ancho de banda agregados: GET/HEAD a 40 GB/s y PUT/POST/DELETE a 40 GB/s.

6. Seleccione **Continuar**.

7. Lea y revise la política de clasificación de tráfico. Utilice el botón **Anterior** para volver atrás y realizar los cambios necesarios. Cuando esté satisfecho con la política, seleccione **Guardar y continuar**.

El tráfico del cliente S3 ahora se maneja de acuerdo con la política de clasificación de tráfico.

Después de terminar

"[Ver métricas de tráfico de red](#)" para verificar que las políticas estén haciendo cumplir los límites de tráfico esperados.

Editar la política de clasificación de tráfico

Puede editar una política de clasificación de tráfico para cambiar su nombre o descripción, o para crear, editar o eliminar cualquier regla o límite para la política.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tú tienes el "[Permiso de acceso root](#)".

Pasos

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

Aparece la página de Políticas de clasificación de tráfico y las políticas existentes se enumeran en una tabla.

2. Edite la política utilizando el menú Acciones o la página de detalles. Ver "[crear políticas de clasificación de tráfico](#)" para qué entrar.

Menú de acciones

- a. Seleccione la casilla de verificación de la política.
- b. Seleccione **Acciones > Editar**.

Página de detalles

- a. Seleccione el nombre de la política.
- b. Seleccione el botón **Editar** junto al nombre de la política.

3. Para el paso Ingresar nombre de política, opcionalmente edite el nombre o la descripción de la política y seleccione **Continuar**.
4. Para el paso Agregar reglas coincidentes, opcionalmente agregue una regla o edite el **Tipo** y el **Valor de coincidencia** de la regla existente y seleccione **Continuar**.
5. Para el paso Establecer límites, opcionalmente agregue, edite o elimine un límite y seleccione **Continuar**.
6. Revise la política actualizada y seleccione **Guardar y continuar**.

Los cambios realizados en la política se guardan y el tráfico de red ahora se maneja de acuerdo con las políticas de clasificación de tráfico. Puede ver los gráficos de tráfico y verificar que las políticas estén aplicando los límites de tráfico esperados.

Eliminar una política de clasificación de tráfico

Puede eliminar una política de clasificación de tráfico si ya no la necesita. Asegúrese de eliminar la política correcta porque una política no se puede recuperar una vez eliminada.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .

Pasos

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

La página de Políticas de clasificación de tráfico aparece con las políticas existentes enumeradas en una tabla.

2. Elimine la política mediante el menú Acciones o la página de detalles.

Menú de acciones

- a. Seleccione la casilla de verificación de la política.
- b. Seleccione **Acciones > Eliminar**.

Página de detalles de la política

- a. Seleccione el nombre de la política.
- b. Seleccione el botón **Eliminar** junto al nombre de la política.

3. Seleccione **Sí** para confirmar que desea eliminar la política.

La política se elimina.

Ver métricas de tráfico de red

Puede supervisar el tráfico de la red viendo los gráficos disponibles en la página Políticas de clasificación de tráfico.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso de root o de cuentas de inquilino"](#) .

Acerca de esta tarea

Para cualquier política de clasificación de tráfico existente, puede ver las métricas del servicio de balanceador de carga para determinar si la política está limitando exitosamente el tráfico en la red. Los datos en los gráficos pueden ayudarle a determinar si necesita ajustar la política.

Incluso si no se establecen límites para una política de clasificación de tráfico, se recopilan métricas y los gráficos proporcionan información útil para comprender las tendencias del tráfico.

Pasos

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

Aparece la página de Políticas de clasificación de tráfico y las políticas existentes se enumeran en la tabla.

2. Seleccione el nombre de la política de clasificación de tráfico cuyas métricas desea ver.
3. Seleccione la pestaña **Métricas**.

Aparecen los gráficos de la política de clasificación de tráfico. Los gráficos muestran métricas solo para el tráfico que coincide con la política seleccionada.

Los siguientes gráficos se incluyen en la página.

- Tasa de solicitud: este gráfico proporciona la cantidad de ancho de banda que coincide con esta política manejada por todos los balanceadores de carga. Los datos recibidos incluyen los encabezados de solicitud para todas las solicitudes y el tamaño de los datos del cuerpo para las respuestas que tienen datos del cuerpo. Enviado incluye encabezados de respuesta para todas las solicitudes y el tamaño de los datos del cuerpo de respuesta para las solicitudes que incluyen datos del cuerpo en la respuesta.



Cuando se completan las solicitudes, este gráfico solo muestra el uso del ancho de banda. Para solicitudes de objetos grandes o lentos, el ancho de banda instantáneo real puede diferir de los valores informados en este gráfico.

- Tasa de respuesta de error: este gráfico proporciona una tasa aproximada a la que las solicitudes que coinciden con esta política devuelven errores (código de estado HTTP ≥ 400) a los clientes.
 - Duración promedio de la solicitud (sin errores): este gráfico proporciona una duración promedio de las solicitudes exitosas que coinciden con esta política.
 - Uso del ancho de banda de la política: este gráfico proporciona la cantidad de ancho de banda que coincide con esta política manejada por todos los balanceadores de carga. Los datos recibidos incluyen los encabezados de solicitud para todas las solicitudes y el tamaño de los datos del cuerpo para las respuestas que tienen datos del cuerpo. Enviado incluye encabezados de respuesta para todas las solicitudes y el tamaño de los datos del cuerpo de respuesta para las solicitudes que incluyen datos del cuerpo en la respuesta.
4. Coloque el cursor sobre un gráfico de líneas para ver una ventana emergente de valores en una parte específica del gráfico.
 5. Seleccione **Panel de Grafana** justo debajo del título Métricas para ver todos los gráficos de una política. Además de los cuatro gráficos de la pestaña **Métricas**, puedes ver dos gráficos más:
 - Tasa de solicitud de escritura por tamaño de objeto: la tasa de solicitudes PUT/POST/DELETE que coinciden con esta política. El posicionamiento en una celda individual muestra las velocidades por segundo. Las tarifas que se muestran en la vista flotante se truncan a recuentos de números enteros y pueden informar 0 cuando hay solicitudes distintas de cero en el depósito.
 - Tasa de solicitud de lectura por tamaño de objeto: la tasa de solicitudes GET/HEAD que coinciden con esta política. El posicionamiento en una celda individual muestra las velocidades por segundo. Las tarifas que se muestran en la vista flotante se truncan a recuentos de números enteros y pueden informar 0 cuando hay solicitudes distintas de cero en el depósito.
 6. Alternativamente, acceda a los gráficos desde el menú **SOPORTE**.
 - a. Seleccione **SOPORTE > Herramientas > Métricas**.
 - b. Seleccione **Política de clasificación de tráfico** en la sección **Grafana**.
 - c. Seleccione la política del menú en la parte superior izquierda de la página.
 - d. Coloque el cursor sobre un gráfico para ver una ventana emergente que muestra la fecha y la hora de la muestra, los tamaños de los objetos que se agregan en el recuento y la cantidad de solicitudes por

segundo durante ese período de tiempo.

Las políticas de clasificación de tráfico se identifican por su ID. Los ID de políticas se enumeran en la página de políticas de clasificación de tráfico.

7. Analice los gráficos para determinar con qué frecuencia la política limita el tráfico y si necesita ajustarla.

Cifrados compatibles para conexiones TLS salientes

El sistema StorageGRID admite un conjunto limitado de conjuntos de cifrados para conexiones de seguridad de la capa de transporte (TLS) a los sistemas externos utilizados para la federación de identidades y los grupos de almacenamiento en la nube.

Versiones compatibles de TLS

StorageGRID admite TLS 1.2 y TLS 1.3 para conexiones a sistemas externos utilizados para la federación de identidades y grupos de almacenamiento en la nube.

Los cifrados TLS compatibles con el uso de sistemas externos se han seleccionado para garantizar la compatibilidad con una variedad de sistemas externos. La lista es más grande que la lista de cifrados compatibles para su uso con aplicaciones cliente S3. Para configurar cifrados, vaya a **CONFIGURACIÓN > Seguridad > Configuración de seguridad** y seleccione **Políticas TLS y SSH**.



Las opciones de configuración de TLS, como versiones de protocolo, cifrados, algoritmos de intercambio de claves y algoritmos MAC, no se pueden configurar en StorageGRID. Comuníquese con su representante de cuenta de NetApp si tiene solicitudes específicas sobre estas configuraciones.

Beneficios de las conexiones HTTP activas, inactivas y simultáneas

La forma en que configura las conexiones HTTP puede afectar el rendimiento del sistema StorageGRID. Las configuraciones difieren dependiendo de si la conexión HTTP está activa o inactiva o si tiene múltiples conexiones simultáneas.

Puede identificar los beneficios de rendimiento para los siguientes tipos de conexiones HTTP:

- Conexiones HTTP inactivas
- Conexiones HTTP activas
- Conexiones HTTP concurrentes

Beneficios de mantener abiertas las conexiones HTTP inactivas

Debe mantener abiertas las conexiones HTTP incluso cuando las aplicaciones cliente estén inactivas para permitir que las aplicaciones cliente realicen transacciones posteriores a través de la conexión abierta. Según las mediciones del sistema y la experiencia de integración, debe mantener una conexión HTTP inactiva abierta durante un máximo de 10 minutos. StorageGRID podría cerrar automáticamente una conexión HTTP que permanezca abierta e inactiva durante más de 10 minutos.

Las conexiones HTTP abiertas e inactivas proporcionan los siguientes beneficios:

- Latencia reducida 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 principal ventaja, especialmente por el tiempo necesario para establecer conexiones TCP/IP y TLS.

- Aumento de la velocidad de transferencia de datos al activar el algoritmo de inicio lento TCP/IP con transferencias realizadas previamente
- Notificación instantánea de varias clases de condiciones de falla que interrumpen la conectividad entre la aplicación cliente y el sistema StorageGRID

Determinar cuánto tiempo mantener abierta una conexión inactiva es una cuestión de equilibrio entre los beneficios del inicio lento asociado con la conexión existente y la asignación ideal de la conexión a los recursos internos del sistema.

Beneficios de las conexiones HTTP activas

Para las conexiones directas a los nodos de almacenamiento, debe limitar la duración de una conexión HTTP activa a un máximo de 10 minutos, incluso si la conexión HTTP realiza transacciones continuamente.

Determinar la duración máxima que una conexión debe mantenerse abierta es un equilibrio entre los beneficios de la persistencia de la conexión y la asignación ideal de la conexión a los recursos internos del sistema.

Para las conexiones de clientes a nodos de almacenamiento, limitar las conexiones HTTP activas proporciona los siguientes beneficios:

- Permite un equilibrio de carga óptimo en todo el sistema StorageGRID .

Con el tiempo, una conexión HTTP puede dejar de ser óptima a medida que cambian los requisitos de equilibrio de carga. El sistema logra su mejor equilibrio de carga cuando las aplicaciones cliente establecen una conexión HTTP separada para cada transacción, pero esto anula las ganancias mucho más valiosas asociadas con las conexiones persistentes.

- Permite que las aplicaciones cliente dirijan transacciones HTTP a servicios LDR que tengan espacio disponible.
- Permite iniciar procedimientos de mantenimiento.

Algunos procedimientos de mantenimiento comienzan solo después de que se hayan completado todas las conexiones HTTP en curso.

Para las conexiones de clientes al servicio Load Balancer, limitar la duración de las conexiones abiertas puede ser útil para permitir que algunos procedimientos de mantenimiento se inicien rápidamente. Si la duración de las conexiones del cliente no está limitada, es posible que pasen varios minutos hasta que las conexiones activas finalicen automáticamente.

Beneficios de las conexiones HTTP concurrentes

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 una variedad de factores.

Las conexiones HTTP simultáneas proporcionan los siguientes beneficios:

- Latencia reducida

Las transacciones pueden comenzar inmediatamente en lugar de esperar a que se completen otras transacciones.

- Mayor rendimiento

El sistema StorageGRID puede realizar transacciones paralelas y aumentar el rendimiento de las transacciones agregadas.

Las aplicaciones cliente deben establecer múltiples 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.

La topología de cada sistema StorageGRID tiene un rendimiento máximo diferente para transacciones y conexiones simultáneas antes de que el rendimiento comience a degradarse. El rendimiento máximo depende de factores como los recursos informáticos, los recursos de red, los recursos de almacenamiento y los enlaces WAN. La cantidad de servidores y servicios y la cantidad de aplicaciones que admite el sistema StorageGRID también son factores.

Los sistemas StorageGRID suelen admitir múltiples aplicaciones cliente. Debe tener esto en cuenta al determinar la cantidad máxima de conexiones simultáneas utilizadas por una aplicación cliente. Si la aplicación cliente consta de varias entidades de software que establecen conexiones con el sistema StorageGRID, debe sumar todas las conexiones entre las entidades. Es posible que tengas que ajustar el número máximo de conexiones simultáneas en las siguientes situaciones:

- La topología del sistema StorageGRID afecta la cantidad máxima de transacciones y conexiones simultáneas que el sistema puede admitir.
- Las aplicaciones cliente que interactúan con el sistema StorageGRID a través de una red con ancho de banda limitado podrían tener que reducir el grado de simultaneidad para garantizar que las transacciones individuales se completen en un tiempo razonable.
- Cuando muchas aplicaciones cliente comparten el sistema StorageGRID, es posible que deba reducir el grado de simultaneidad para evitar exceder los límites del sistema.

Separación de grupos de conexiones HTTP para operaciones de lectura y escritura

Puede utilizar grupos separados de conexiones HTTP para operaciones de lectura y escritura y controlar qué parte de un grupo utilizar para cada una. 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 en la recuperación (lectura) o dominantes en el almacenamiento (escritura). Con grupos separados de conexiones HTTP para transacciones de lectura y escritura, puede ajustar qué parte de cada grupo dedicar a transacciones de lectura o escritura.

Administrar los costos de los enlaces

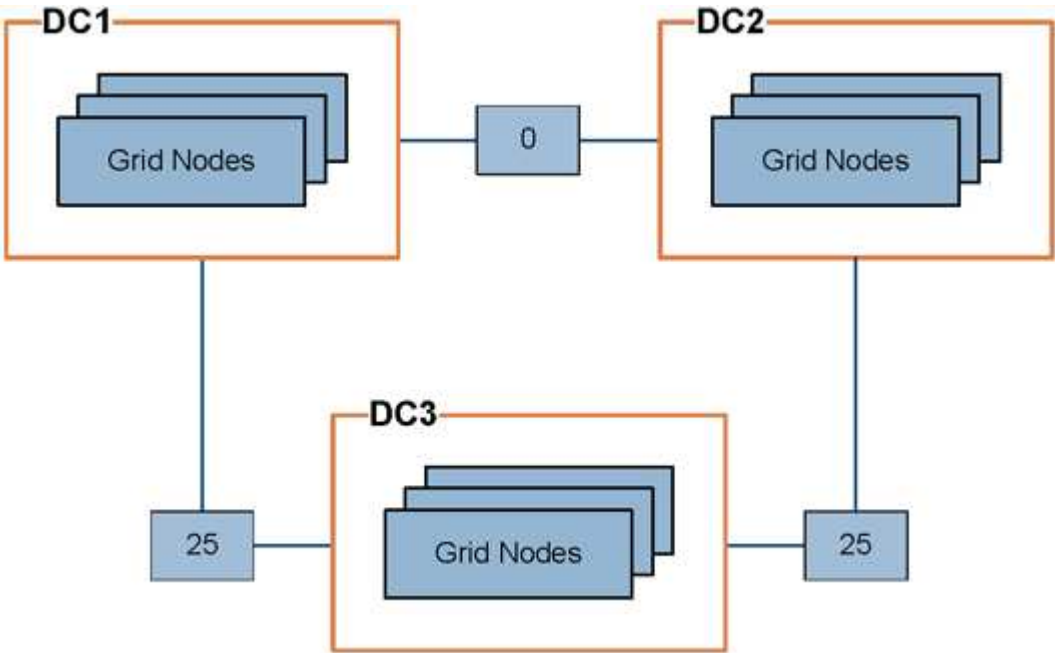
Los costos de enlace le permiten priorizar qué sitio del centro de datos proporciona un servicio solicitado cuando existen dos o más sitios de centros de datos. Puede ajustar los costos de los enlaces para reflejar la latencia entre sitios.

¿Qué son los costos de enlace?

- Los costos de enlace se utilizan para priorizar qué copia de objeto se utiliza para completar las recuperaciones de objetos.
- La API de administración de red y la API de administración de inquilinos utilizan los costos de enlace para determinar qué servicios internos de StorageGRID utilizar.
- El servicio Load Balancer utiliza los costos de enlace en los nodos de administración y los nodos de puerta

de enlace para dirigir las conexiones de los clientes. Ver ["Consideraciones para el equilibrio de carga"](#) .

El diagrama muestra una cuadrícula de tres sitios que tiene costos de enlace configurados entre sitios:



- El servicio Load Balancer en los nodos de administración y los nodos de puerta de enlace distribuye equitativamente las conexiones de los clientes a todos los nodos de almacenamiento en el mismo sitio del centro de datos y a cualquier sitio del centro de datos con un costo de enlace de 0.

En el ejemplo, un nodo de puerta de enlace en el sitio del centro de datos 1 (DC1) distribuye equitativamente las conexiones de cliente a los nodos de almacenamiento en DC1 y a los nodos de almacenamiento en DC2. Un nodo de puerta de enlace en DC3 envía conexiones de cliente únicamente a nodos de almacenamiento en DC3.

- Al recuperar un objeto que existe como múltiples copias replicadas, StorageGRID recupera la copia en el centro de datos que tiene el costo de enlace más bajo.

En el ejemplo, si una aplicación cliente en DC2 recupera un objeto que está almacenado tanto en DC1 como en DC3, el objeto se recupera de DC1, porque el costo del enlace de DC1 a DC2 es 0, que es menor que el costo del enlace de DC3 a DC2 (25).

Los costos de enlace son números relativos arbitrarios sin una unidad de medida específica. Por ejemplo, un coste de enlace de 50 se utiliza con menos preferencia que un coste de enlace de 25. La tabla muestra los costos de enlaces más utilizados.

Enlace	Costo del enlace	Notas
Entre sitios de centros de datos físicos	25 (predeterminado)	Centros de datos conectados mediante un enlace WAN.
Entre sitios de centros de datos lógicos en la misma ubicación física	0	Centros de datos lógicos en el mismo edificio físico o campus conectados por una LAN.

Costos de actualización de enlaces

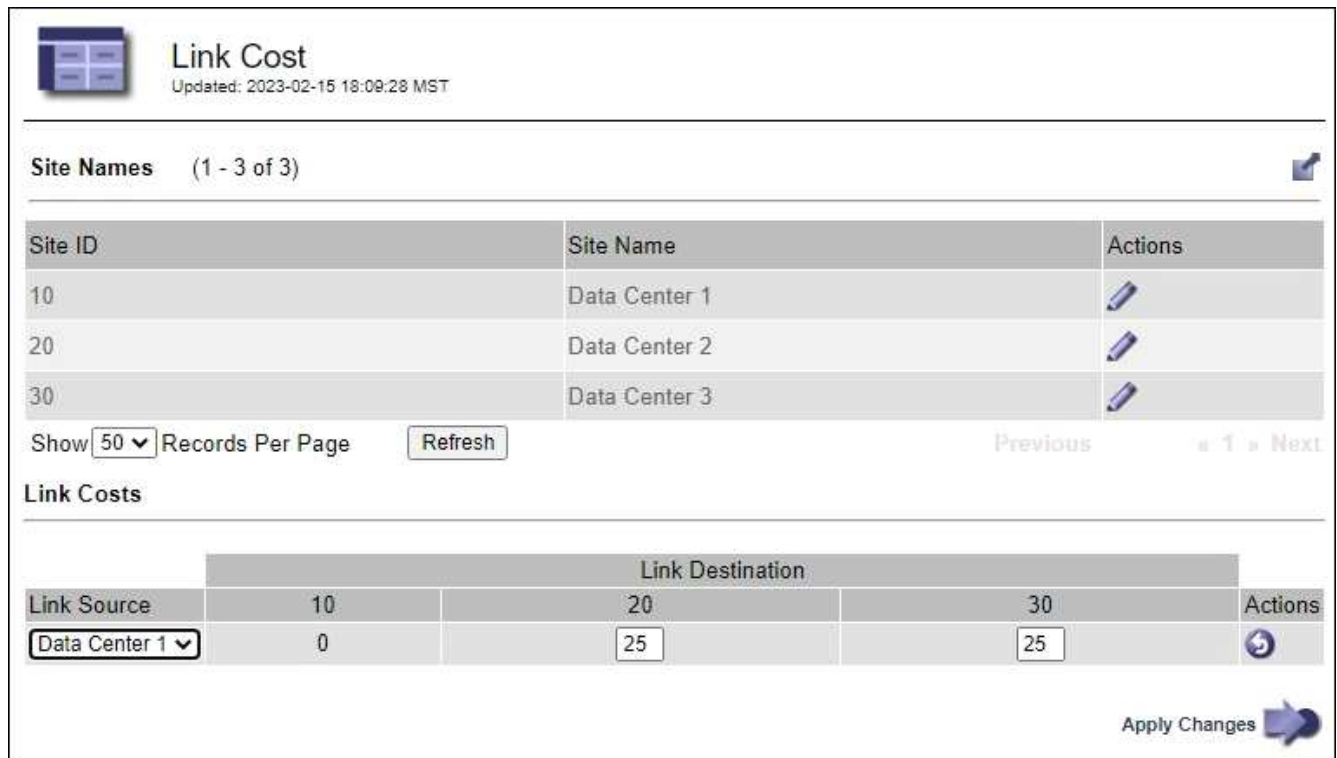
Puede actualizar los costos de enlace entre los sitios de los centros de datos para reflejar la latencia entre sitios.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de configuración de la página de topología de cuadrícula"](#) .

Pasos

1. Seleccione **SOPORTE > Otro > Costo del enlace**.



Link Cost
Updated: 2023-02-15 18:09:28 MST

Site Names (1 - 3 of 3)

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	
30	Data Center 3	

Show Records Per Page Previous 1 Next

Link Costs

Link Source	10	20	30	Actions
Data Center 1	0	25	25	



2. Seleccione un sitio en **Fuente del enlace** e ingrese un valor de costo entre 0 y 100 en **Destino del enlace**.

No puedes cambiar el costo del enlace si el origen es el mismo que el destino.

Para cancelar los cambios, seleccione  **Revertir**.

3. Seleccione **Aplicar cambios**.

Utilice AutoSupport

¿Qué es AutoSupport?

La función AutoSupport permite que StorageGRID envíe paquetes de estado y salud al soporte técnico de NetApp .

El uso de AutoSupport puede acelerar significativamente la determinación y resolución de problemas. El soporte técnico también puede monitorear las necesidades de almacenamiento de su sistema y ayudarlo a determinar si necesita agregar nuevos nodos o sitios. Opcionalmente, puede configurar los paquetes de

AutoSupport para que se envíen a un destino adicional.

StorageGRID tiene dos tipos de AutoSupport:

- * StorageGRID AutoSupport* informa problemas de software de StorageGRID . Habilitado de forma predeterminada cuando instala StorageGRID por primera vez. Puede ["cambiar la configuración predeterminada de AutoSupport"](#) Si es necesario.



Si StorageGRID 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 memoria caché de su navegador, incluso si AutoSupport permanece deshabilitado.

- * AutoSupport de hardware del dispositivo* informa problemas con el dispositivo StorageGRID . Usted debe ["Configurar AutoSupport de hardware en cada dispositivo"](#) .

¿Qué es Active IQ?

Active IQ es un asesor digital basado en la nube que aprovecha el análisis predictivo y la sabiduría de la comunidad de la base instalada de NetApp. Sus evaluaciones de riesgos continuas, alertas predictivas, orientación prescriptiva y acciones automatizadas lo ayudan a prevenir problemas antes de que ocurran, lo que genera una mejor salud del sistema y una mayor disponibilidad del sistema.

Si desea utilizar los paneles y la funcionalidad de Active IQ en el sitio de soporte de NetApp , debe habilitar AutoSupport.

["Documentación del Digital Advisor Active IQ"](#)

Información incluida en el paquete AutoSupport

Un paquete de AutoSupport contiene los siguientes archivos y detalles.

Nombre del archivo	Campos	Descripción
HISTORIAL DE AUTOSOPORTE.XML	Número de secuencia de AutoSupport + Destino para este AutoSupport + Estado de entrega + Intentos de entrega + Asunto de AutoSupport + URI de entrega + Último error + Nombre de archivo PUT de AutoSupport + Hora de generación + Tamaño comprimido de AutoSupport + Tamaño descomprimido de AutoSupport + Tiempo total de recopilación (ms)	Archivo de historial de AutoSupport .

Nombre del archivo	Campos	Descripción
AUTOSOPORTE.XML	Nodo + Protocolo para contactar con soporte + URL de soporte para HTTP/HTTPS + Dirección de soporte + Estado de AutoSupport OnDemand + URL del servidor de AutoSupport OnDemand + Intervalo de sondeo de AutoSupport OnDemand	Archivo de estado de AutoSupport . Proporciona detalles del protocolo utilizado, la URL y la dirección de soporte técnico, el intervalo de sondeo y el AutoSupport a pedido si está habilitado o deshabilitado.
CUBOS.XML	ID de bucket + ID de cuenta + Versión de compilación + Configuración de restricción de ubicación + Cumplimiento habilitado + Configuración de cumplimiento + Bloqueo de objetos S3 habilitado + Configuración de bloqueo de objetos S3 + Configuración de consistencia + CORS habilitado + Configuración de CORS + Hora del último acceso habilitada + Política habilitada + Configuración de política + Notificaciones habilitadas + Configuración de notificaciones + Espejo en la nube habilitado + Configuración de espejo en la nube + Búsqueda habilitada + Configuración de búsqueda + Etiquetado de bucket habilitado + Configuración de etiquetado de bucket + Configuración de control de versiones	Proporciona detalles de configuración y estadísticas a nivel de depósito. Algunos ejemplos de configuraciones de bucket incluyen servicios de plataforma, cumplimiento y consistencia de bucket.
CONFIGURACIONES DE RED.XML	ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Archivo de información de configuración de toda la red. Contiene información sobre certificados de red, espacio reservado de metadatos, configuraciones de toda la red (cumplimiento, bloqueo de objetos S3, compresión de objetos, alertas, syslog y configuración de ILM), detalles del perfil de codificación de borrado, nombre DNS y "Nombre NMS" .

Nombre del archivo	Campos	Descripción
GRID-SPEC.XML	Especificaciones de la cuadrícula, XML sin procesar	Se utiliza para configurar e implementar StorageGRID. Contiene especificaciones de la red, IP del servidor NTP, IP del servidor DNS, topología de red y perfiles de hardware de los nodos.
GRID-TAREAS.XML	Nodo + Ruta de servicio + ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Archivo de estado de tareas de red (procedimientos de mantenimiento). Proporciona detalles de las tareas activas, finalizadas, completadas, fallidas y pendientes de la red.
CUADRÍCULA.JSON	Grid + Revisión + Versión de software + Descripción + Licencia + Contraseñas + DNS + NTP + Sitios + Nodos	Información de la cuadrícula.
ILM-CONFIGURACIÓN.XML	ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Lista de atributos para configuraciones de ILM.
ILM-STATUS.XML	Nodo + Ruta de servicio + ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Archivo de información de métricas ILM. Contiene tasas de evaluación de ILM para cada nodo y métricas de toda la red.
ILM.XML	XML sin procesar de ILM	Archivo de política activa de ILM. Contiene detalles sobre las políticas ILM activas, como ID de grupo de almacenamiento, comportamiento de ingesta, filtros, reglas y descripción.
REGISTRO.TGZ	<i>n / A</i>	Archivo de registro descargable. Contiene <code>broadcast-err.log</code> y <code>servermanager.log</code> desde cada nodo.
MANIFIESTO.XML	Orden de recopilación + Nombre del archivo de contenido de AutoSupport para estos datos + Descripción de este elemento de datos + Número de bytes recopilados + Tiempo dedicado a la recopilación + Estado de este elemento de datos + Descripción del error + Tipo de contenido de AutoSupport para estos datos +	Contiene metadatos de AutoSupport y breves descripciones de todos los archivos de AutoSupport .

Nombre del archivo	Campos	Descripción
ENTIDADES NMS.XML	Índice de atributo + OID de entidad + ID de nodo + ID de modelo de dispositivo + Versión de modelo de dispositivo + Nombre de entidad	Entidades de grupo y de servicios en el " Árbol NMS ". Proporciona detalles de la topología de la red. El nodo se puede determinar en función de los servicios que se ejecutan en el nodo.
OBJETOS-ESTADO.XML	Nodo + Ruta de servicio + ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Estado del objeto, incluido el estado de escaneo en segundo plano, transferencia activa, velocidad de transferencia, transferencias totales, velocidad de eliminación, fragmentos dañados, objetos perdidos, objetos faltantes, reparación intentada, velocidad de escaneo, período de escaneo estimado y estado de finalización de la reparación.
ESTADO DEL SERVIDOR.XML	Nodo + Ruta de servicio + ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Configuraciones del servidor. Contiene estos detalles para cada nodo: tipo de plataforma, sistema operativo, memoria instalada, memoria disponible, conectividad de almacenamiento, número de serie del chasis del dispositivo de almacenamiento, recuento de unidades fallidas del controlador de almacenamiento, temperatura del chasis del controlador de cómputo, hardware de cómputo, número de serie del controlador de cómputo, fuente de alimentación, tamaño de la unidad y tipo de unidad.
ESTADO DEL SERVICIO.XML	Nodo + Ruta de servicio + ID de atributo + Nombre de atributo + Valor + Índice + ID de tabla + Nombre de tabla	Archivo de información del nodo de servicio. Contiene detalles como espacio de tabla asignado, espacio de tabla libre, métricas de Reaper de la base de datos, duración de reparación de segmento, duración del trabajo de reparación, reinicios automáticos de trabajos y finalización automática de trabajos.
GRADOS DE ALMACENAMIENTO.XML	ID de grado de almacenamiento + Nombre de grado de almacenamiento + ID de nodo de almacenamiento + Ruta del nodo de almacenamiento	Archivo de definiciones de grado de almacenamiento para cada nodo de almacenamiento.

Nombre del archivo	Campos	Descripción
RESUMEN-ATRIBUTOS.XML	OID de grupo + Ruta de grupo + ID de atributo de resumen + Nombre de atributo de resumen + Valor + Índice + ID de tabla + Nombre de tabla	Datos de estado del sistema de alto nivel que resumen la información de uso de StorageGRID . Proporciona detalles como el nombre de la red, los nombres de los sitios, la cantidad de nodos de almacenamiento por red y por sitio, el tipo de licencia, la capacidad y el uso de la licencia, los términos de soporte del software y los detalles de las operaciones de S3.
ALERTAS DEL SISTEMA.XML	Nombre + Gravedad + Nombre del nodo + Estado de la alerta + Nombre del sitio + Hora de activación de la alerta + Hora de resolución de la alerta + ID de regla + ID del nodo + ID del sitio + Silenciado + Otras anotaciones + Otras etiquetas	Alertas actuales del sistema que indican problemas potenciales en el sistema StorageGRID .
USERAGENTS.XML	Agente de usuario + Número de días + Total de solicitudes HTTP + Total de bytes ingeridos + Total de bytes recuperados + Solicitudes PUT + Solicitudes GET + Solicitudes DELETE + Solicitudes HEAD + Solicitudes POST + Solicitudes OPTIONS + Tiempo promedio de solicitud (ms) + Tiempo promedio de solicitud PUT (ms) + Tiempo promedio de solicitud GET (ms) + Tiempo promedio de solicitud DELETE (ms) + Tiempo promedio de solicitud HEAD (ms) + Tiempo promedio de solicitud POST (ms) + Tiempo promedio de solicitud OPTIONS (ms)	Estadísticas basadas en los agentes de usuario de la aplicación. Por ejemplo, la cantidad de operaciones PUT/GET/DELETE/HEAD por agente de usuario y el tamaño total de bytes de cada operación.
DATOS DEL ENCABEZADO X	X-Netapp-asup-generado-en + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject + X-Netapp-asup-system-id + X-Netapp-asup-model-name +	Datos de encabezado de AutoSupport .

Configurar AutoSupport

De forma predeterminada, la función StorageGRID AutoSupport está habilitada cuando instala StorageGRID por primera vez. Sin embargo, debe configurar AutoSupport de hardware en cada dispositivo. Según sea necesario, puede cambiar la configuración de AutoSupport .

Si desea cambiar la configuración de StorageGRID AutoSupport, realice los cambios solo en el nodo de administración principal. Usted debe [configurar hardware AutoSupport](#) en cada aparato.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .
- Si va a utilizar HTTPS para enviar paquetes de AutoSupport , ha proporcionado acceso a Internet saliente al nodo de administración principal, ya sea de manera directa o ["utilizando un servidor proxy"](#) (no se requieren conexiones entrantes).
- Si se selecciona HTTP en la página StorageGRID AutoSupport , tiene ["configuró un servidor proxy"](#) para reenviar paquetes de AutoSupport como HTTPS. Los servidores AutoSupport de NetApp rechazarán los paquetes enviados mediante HTTP.
- Si va a utilizar SMTP como protocolo para los paquetes de AutoSupport , habrá configurado un servidor de correo SMTP.

Acerca de esta tarea

Puede utilizar cualquier combinación de las siguientes opciones para enviar paquetes de AutoSupport al soporte técnico:

- **Semanal:** envía automáticamente paquetes de AutoSupport una vez por semana. Configuración predeterminada: habilitado.
- **Activado por eventos:** envía automáticamente paquetes de AutoSupport cada hora o cuando ocurren eventos importantes del sistema. Configuración predeterminada: habilitado.
- **A pedido:** permite que el soporte técnico solicite que su sistema StorageGRID envíe paquetes de AutoSupport automáticamente, lo que resulta útil cuando están trabajando activamente en un problema (requiere el protocolo de transmisión AutoSupport HTTPS). Configuración predeterminada: deshabilitado.
- **Activado por el usuario:** envía manualmente paquetes de AutoSupport en cualquier momento.

Especifique el protocolo para los paquetes de AutoSupport

Puede utilizar cualquiera de los siguientes protocolos para enviar paquetes de AutoSupport :

- **HTTPS:** Esta es la configuración predeterminada y recomendada para nuevas instalaciones. Este protocolo utiliza el puerto 443. Si quieres [Habilitar la función AutoSupport on Demand](#) , debes utilizar HTTPS.
- **HTTP:** Si selecciona HTTP, debe configurar un servidor proxy para reenviar los paquetes de AutoSupport como HTTPS. Los servidores AutoSupport de NetApp rechazan los paquetes enviados mediante HTTP. Este protocolo utiliza el puerto 80.
- **SMTP:** utilice esta opción si desea que los paquetes de AutoSupport se envíen por correo electrónico.

El protocolo que configure se utiliza para enviar todo tipo de paquetes de AutoSupport .

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport* > Configuración**.
2. Seleccione el protocolo que desea utilizar para enviar paquetes de AutoSupport .
3. Si seleccionó **HTTPS**, seleccione si desea utilizar un certificado de soporte de NetApp (certificado TLS) para proteger la conexión al servidor de soporte técnico.
 - **Verificar certificado** (predeterminado): garantiza que la transmisión de paquetes de AutoSupport sea segura. El certificado de soporte de NetApp ya está instalado con el software StorageGRID .
 - **No verificar el certificado**: seleccione esta opción solo cuando tenga una buena razón para no utilizar la validación del certificado, como cuando hay un problema temporal con un certificado.
4. Seleccione **Guardar**. Todos los paquetes semanales, activados por el usuario y activados por eventos se envían mediante el protocolo seleccionado.

Desactivar el AutoSupport semanal

De forma predeterminada, el sistema StorageGRID está configurado para enviar un paquete de AutoSupport al soporte técnico una vez por semana.

Para determinar cuándo se enviará el paquete de AutoSupport semanal, vaya a la pestaña *** AutoSupport* > Resultados**. En la sección *** AutoSupport semanal***, observe el valor de **Próxima hora programada**.

Puede desactivar el envío automático de paquetes semanales de AutoSupport en cualquier momento.

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport* > Configuración**.
2. Desmarque la casilla de verificación **Habilitar AutoSupport semanal**.
3. Seleccione **Guardar**.

Deshabilitar el AutoSupport activado por eventos

De forma predeterminada, el sistema StorageGRID está configurado para enviar un paquete de AutoSupport al soporte técnico cada hora.

Puede desactivar el AutoSupport activado por eventos en cualquier momento.

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport* > Configuración**.
2. Desmarque la casilla de verificación **Habilitar AutoSupport activado por eventos**.
3. Seleccione **Guardar**.

Habilitar AutoSupport a pedido

AutoSupport on Demand puede ayudar a resolver problemas en los que el soporte técnico está trabajando activamente.

De forma predeterminada, AutoSupport on Demand está deshabilitado. Al habilitar esta función, el soporte técnico puede solicitar que su sistema StorageGRID envíe paquetes de AutoSupport automáticamente. El soporte técnico también puede establecer el intervalo de tiempo de sondeo para las consultas de AutoSupport on Demand.

El soporte técnico no puede habilitar ni deshabilitar AutoSupport on Demand.

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport* > Configuración**.
2. Seleccione **HTTPS** para el protocolo.
3. Seleccione la casilla de verificación **Habilitar AutoSupport semanal**.
4. Seleccione la casilla de verificación **Habilitar AutoSupport a pedido**.
5. Seleccione **Guardar**.

AutoSupport on Demand está habilitado y el soporte técnico puede enviar solicitudes de AutoSupport on Demand a StorageGRID.

Deshabilitar las comprobaciones de actualizaciones de software

De forma predeterminada, StorageGRID se comunica con NetApp para determinar si hay actualizaciones de software disponibles para su sistema. Si hay una revisión o una nueva versión de StorageGRID disponible, la nueva versión se muestra en la página Actualización de StorageGRID .

Según sea necesario, puede desactivar opcionalmente la búsqueda de actualizaciones de software. Por ejemplo, si su sistema no tiene acceso WAN, debe deshabilitar la verificación para evitar errores de descarga.

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport* > Configuración**.
2. Desmarque la casilla **Buscar actualizaciones de software**.
3. Seleccione **Guardar**.

Agregar un destino de AutoSupport adicional

Cuando habilita AutoSupport, los paquetes de estado y salud se envían al soporte técnico. Puede especificar un destino adicional para todos los paquetes de AutoSupport .

Para verificar o cambiar el protocolo utilizado para enviar paquetes de AutoSupport , consulte las instrucciones para [especificar el protocolo para los paquetes de AutoSupport](#) .



No puede utilizar el protocolo SMTP para enviar paquetes de AutoSupport a un destino adicional.

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport* > Configuración**.
2. Seleccione **Habilitar destino de AutoSupport adicional**.
3. Especifique lo siguiente:

Nombre de host

El nombre de host del servidor o la dirección IP de un servidor de destino de AutoSupport adicional.



Sólo puedes introducir un destino adicional.

Puerto

El puerto utilizado para conectarse a un servidor de destino de AutoSupport adicional. El puerto predeterminado es el puerto 80 para HTTP o el puerto 443 para HTTPS.

Validación de certificados

Si se utiliza un certificado TLS para proteger la conexión al destino adicional.

- Seleccione **Verificar certificado** para utilizar la validación del certificado.
- Seleccione **No verificar certificado** para enviar sus paquetes de AutoSupport sin validación del certificado.

Seleccione esta opción solo cuando tenga un buen motivo para no utilizar la validación de certificados, como cuando hay un problema temporal con un certificado.

4. Si seleccionó **Verificar certificado**, haga lo siguiente:

- a. Busque la ubicación del certificado CA.
- b. Subir el archivo del certificado CA.

Aparecen los metadatos del certificado CA.

5. Seleccione **Guardar**.

Todos los paquetes futuros de AutoSupport activados por eventos, semanales o por el usuario se enviarán al destino adicional.

Configurar AutoSupport para dispositivos

AutoSupport para dispositivos informa sobre problemas de hardware de StorageGRID , y StorageGRID AutoSupport informa sobre problemas de software de StorageGRID , con una excepción: para el SGF6112, StorageGRID AutoSupport informa sobre problemas de hardware y software. Debe configurar AutoSupport en cada dispositivo excepto el SGF6112, que no requiere configuración adicional. AutoSupport se implementa de manera diferente para los dispositivos de servicios y los dispositivos de almacenamiento.

Utilice SANtricity para habilitar AutoSupport para cada dispositivo de almacenamiento. Puede configurar SANtricity AutoSupport durante la configuración inicial del dispositivo o después de haberlo instalado:

- Para los dispositivos SG6000 y SG5700, ["Configurar AutoSupport en SANtricity System Manager"](#)

Los paquetes de AutoSupport de los dispositivos E-Series se pueden incluir en StorageGRID AutoSupport si configura la entrega de AutoSupport por proxy en ["SANtricity System Manager"](#) .

StorageGRID AutoSupport no informa problemas de hardware, como fallas de DIMM o de tarjeta de interfaz de host (HIC). Sin embargo, algunas fallas de componentes podrían provocar ["alertas de hardware"](#) . Para los dispositivos StorageGRID con un controlador de administración de placa base (BMC), puede configurar trampas de correo electrónico y SNMP para informar fallas de hardware:

- ["Configurar notificaciones por correo electrónico para alertas de BMC"](#)
- ["Configurar los ajustes de SNMP para BMC"](#)

Información relacionada

["Soporte de NetApp"](#)

Activar manualmente un paquete de AutoSupport

Para ayudar al soporte técnico a solucionar problemas con su sistema StorageGRID , puede activar manualmente el envío de un paquete de AutoSupport .

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Debe tener acceso de root u otro permiso de configuración de red.

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport***.
2. En la pestaña **Acciones**, seleccione **Enviar AutoSupport activado por el usuario**.

StorageGRID intenta enviar un paquete de AutoSupport al sitio de soporte de NetApp . Si el intento es exitoso, se actualizan los valores **Resultado más reciente** y **Última vez exitoso** en la pestaña **Resultados**. Si hay un problema, el valor **Resultado más reciente** se actualiza a "Error" y StorageGRID no intenta enviar el paquete AutoSupport nuevamente.



Después de enviar un paquete de AutoSupport activado por el usuario, actualice la página de AutoSupport en su navegador después de 1 minuto para acceder a los resultados más recientes.

Solucionar problemas de paquetes de AutoSupport

Si falla un intento de enviar un paquete de AutoSupport , el sistema StorageGRID toma diferentes acciones según el tipo de paquete de AutoSupport . Puede comprobar el estado de los paquetes de AutoSupport seleccionando **SOPORTE > Herramientas > * AutoSupport* > Resultados**.

Cuando el paquete de AutoSupport no se puede enviar, aparece "Error" en la pestaña **Resultados** de la página *** AutoSupport***.



Si configuró un servidor proxy para reenviar paquetes de AutoSupport a NetApp, debe ["verificar que la configuración del servidor proxy sea correcta"](#) .

Falla del paquete de AutoSupport semanal

Si no se puede enviar un paquete de AutoSupport semanal, el sistema StorageGRID toma las siguientes acciones:

1. Actualiza el atributo Resultado más reciente a Reintentar.
2. Intenta reenviar el paquete de AutoSupport 15 veces cada cuatro minutos durante una hora.
3. Después de una hora de fallas de envío, actualiza el atributo Resultado más reciente a Fallido.
4. Intenta enviar un paquete de AutoSupport nuevamente en el próximo horario programado.
5. Mantiene la programación regular de AutoSupport si el paquete falla porque el servicio NMS no está disponible y si se envía un paquete antes de que pasen siete días.
6. Cuando el servicio NMS vuelve a estar disponible, envía un paquete de AutoSupport inmediatamente si no se ha enviado un paquete durante siete días o más.

Error del paquete de AutoSupport activado por el usuario o por evento

Si un paquete de AutoSupport activado por el usuario o por evento no se puede enviar, el sistema StorageGRID toma las siguientes acciones:

1. Muestra un mensaje de error si se conoce el error. Por ejemplo, si un usuario selecciona el protocolo SMTP sin proporcionar la configuración de correo electrónico correcta, se muestra el siguiente error:
`AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. No intenta enviar el paquete nuevamente.
3. Registra el error en `nms.log`.

Si ocurre una falla y SMTP es el protocolo seleccionado, verifique que el servidor de correo electrónico del sistema StorageGRID esté configurado correctamente y que su servidor de correo electrónico esté ejecutándose (**SOPORTE > Alarmas (heredado) > Configuración de correo electrónico heredado**). El siguiente mensaje de error podría aparecer en la página de AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Aprenda a... ["configurar los ajustes del servidor de correo electrónico"](#).

Corregir una falla del paquete AutoSupport

Si ocurre una falla y SMTP es el protocolo seleccionado, verifique que el servidor de correo electrónico del sistema StorageGRID esté configurado correctamente y que su servidor de correo electrónico esté ejecutándose. El siguiente mensaje de error podría aparecer en la página de AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envíe paquetes de AutoSupport de la serie E a través de StorageGRID

Puede enviar paquetes de AutoSupport de E-Series SANtricity System Manager al soporte técnico a través de un nodo de administración de StorageGRID en lugar de a través del puerto de administración del dispositivo de almacenamiento.

Ver ["AutoSupport de hardware de la serie E"](#) para obtener más información sobre el uso de AutoSupport con dispositivos de la serie E.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Administrador del dispositivo de almacenamiento o permiso de acceso raíz"](#).
- Ha configurado SANtricity AutoSupport:
 - Para los dispositivos SG6000 y SG5700, ["Configurar AutoSupport en SANtricity System Manager"](#)



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

Acerca de esta tarea

Los paquetes AutoSupport de la serie E contienen detalles del hardware de almacenamiento y son más específicos que otros paquetes AutoSupport enviados por el sistema StorageGRID.

Puede configurar una dirección de servidor proxy especial en SANtricity System Manager para transmitir paquetes de AutoSupport a través de un nodo de administración de StorageGRID sin utilizar el puerto de administración del dispositivo. Los paquetes de AutoSupport transmitidos de esta manera son enviados por el ["Nodo de administración del remitente preferido"](#), y utilizan cualquier ["configuración del proxy de](#)

administración" que se han configurado en el Administrador de cuadrícula.

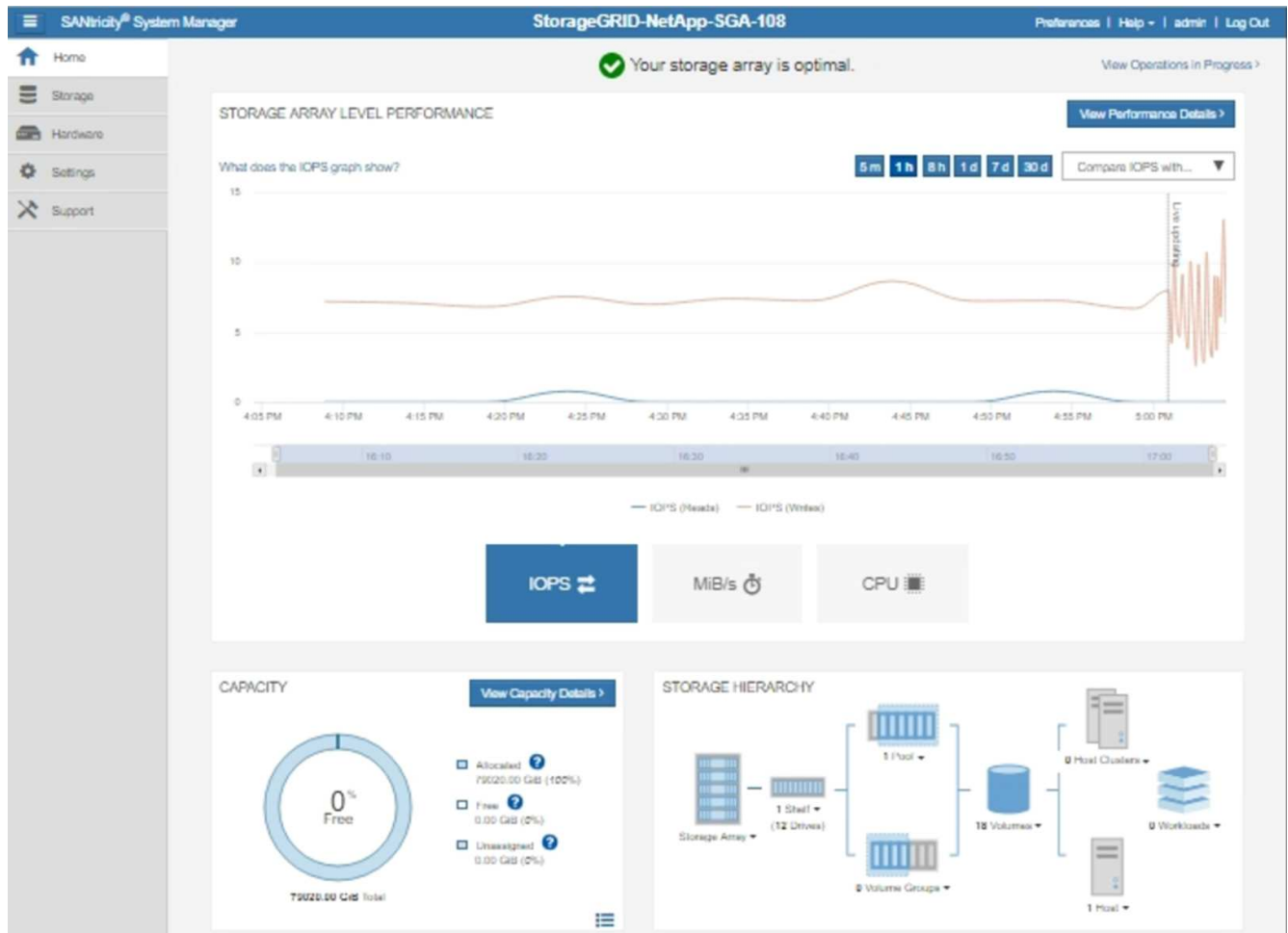


Este procedimiento es solo para configurar un servidor proxy StorageGRID para paquetes E-Series AutoSupport . Para obtener detalles adicionales sobre la configuración de AutoSupport de la serie E, consulte la "[Documentación de NetApp E-Series y SANtricity](#)".

Pasos

1. En el Administrador de cuadrícula, seleccione **NODOS**.
2. De la lista de nodos de la izquierda, seleccione el nodo del dispositivo de almacenamiento que desea configurar.
3. Seleccione * SANtricity System Manager*.

Aparece la página de inicio de SANtricity System Manager.



4. Seleccione **SOPORTE > Centro de soporte > * AutoSupport***.

Aparece la página de operaciones de AutoSupport .

Technical Support

Chassis serial number: 031517000693

 [NetApp My Support](#)

US/Canada 888.463.8277

[Other Contacts](#)

Support Resources

Diagnostics

AutoSupport

AutoSupport operations

AutoSupport status: Enabled 

[Enable/Disable AutoSupport Features](#)
AutoSupport proactively monitors the health of your storage array and automatically sends support data ("dispatches") to the support team.

[Configure AutoSupport Delivery Method](#)
Connect to the support team via HTTPS, HTTP or Mail (SMTP) server delivery methods.

[Schedule AutoSupport Dispatches](#)
AutoSupport dispatches are sent daily at 03:06 PM UTC and weekly at 07:39 AM UTC on Thursday.

[Send AutoSupport Dispatch](#)
Automatically sends the support team a dispatch to troubleshoot system issues without waiting for periodic dispatches.

[View AutoSupport Log](#)
The AutoSupport log provides information about status, dispatch history, and errors encountered during delivery of AutoSupport dispatches.

[Enable AutoSupport Maintenance Window](#)
Enable AutoSupport Maintenance window to allow maintenance activities to be performed on the storage array without generating support cases.

[Disable AutoSupport Maintenance Window](#)
Disable AutoSupport Maintenance window to allow the storage array to generate support cases on component failures and other destructive actions.

5. Seleccione *Configurar método de entrega de AutoSupport*.

Aparece la página Configurar método de entrega de AutoSupport .

Configure AutoSupport Delivery Method [X]

Select AutoSupport dispatch delivery method...

☒ **HTTPS**

☐ HTTP

☐ Email

HTTPS delivery settings Show destination address

Connect to support team...

☐ Directly ?

☒ **via Proxy server** ?

Host address ?

tunnel-host

Port number ?

10225

☐ My proxy server requires authentication

☐ via Proxy auto-configuration script (PAC) ?

Save **Test Configuration** Cancel

6. Seleccione **HTTPS** como método de entrega.



El certificado que habilita HTTPS está preinstalado.

7. Seleccionar **a través del servidor proxy**.

8. Ingresar `tunnel-host` para la **Dirección del host**.

`tunnel-host` es la dirección especial para utilizar un nodo de administración para enviar paquetes de AutoSupport de la serie E.

9. Ingresar 10225 para el **Número de puerto**.

`10225` es el número de puerto en el servidor proxy StorageGRID que recibe paquetes de AutoSupport del controlador E-Series en el dispositivo.

10. Seleccione **Probar configuración** para probar el enrutamiento y la configuración de su servidor proxy de AutoSupport .

Si es correcto, aparecerá un mensaje en un banner verde: "Su configuración de AutoSupport ha sido

verificada".

Si la prueba falla, aparece un mensaje de error en un banner rojo. Verifique la configuración de DNS y la red de StorageGRID y asegúrese de que "[Nodo de administración del remitente preferido](#)" puede conectarse al sitio de soporte de NetApp e intentar la prueba nuevamente.

11. Seleccione **Guardar**.

La configuración se guarda y aparece un mensaje de confirmación: "Se ha configurado el método de entrega de AutoSupport".

Administrar nodos de almacenamiento

Administrar nodos de almacenamiento

Los nodos de almacenamiento proporcionan capacidad y servicios de almacenamiento en disco. La gestión de nodos de almacenamiento implica lo siguiente:

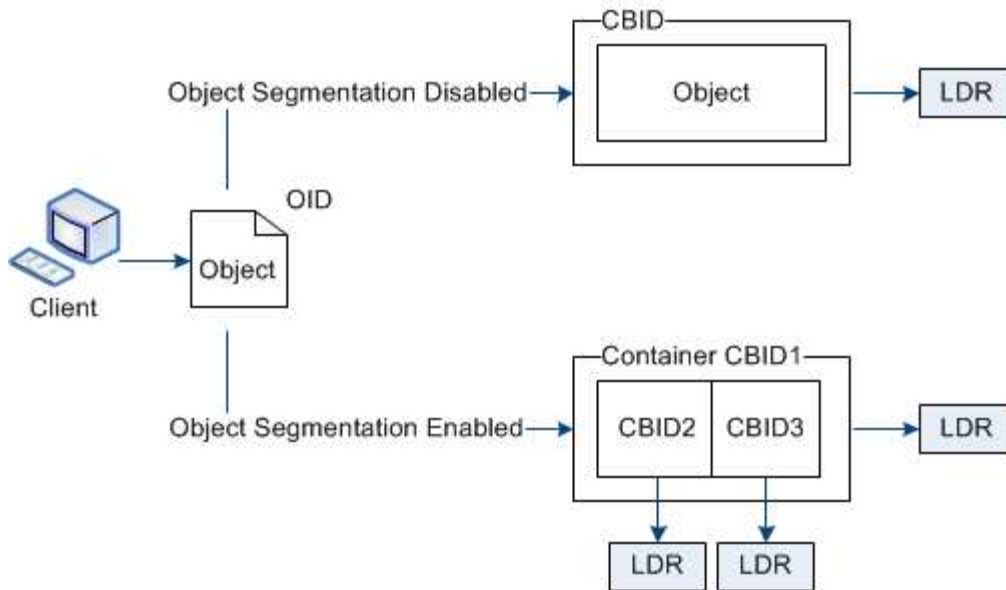
- Administrar las opciones de almacenamiento
- Comprender qué son las marcas de agua del volumen de almacenamiento y cómo puede usar las anulaciones de marcas de agua para controlar cuándo los nodos de almacenamiento se vuelven de solo lectura
- Monitoreo y gestión del espacio utilizado para los metadatos de los objetos
- Configuración de ajustes globales para objetos almacenados
- Aplicación de la configuración del nodo de almacenamiento
- Administración de nodos de almacenamiento completos

Utilice las opciones de almacenamiento

¿Qué es la segmentación de objetos?

La segmentación de objetos es el proceso de dividir un objeto en una colección de objetos más pequeños de tamaño fijo para optimizar el uso de almacenamiento y recursos para objetos grandes. La carga multiparte de S3 también crea objetos segmentados, con un objeto que representa cada parte.

Cuando se ingiere un objeto en el sistema StorageGRID, el servicio LDR divide el objeto en segmentos y crea un contenedor de segmentos que enumera la información del encabezado de todos los segmentos como contenido.



Al recuperar un contenedor de segmentos, el servicio LDR ensambla el objeto original a partir de sus segmentos y devuelve el objeto al cliente.

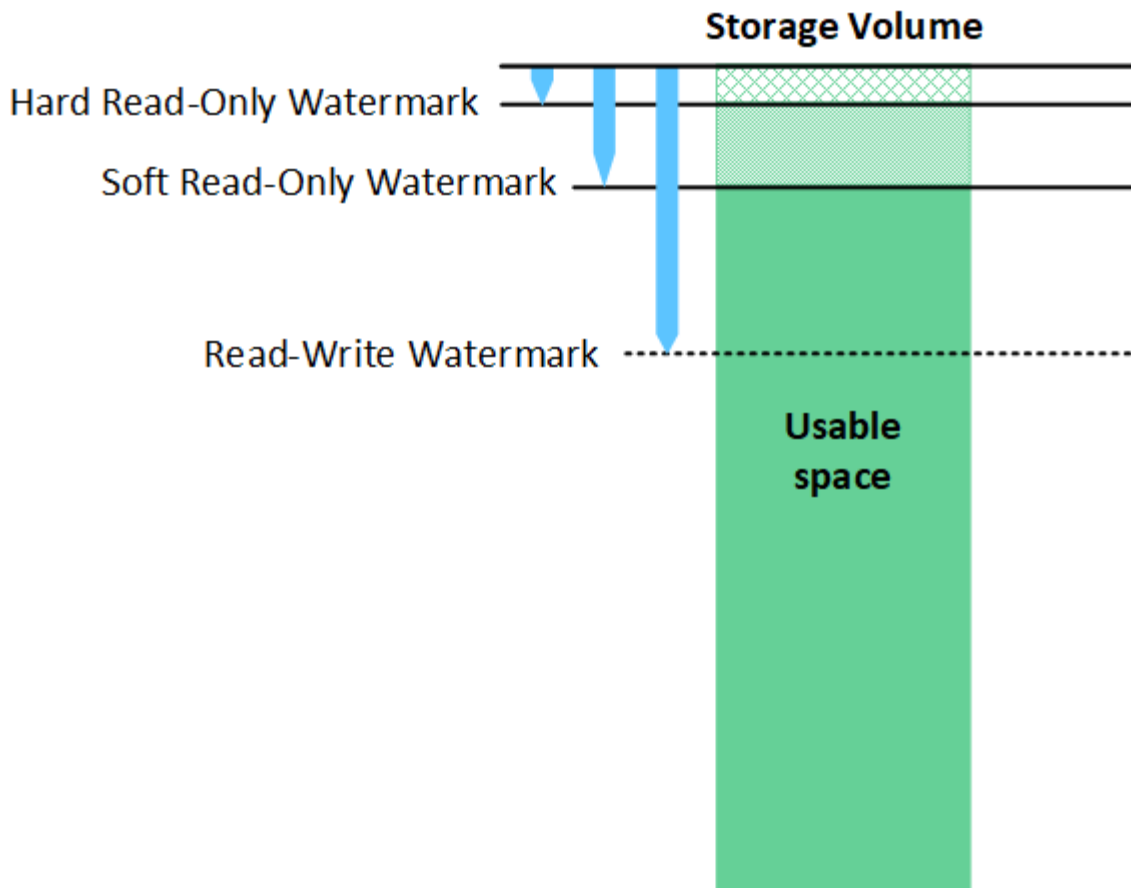
El contenedor y los segmentos no necesariamente se almacenan en el mismo nodo de almacenamiento. Los contenedores y segmentos se pueden almacenar en cualquier nodo de almacenamiento dentro del grupo de almacenamiento especificado en la regla ILM.

El sistema StorageGRID trata cada segmento de forma independiente y contribuye al recuento de atributos como objetos administrados y objetos almacenados. Por ejemplo, si un objeto almacenado en el sistema StorageGRID se divide en dos segmentos, el valor de Objetos administrados aumenta en tres después de que se completa la ingesta, de la siguiente manera:

`segment container + segment 1 + segment 2 = three stored objects`

¿Qué son las marcas de agua del volumen de almacenamiento?

StorageGRID utiliza tres marcas de agua de volumen de almacenamiento para garantizar que los nodos de almacenamiento pasen de forma segura a un estado de solo lectura antes de que se queden críticamente sin espacio y para permitir que los nodos de almacenamiento que han pasado a un estado de solo lectura vuelvan a ser de lectura y escritura.



Las marcas de agua del volumen de almacenamiento solo se aplican al espacio utilizado para datos de objetos replicados y codificados para borrado. Para obtener más información sobre el espacio reservado para los metadatos de objetos en el volumen 0, vaya a ["Administrar el almacenamiento de metadatos de objetos"](#).

¿Qué es la marca de agua suave de solo lectura?

La **marca de agua de solo 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 de objetos se está llenando.

Si cada volumen de un nodo de almacenamiento tiene menos espacio libre que la marca de agua de solo lectura de ese volumen, el nodo de almacenamiento pasa 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 cumple con todas las solicitudes de escritura pendientes.

Por ejemplo, supongamos que cada volumen de un nodo de almacenamiento tiene una marca de agua de solo lectura de 10 GB. Tan pronto como cada volumen tenga menos de 10 GB de espacio libre, el nodo de almacenamiento pasará al modo de solo lectura suave.

¿Qué es la marca de agua de sólo lectura?

La **marca de agua de solo lectura del volumen de almacenamiento** es la siguiente marca de agua que indica que el espacio utilizable de un nodo para los datos de objetos se está llenando.

Si el espacio libre en un volumen es menor que la marca de agua de solo 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 solo lectura.

Por ejemplo, supongamos que cada volumen de un nodo de almacenamiento tiene una marca de agua de solo lectura de 5 GB. Tan pronto como 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 de solo lectura dura siempre es menor que la marca de agua de solo lectura suave.

¿Qué es la marca de agua de lectura y escritura?

La **marca de agua de lectura y escritura del volumen de almacenamiento** se aplica únicamente a los nodos de almacenamiento que han pasado al modo de solo lectura. Determina cuándo el nodo puede volver a ser de lectura y escritura. Cuando el espacio libre en cualquier volumen de almacenamiento en un nodo de almacenamiento es mayor que la marca de agua de lectura y escritura de ese volumen, el nodo vuelve 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. Tan pronto como el espacio libre para cualquier volumen aumenta a 30 GB, el nodo vuelve a ser de lectura y escritura.

La marca de agua de lectura y escritura siempre es más grande que la marca de agua de solo lectura suave y que la marca de agua de solo lectura dura.

Ver marcas de agua del volumen de almacenamiento

Puede ver la configuración actual de la marca de agua y los valores optimizados del sistema. Si no se utilizan marcas de agua optimizadas, puede determinar si puede o debe ajustar la configuración.

Antes de empezar

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

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 cuadrícula.

Pasos

1. Seleccione **SOPORTE > Otros > Marcas de agua de almacenamiento**.
2. En la página Marcas de agua de almacenamiento, mire la casilla de verificación Usar valores optimizados.
 - Si se selecciona la casilla de verificación, las tres marcas de agua se optimizan para cada volumen de almacenamiento en cada nodo de almacenamiento, según el tamaño del nodo de almacenamiento y la capacidad relativa del volumen.

Esta es la configuración predeterminada y recomendada. No actualice estos valores. Opcionalmente, puedes [Ver marcas de agua de almacenamiento optimizadas](#).

- Si la casilla de verificación Usar valores optimizados no está seleccionada, se utilizarán marcas de agua personalizadas (no optimizadas). No se recomienda utilizar configuraciones de marca de agua personalizadas. Utilice las instrucciones para ["Solución de problemas de alertas de anulación de marca de agua de solo lectura baja"](#) para determinar si puede o debe ajustar la configuración.

Al especificar configuraciones de marca de agua personalizadas, debe ingresar valores mayores a 0.

Ver marcas de agua de almacenamiento optimizadas

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

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

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

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

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

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

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

Administrar 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 su sistema StorageGRID tenga espacio adecuado para almacenar nuevos objetos, debe comprender dónde y cómo StorageGRID almacena los metadatos de los objetos.

¿Qué son los metadatos de un objeto?

Los metadatos de un objeto son cualquier información que describe un objeto. StorageGRID utiliza metadatos de objetos para rastrear las ubicaciones de todos los objetos en la red y administrar el ciclo de vida de cada objeto a lo largo del tiempo.

Para un objeto en StorageGRID, los metadatos del objeto incluyen los siguientes tipos de información:

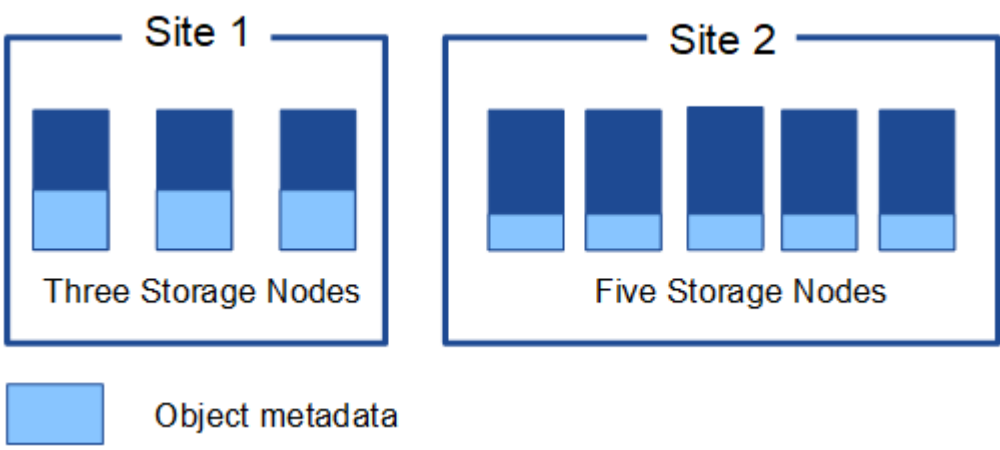
- Metadatos del sistema, incluido un ID único para cada objeto (UUID), el nombre del objeto, el nombre del depósito S3, el nombre o ID de la cuenta del inquilino, el tamaño lógico del objeto, la fecha y hora en que se creó el objeto por primera vez y la fecha y hora en que se modificó el objeto por última vez.
- Cualquier par clave-valor de metadatos de usuario personalizados asociados con el objeto.
- Para los objetos S3, cualquier par clave-valor de etiqueta de objeto asociado con el objeto.
- Para copias de objetos replicados, la ubicación de almacenamiento actual de cada copia.
- Para las copias de objetos con código de borrado, la ubicación de almacenamiento actual de cada fragmento.

- Para las copias de objetos en un grupo de almacenamiento en la nube, la ubicación del objeto, incluido el nombre del depósito externo y el identificador único del objeto.
- Para objetos segmentados y objetos multiparte, identificadores de segmento y tamaños de datos.

¿Cómo se almacenan los metadatos de los objetos?

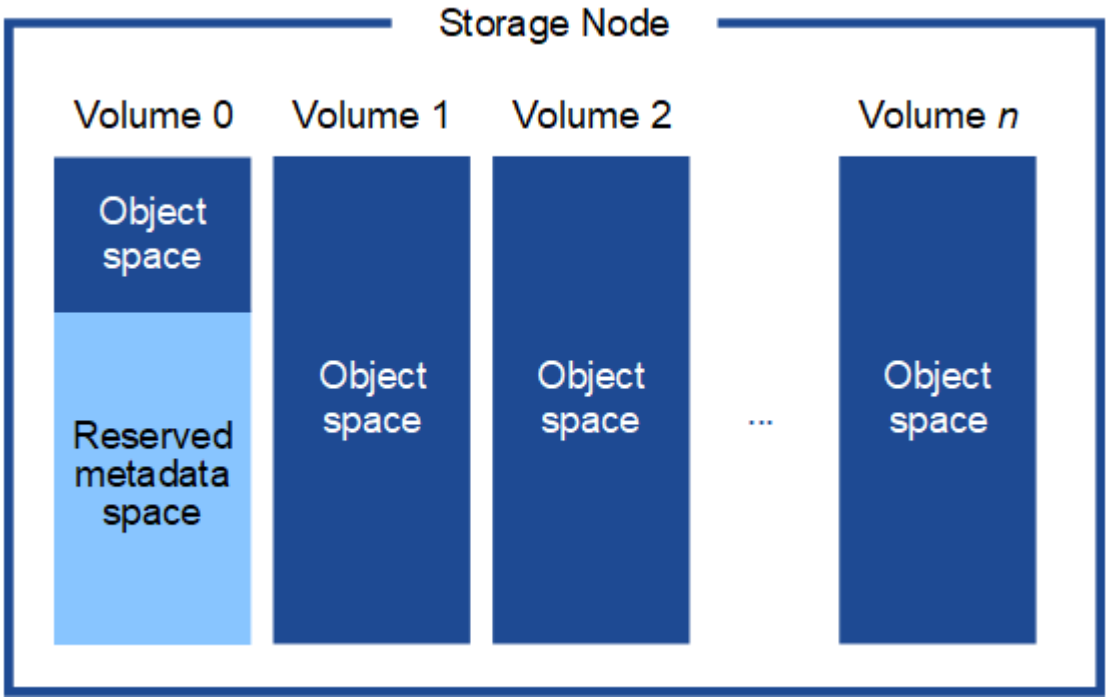
StorageGRID mantiene los metadatos de los objetos en una base de datos Cassandra, que se almacena independientemente de los datos de los objetos. Para proporcionar redundancia y proteger los metadatos de los objetos contra pérdidas, StorageGRID almacena tres copias de los metadatos de todos los objetos del sistema en cada sitio.

Esta figura representa los nodos de almacenamiento en dos sitios. Cada sitio tiene la misma cantidad de metadatos de objetos, y los metadatos de cada sitio se subdividen entre todos los nodos de almacenamiento de ese sitio.



¿Dónde se almacenan los metadatos de los objetos?

Esta figura representa los volúmenes de almacenamiento para un solo nodo de almacenamiento.



Como se muestra en la figura, StorageGRID reserva espacio para los metadatos de objetos 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 en el nodo de almacenamiento se utilizan exclusivamente para datos de objetos (copias replicadas y fragmentos con código de borrado).

La cantidad de espacio que se reserva para los metadatos de objetos en un nodo de almacenamiento en particular depende de varios factores, que se describen a continuación.

Configuración de espacio reservado para metadatos

El *Espacio reservado para metadatos* es una configuración de todo el sistema que representa la cantidad de espacio que se reservará para los metadatos en el volumen 0 de cada nodo de almacenamiento. Como se muestra en la tabla, el valor predeterminado de esta configuración se basa en:

- La versión del software que estaba utilizando cuando instaló StorageGRID inicialmente.
- 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 predeterminada del espacio reservado para metadatos
11,5 a 11,9	128 GB o más en cada nodo de almacenamiento de la red	8 TB (8000 GB)
	Menos de 128 GB en cualquier nodo de almacenamiento de la red	3 TB (3000 GB)
11.1 a 11.4	128 GB o más en cada nodo de almacenamiento en cualquier sitio	4 TB (4000 GB)
	Menos de 128 GB en cualquier nodo de almacenamiento en cada sitio	3 TB (3000 GB)
11.0 o anterior	Cualquier cantidad	2 TB (2000 GB)

Ver la configuración del espacio reservado de metadatos

Siga estos pasos para ver la configuración del espacio reservado de metadatos para su sistema StorageGRID .

Pasos

1. Seleccione **CONFIGURACIÓN > Sistema > Configuración de almacenamiento**.
2. En la página de configuración de almacenamiento, expanda la sección **Espacio reservado de metadatos**.

Para StorageGRID 11.8 o superior, el valor del espacio reservado de metadatos debe ser de al menos 100 GB y no más de 1 PB.

La configuración predeterminada para una nueva instalación de StorageGRID 11.6 o superior en la que cada

nodo de almacenamiento tiene 128 GB o más de RAM es 8000 GB (8 TB).

Espacio reservado real para metadatos

A diferencia de la configuración de espacio reservado de metadatos de todo el sistema, el *espacio reservado real* para los metadatos de objetos se determina para cada nodo de almacenamiento. Para cualquier nodo de almacenamiento determinado, el espacio reservado real para metadatos depende del tamaño del volumen 0 del nodo y de la configuración del espacio reservado de metadatos de todo el sistema.

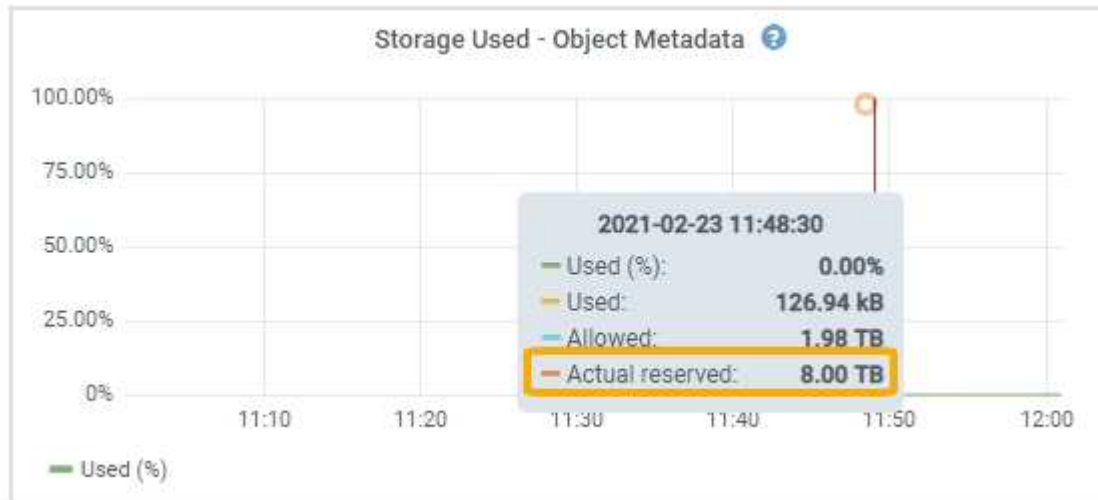
Tamaño del volumen 0 para el nodo	Espacio reservado real para metadatos
Menos de 500 GB (uso no productivo)	10% del volumen 0
500 GB o más + o + Nodos de almacenamiento solo de metadatos	El menor de estos valores: • Volumen 0 • Configuración de espacio reservado para metadatos Nota: Solo se requiere una rangedb para los nodos de almacenamiento de solo metadatos.

Ver el espacio reservado real para metadatos

Siga estos pasos para ver el espacio reservado real para metadatos en un nodo de almacenamiento en particular.

Pasos

1. Desde el Administrador de red, seleccione **NODOS** > **Nodo de almacenamiento**.
2. Seleccione la pestaña **Almacenamiento**.
3. Coloque el cursor sobre el gráfico Almacenamiento utilizado - Metadatos del 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 de 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.

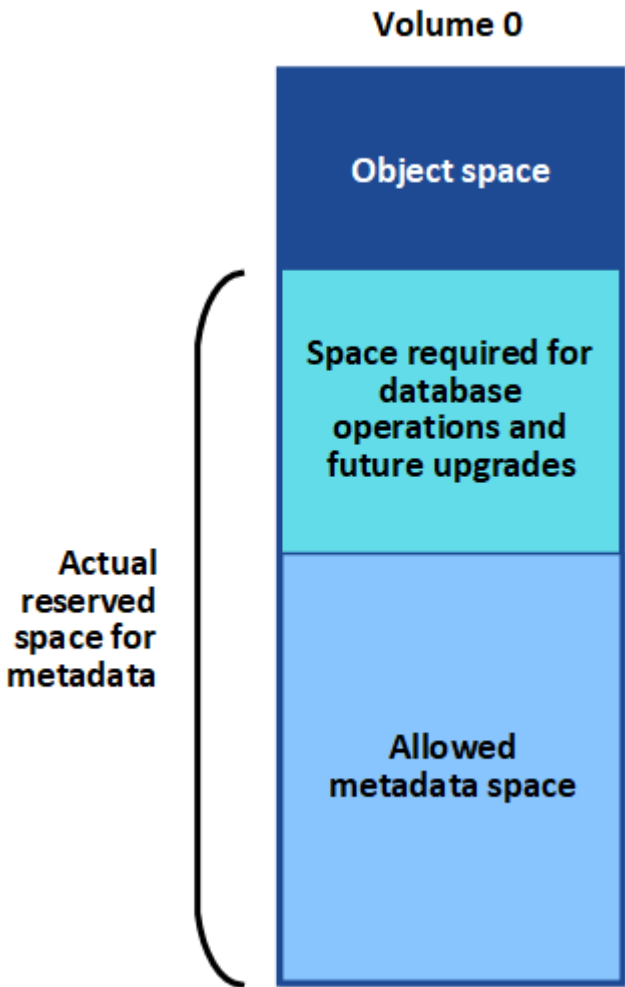
Ejemplo de espacio de metadatos reservado real

Supongamos que instala un nuevo sistema StorageGRID utilizando la versión 11.7 o posterior. Para este ejemplo, supongamos que cada nodo de almacenamiento tiene más de 128 GB de RAM y que el volumen 0 del nodo de almacenamiento 1 (SN1) es de 6 TB. Basándonos en estos valores:

- El espacio reservado para metadatos de todo el sistema está establecido en 8 TB. (Este es el valor predeterminado para una nueva instalación de StorageGRID 11.6 o superior si cada nodo de almacenamiento tiene más de 128 GB de RAM).
- El espacio reservado real para metadatos para SN1 es de 6 TB. (Todo el volumen está reservado porque el volumen 0 es más pequeño 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 metadatos de objetos (el *espacio de metadatos permitido*) y el espacio requerido para operaciones esenciales de la base de datos (como compactación y reparación) y futuras actualizaciones de hardware y software. El espacio de metadatos permitido determina la capacidad general del objeto.



La siguiente tabla muestra cómo StorageGRID calcula el **espacio de metadatos permitido** para diferentes

nodos de almacenamiento, en función de la cantidad de memoria del nodo y el espacio reservado real para metadatos.

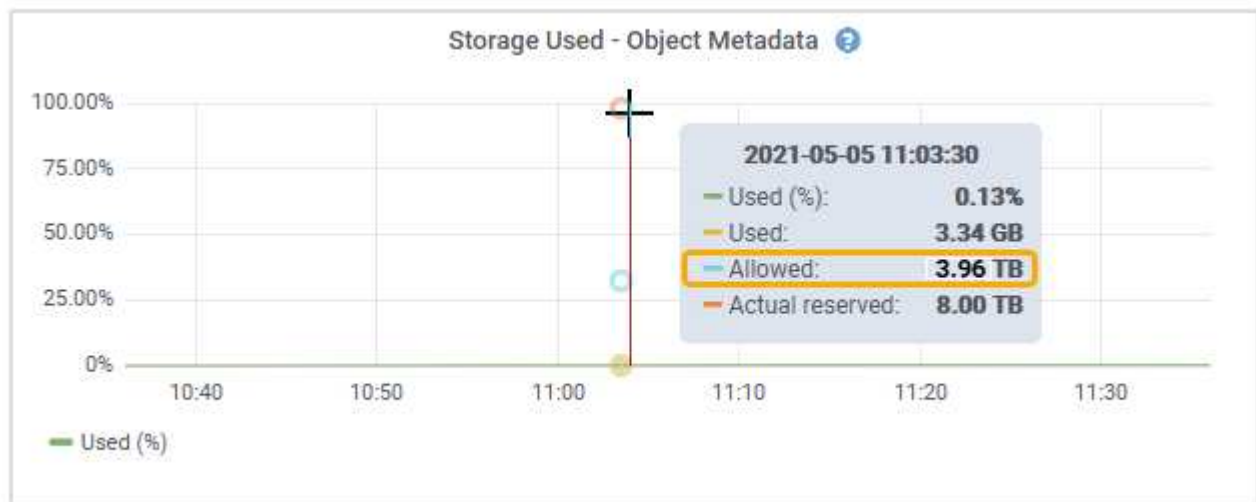
	Cantidad de memoria en el nodo de almacenamiento		
	< 128 GB	>= 128 GB	Espacio reservado real para metadatos
≤ 4 TB	60% del espacio real reservado para metadatos, hasta un máximo de 1,32 TB	60% del espacio real reservado para metadatos, hasta un máximo de 1,98 TB	4 TB

Ver el espacio de metadatos permitido

Siga estos pasos para ver el espacio de metadatos permitido para un nodo de almacenamiento.

Pasos

1. Desde el Administrador de cuadrícula, seleccione **NODOS**.
2. Seleccione el nodo de almacenamiento.
3. Seleccione la pestaña **Almacenamiento**.
4. Coloque el cursor sobre el gráfico de metadatos del objeto Almacenamiento utilizado y localice 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 más de 4 TB.

El valor **Permitido** corresponde a esta métrica de Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Ejemplo de espacio de metadatos permitido

Supongamos que instala un sistema StorageGRID utilizando 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. Basándonos en estos valores:

- El espacio reservado para metadatos de todo el sistema está establecido en 8 TB. (Este es el valor predeterminado para StorageGRID 11.6 o superior cuando cada nodo de almacenamiento tiene más de 128 GB de RAM).
- El espacio reservado real para metadatos para SN1 es de 6 TB. (Todo el volumen está reservado porque el volumen 0 es más pequeño que la configuración **Espacio reservado de metadatos**).
- El espacio permitido para metadatos en SN1 es de 3 TB, según el cálculo que se muestra en [la tabla de espacio permitido para metadatos](#) : $(\text{Espacio reservado real para metadatos} - 1 \text{ TB}) \times 60 \%$, hasta un máximo de 3,96 TB.

Cómo los nodos de almacenamiento de diferentes tamaños afectan la capacidad de los objetos

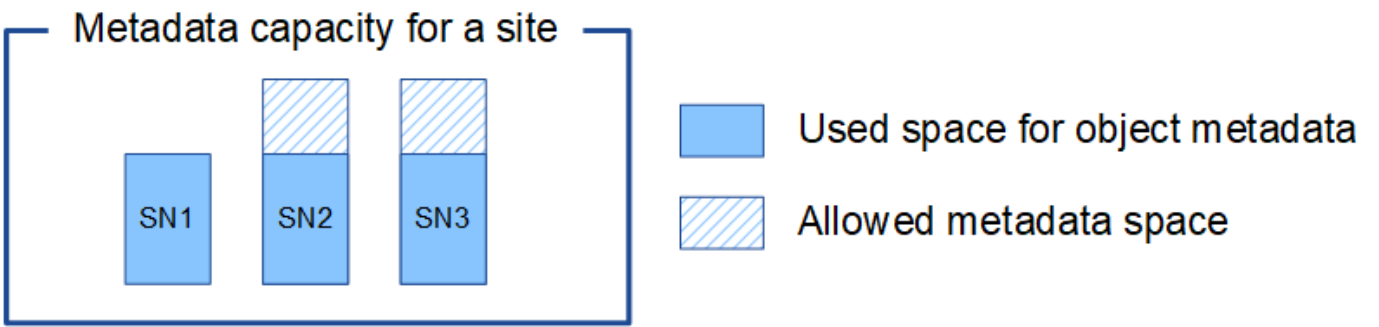
Como se describió anteriormente, StorageGRID distribuye uniformemente los metadatos de los objetos entre los nodos de almacenamiento en cada sitio. Por este motivo, si un sitio contiene nodos de almacenamiento de diferentes tamaños, el nodo más pequeño del sitio determina la capacidad de metadatos del sitio.

Consideremos el siguiente ejemplo:

- Tiene una cuadrícula de un solo sitio que contiene tres nodos de almacenamiento de diferentes tamaños.
- La configuración de **Espacio reservado para metadatos** es 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 de metadatos reservado real	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

Debido a que los metadatos de los objetos se distribuyen de manera uniforme entre los nodos de almacenamiento de un sitio, cada nodo en este ejemplo solo puede contener 1,32 TB de metadatos. Los 0,66 TB adicionales de espacio de metadatos permitido para SN2 y SN3 no se pueden utilizar.



De manera similar, debido a que StorageGRID mantiene todos los metadatos de objetos de un sistema StorageGRID en cada sitio, la capacidad general de metadatos de un sistema StorageGRID está determinada por la capacidad de metadatos de objetos del sitio más pequeño.

Y como la capacidad de metadatos de un objeto controla el recuento máximo de objetos, cuando un nodo se queda sin capacidad de metadatos, la cuadrícula queda prácticamente llena.

Información relacionada

- Para aprender a monitorear la capacidad de metadatos de objetos para cada nodo de almacenamiento, consulte las instrucciones para ["Monitoreo de StorageGRID"](#) .
- Para aumentar la capacidad de metadatos de objetos para su sistema, ["expandir una cuadrícula"](#) agregando nuevos nodos de almacenamiento.

Aumentar la configuración del espacio reservado de metadatos

Es posible que pueda aumentar la configuración del sistema de espacio reservado de metadatos si sus nodos de almacenamiento cumplen requisitos específicos de RAM y espacio disponible.

Lo que necesitarás

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso raíz o la configuración de la página de topología de la red y otros permisos de configuración de la red"](#) .



La página de topología de cuadrícula ha quedado obsoleta y se eliminará en una versión futura.

Acerca de esta tarea

Es posible que pueda aumentar manualmente la configuración del Espacio reservado de metadatos de todo el sistema hasta 8 TB.

Solo puede aumentar el valor de la configuración de Espacio reservado de metadatos de todo el sistema si ambas afirmaciones son verdaderas:

- Los nodos de almacenamiento en cualquier sitio de su sistema tienen cada uno 128 GB o más de RAM.
- Cada uno de los nodos de almacenamiento de cualquier sitio de su sistema tiene suficiente espacio disponible en el volumen de almacenamiento 0.

Tenga en cuenta que si aumenta esta configuración, reducirá simultáneamente 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 prefieras establecer el Espacio reservado de metadatos en un valor menor a 8 TB, en función de los requisitos de metadatos de tu objeto esperados.



En general, es mejor utilizar un valor más alto en lugar de un valor más bajo. Si la configuración de Espacio reservado de metadatos es demasiado grande, puede reducirla más tarde. Por el contrario, si aumenta el valor más adelante, es posible que el sistema necesite mover datos del objeto para liberar espacio.

Para obtener una explicación detallada de cómo la configuración del Espacio reservado de metadatos afecta el espacio permitido para el almacenamiento de metadatos de objetos en un nodo de almacenamiento en particular, consulte ["Administrar el almacenamiento de metadatos de objetos"](#) .

Pasos

1. Determinar la configuración actual del espacio reservado de metadatos.
 - a. Seleccione **CONFIGURACIÓN > Sistema > Opciones de almacenamiento**.
 - b. En la sección Marcas de agua de almacenamiento, anote el valor de **Espacio reservado de metadatos**.
2. Asegúrese de tener suficiente espacio disponible en el volumen de almacenamiento 0 de cada nodo de almacenamiento para aumentar este valor.
 - a. Seleccione **NODOS**.
 - b. Seleccione el primer nodo de almacenamiento en la cuadrícula.
 - c. Seleccione la pestaña Almacenamiento.
 - d. En la sección Volúmenes, busque la entrada **/var/local/rangedb/0**.
 - e. Confirme que el valor Disponible sea igual o mayor que la diferencia entre el nuevo valor que desea utilizar y el valor actual del Espacio reservado de metadatos.

Por ejemplo, si la configuración actual del Espacio reservado de metadatos es 4 TB y desea aumentarla a 6 TB, el valor Disponible debe ser 2 TB o más.

- 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 siguiente paso.
3. Asegúrese de tener al menos 128 GB de RAM en cada nodo de almacenamiento.
 - a. Seleccione **NODOS**.
 - b. Seleccione el primer nodo de almacenamiento en la cuadrícula.
 - c. Seleccione la pestaña **Hardware**.
 - d. Coloque el cursor sobre el gráfico de uso de memoria. Asegúrese de que la **Memoria total** sea 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 se puede aumentar el valor del espacio reservado de metadatos. No continúe con este procedimiento.
 - Si cada nodo de almacenamiento tiene al menos 128 GB de memoria total, vaya al siguiente paso.
4. Actualice la configuración del espacio reservado de metadatos.
 - a. Seleccione **CONFIGURACIÓN > Sistema > Opciones de almacenamiento**.
 - b. Seleccione la pestaña Configuración.
 - c. En la sección Marcas de agua de almacenamiento, seleccione **Espacio reservado de metadatos**.
 - d. Introduzca el nuevo valor.

Por ejemplo, para ingresar 8 TB, que es el valor máximo admitido, ingrese **8000000000000** (8, seguido de 12 ceros)

Storage Options

Overview

Configuration



Configure Storage Options

Updated: 2021-12-10 13:48:23 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1000000000

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0
Storage Volume Soft Read-Only Watermark Override	0
Storage Volume Hard Read-Only Watermark Override	0
Metadata Reserved Space	800000000000

Apply Changes

a. Seleccione **Aplicar cambios**.

Comprimir objetos almacenados

Puede habilitar la compresión de objetos para reducir el tamaño de los objetos almacenados en StorageGRID, de modo que consuman menos almacenamiento.

Antes de empezar

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

Acerca de esta tarea

De forma predeterminada, la compresión de objetos está deshabilitada. Si habilita la compresión, StorageGRID intentará comprimir cada objeto al guardarlo, utilizando compresión sin pérdida.



Si cambia esta configuración, tomará aproximadamente un minuto para que se aplique la nueva configuración. El valor configurado se almacena en caché para mejorar el rendimiento y la escala.

Antes de habilitar la compresión de objetos, tenga en cuenta lo siguiente:

- No debe seleccionar **Comprimir objetos almacenados** a menos que sepa que los datos que se almacenan son comprimibles.
- Las aplicaciones que guardan objetos en StorageGRID pueden comprimirlos antes de guardarlos. Si una aplicación cliente ya ha comprimido un objeto antes de guardarlo en StorageGRID, seleccionar esta opción no reducirá aún más el tamaño del objeto.
- No seleccione **Comprimir objetos almacenados** si está utilizando NetApp FabricPool con StorageGRID.
- Si se selecciona **Comprimir objetos almacenados**, las aplicaciones cliente S3 deben evitar realizar operaciones GetObject que especifiquen un rango de bytes a devolver. Estas operaciones de "lectura de

rango" son ineficientes porque StorageGRID debe descomprimir efectivamente los objetos para acceder a los bytes solicitados. Las operaciones GetObject que solicitan un rango pequeño de bytes de un objeto muy grande son especialmente ineficientes; por ejemplo, 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 expirar.



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 > Configuración de almacenamiento > Compresión de objetos**.
2. Seleccione la casilla de verificación **Comprimir objetos almacenados**.
3. Seleccione **Guardar**.

Administrar nodos de almacenamiento completos

A medida que los nodos de almacenamiento alcanzan su capacidad, debe expandir el sistema StorageGRID mediante la incorporación de nuevo almacenamiento. Hay tres opciones disponibles: agregar volúmenes de almacenamiento, agregar estantes de expansión de almacenamiento y agregar nodos de almacenamiento.

Agregar volúmenes de almacenamiento

Cada nodo de almacenamiento admite una cantidad máxima de volúmenes de almacenamiento. El máximo definido varía según la plataforma. Si un nodo de almacenamiento contiene menos que la cantidad máxima de volúmenes de almacenamiento, puede agregar volúmenes para aumentar su capacidad. Vea las instrucciones para "[Ampliación de un sistema StorageGRID](#)".

Añadir estantes de expansión de almacenamiento

Algunos nodos de almacenamiento del dispositivo StorageGRID, como SG6060 o SG6160, pueden admitir estantes de almacenamiento adicionales. Si tiene dispositivos StorageGRID con capacidades de expansión que aún no se han ampliado a su capacidad máxima, puede agregar estantes de almacenamiento para aumentar la capacidad. Vea las instrucciones para "[Ampliación de un sistema StorageGRID](#)".

Agregar nodos de almacenamiento

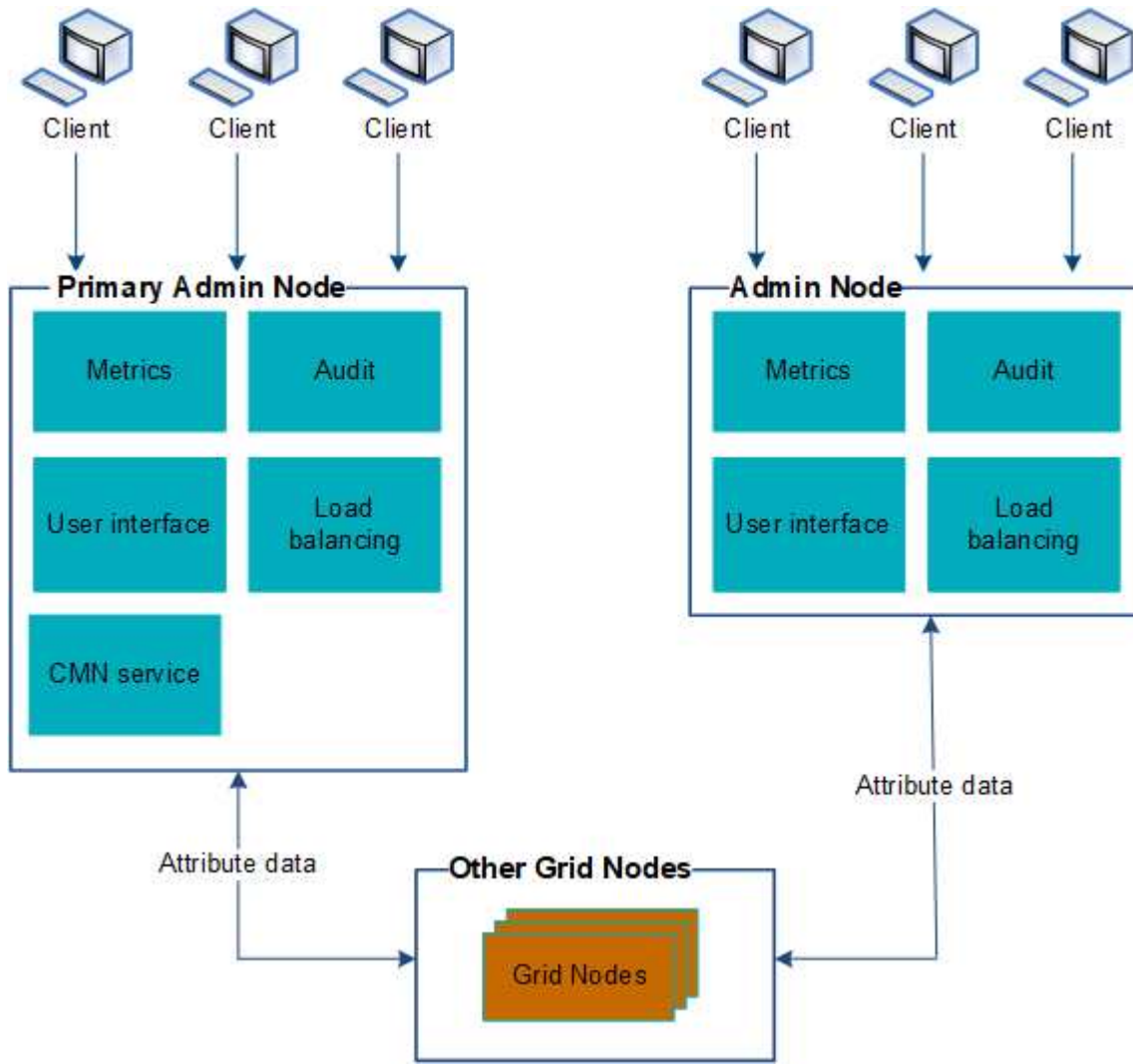
Puede aumentar la capacidad de almacenamiento agregando nodos de almacenamiento. Al agregar almacenamiento se debe tener en cuenta cuidadosamente las reglas ILM actualmente activas y los requisitos de capacidad. Vea las instrucciones para "[Ampliación de un sistema StorageGRID](#)".

Administrar nodos de administración

Utilice varios nodos de administración

Un sistema StorageGRID puede incluir varios nodos de administración para permitirle supervisar y configurar continuamente su sistema StorageGRID incluso si falla un nodo de administración.

Si un nodo de administración deja de estar disponible, el procesamiento de atributos continúa, se siguen activando alertas y se siguen enviando notificaciones por correo electrónico y paquetes de AutoSupport . Sin embargo, tener varios nodos de administración no proporciona protección contra conmutación por error, excepto para las notificaciones y los paquetes de AutoSupport .



Hay dos opciones para continuar viendo y configurando el sistema StorageGRID si falla un nodo de administración:

- Los clientes web pueden reconectarse a cualquier otro nodo de administración disponible.
- Si un administrador del sistema ha configurado un grupo de alta disponibilidad de nodos de administración, los clientes web pueden seguir accediendo al Administrador de red o al Administrador de inquilinos mediante la dirección IP virtual del grupo de alta disponibilidad. Ver ["Administrar grupos de alta disponibilidad"](#) .



Al utilizar un grupo HA, el acceso se interrumpe si falla el nodo de administración activo. Los usuarios deben iniciar sesión nuevamente después de que la dirección IP virtual del grupo HA se conmute a otro nodo de administración en el grupo.

Algunas tareas de mantenimiento solo se pueden realizar mediante el nodo de administración principal. Si el nodo de administración principal falla, debe recuperarse antes de que el sistema StorageGRID vuelva a funcionar por completo.

Identificar el nodo de administración principal

El nodo de administración principal proporciona más funciones que los nodos de administración no principales. Por ejemplo, algunos procedimientos de mantenimiento deben realizarse utilizando el nodo de administración principal.

Para obtener más información sobre los nodos de administración, consulte "[¿Qué es un nodo de administración?](#)".

Antes de empezar

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

Pasos

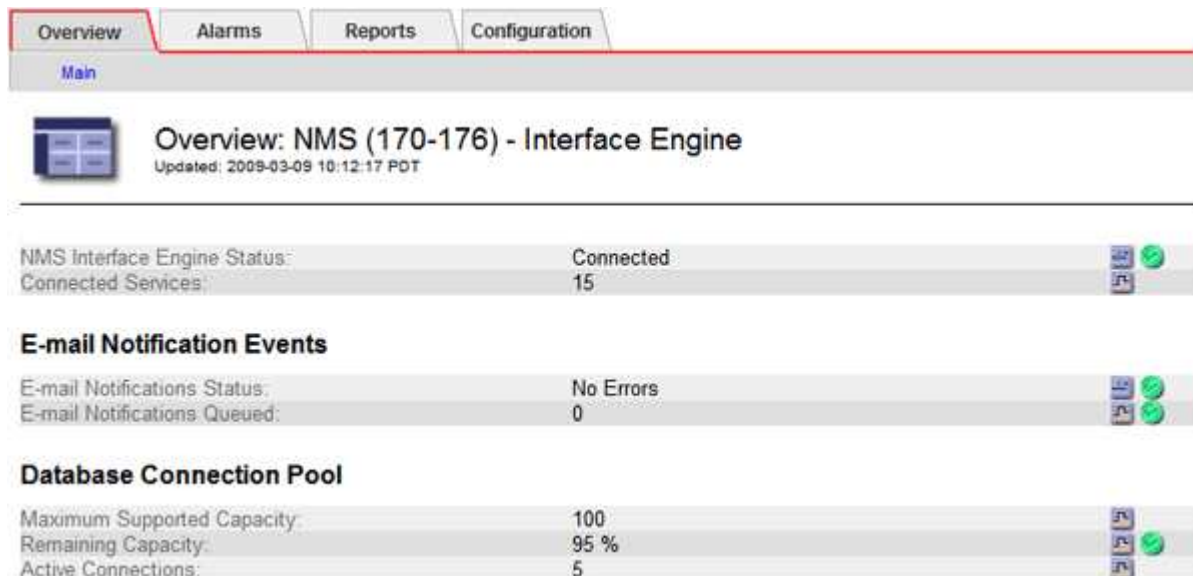
1. Seleccione **NODOS**.
2. Introduzca **primary** en el cuadro de búsqueda.

En los resultados de la búsqueda, identifique el nodo con "Nodo de administración principal" que se muestra en la columna Tipo. Se debe incluir un nodo de administración principal.

Ver el estado de las notificaciones y las colas

El servicio del Sistema de administración de red (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 **SOPORTE > Herramientas > Topología de cuadrícula**. Luego seleccione **site > Admin Node > NMS > Interface Engine**.



The screenshot displays the 'Overview: NMS (170-176) - Interface Engine' page. At the top, there are tabs for 'Overview', 'Alarms', 'Reports', and 'Configuration'. Below the tabs, the page title is 'Overview: NMS (170-176) - Interface Engine' with a timestamp 'Updated: 2009-03-09 10:12:17 PDT'. The main content area is divided into three sections:

- NMS Interface Engine Status:** Shows 'Connected' with a green checkmark icon. Below it, 'Connected Services:' shows '15' with a green checkmark icon.
- E-mail Notification Events:** Shows 'E-mail Notifications Status:' as 'No Errors' and 'E-mail Notifications Queued:' as '0', both with green checkmark icons.
- Database Connection Pool:** Shows 'Maximum Supported Capacity:' as '100', 'Remaining Capacity:' as '95 %', and 'Active Connections:' as '5', all with green checkmark icons.

Las notificaciones se procesan a través de la cola de notificaciones por 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, el máximo esfuerzo posible para 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

elimina de la cola de notificaciones y se intenta enviar la siguiente notificación en la cola.

Administrar objetos con ILM

Administrar objetos con ILM

Las reglas de administración del ciclo de vida de la información (ILM) en una política ILM indican a StorageGRID cómo crear y distribuir copias de datos de objetos y cómo administrar esas copias a lo largo del tiempo.

Acerca de estas instrucciones

El diseño y la implementación de reglas y políticas de ILM requieren una planificación cuidadosa. Debe comprender sus requisitos operativos, la topología de su sistema StorageGRID, sus necesidades de protección de objetos y los tipos de almacenamiento disponibles. Luego, debes determinar cómo quieres que se copien, distribuyan y almacenen los diferentes tipos de objetos.

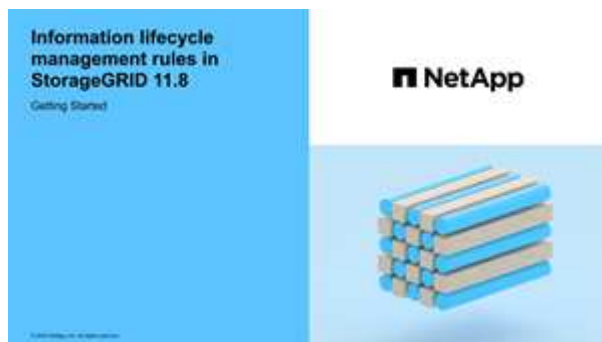
Utilice estas instrucciones para:

- Obtenga más información sobre StorageGRID ILM, incluido ["Cómo funciona ILM a lo largo de la vida de un objeto"](#).
- Aprenda a configurar ["grupos de almacenamiento"](#), ["Grupos de almacenamiento en la nube"](#), y ["Reglas de ILM"](#).
- Aprenda cómo ["crear, simular y activar una política ILM"](#) que protegerá los datos de los objetos en uno o más sitios.
- Aprenda cómo ["Administrar objetos con S3 Object Lock"](#), lo que ayuda a garantizar que los objetos en depósitos S3 específicos no se eliminen ni se sobrescriban durante un período de tiempo específico.

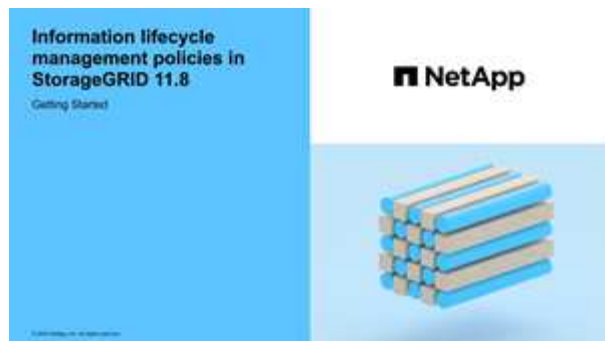
Más información

Para obtener más información, revise estos videos:

- ["Vídeo: Resumen de las reglas de ILM"](#).



- ["Vídeo: Resumen de las políticas de ILM"](#)



ILM y ciclo de vida de los objetos

Cómo funciona ILM a lo largo de la vida de un objeto

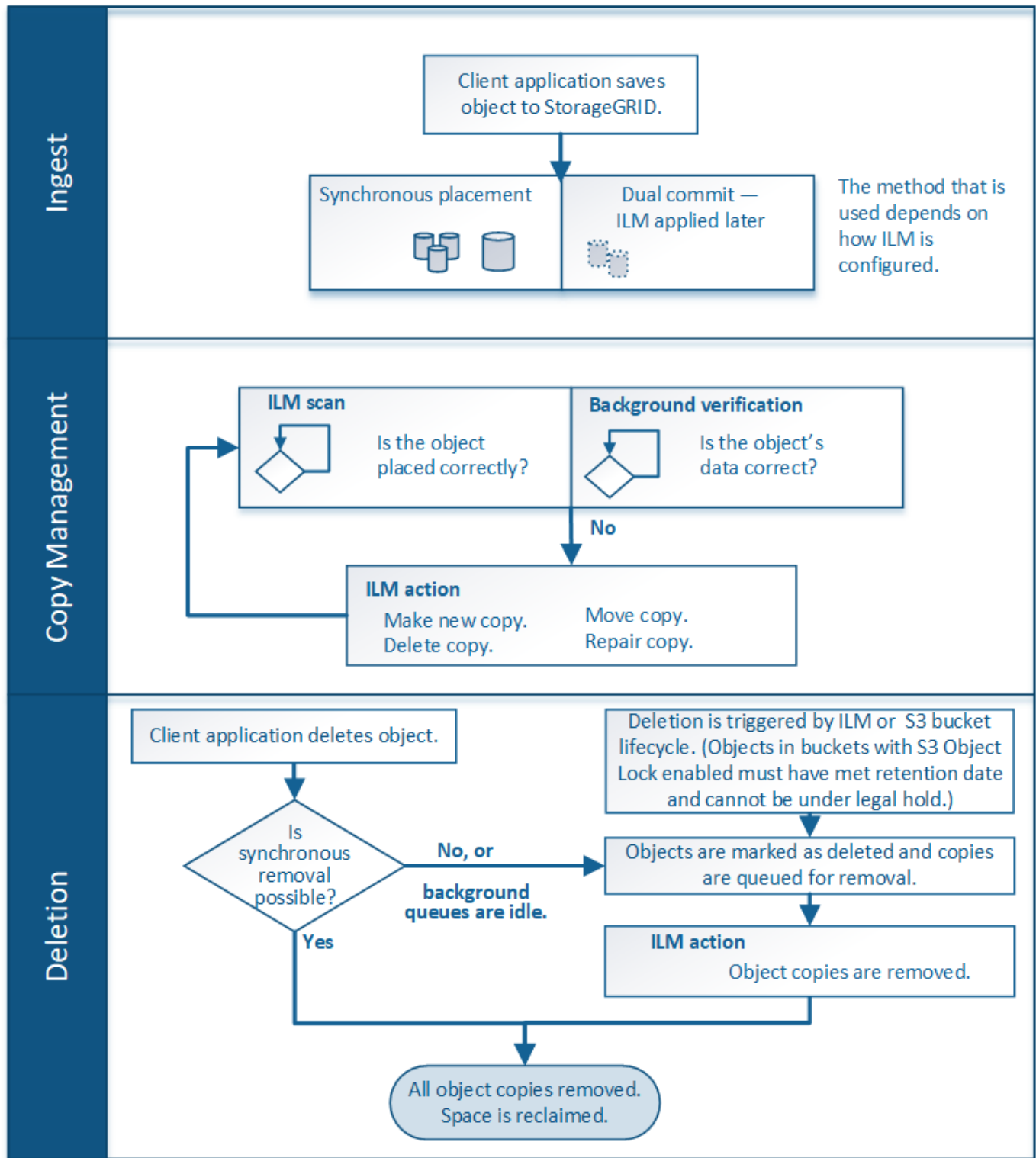
Comprender cómo StorageGRID utiliza ILM para administrar objetos durante cada etapa de su vida puede ayudarlo a diseñar una política más efectiva.

- **Ingesta:** la ingesta comienza cuando una aplicación cliente S3 establece una conexión para guardar un objeto en el sistema StorageGRID y se completa cuando StorageGRID devuelve un mensaje de "ingesta exitosa" al cliente. Los datos de los objetos se protegen durante la ingesta ya sea aplicando instrucciones ILM inmediatamente (colocación sincrónica) o creando copias provisionales y aplicando ILM más tarde (confirmación dual), dependiendo de cómo se especificaron los requisitos de ILM.
- **Administración de copias:** después de crear la cantidad y el tipo de copias de objetos que se especifican en las instrucciones de ubicación de ILM, StorageGRID administra las ubicaciones de los objetos y los protege contra pérdidas.
 - **Escaneo y evaluación de ILM:** StorageGRID escanea continuamente la lista de objetos almacenados en la red y verifica si las copias actuales cumplen con los requisitos de ILM. Cuando se requieren diferentes tipos, números o ubicaciones de copias de objetos, StorageGRID crea, elimina o mueve copias según sea necesario.
 - **Verificación en segundo plano:** StorageGRID realiza continuamente una verificación en segundo plano para comprobar la integridad de los datos de los objetos. Si se encuentra un problema, StorageGRID crea automáticamente una nueva copia del objeto o un fragmento de objeto con código de borrado de reemplazo en una ubicación que cumpla con los requisitos ILM actuales. Ver ["Verificar la integridad del objeto"](#).
- **Eliminación de objetos:** la administración 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 como resultado de una eliminación por parte de ILM o una eliminación causada por la expiración del ciclo de vida de un bucket de S3.



Los objetos de un bucket que tiene habilitado el bloqueo de objetos S3 no se pueden eliminar si están bajo una retención legal o si se ha especificado una fecha de retención pero aún no se cumple.

El diagrama resume cómo funciona ILM a lo largo del ciclo de vida de un objeto.



Cómo se ingieren los objetos

Opciones de ingesta

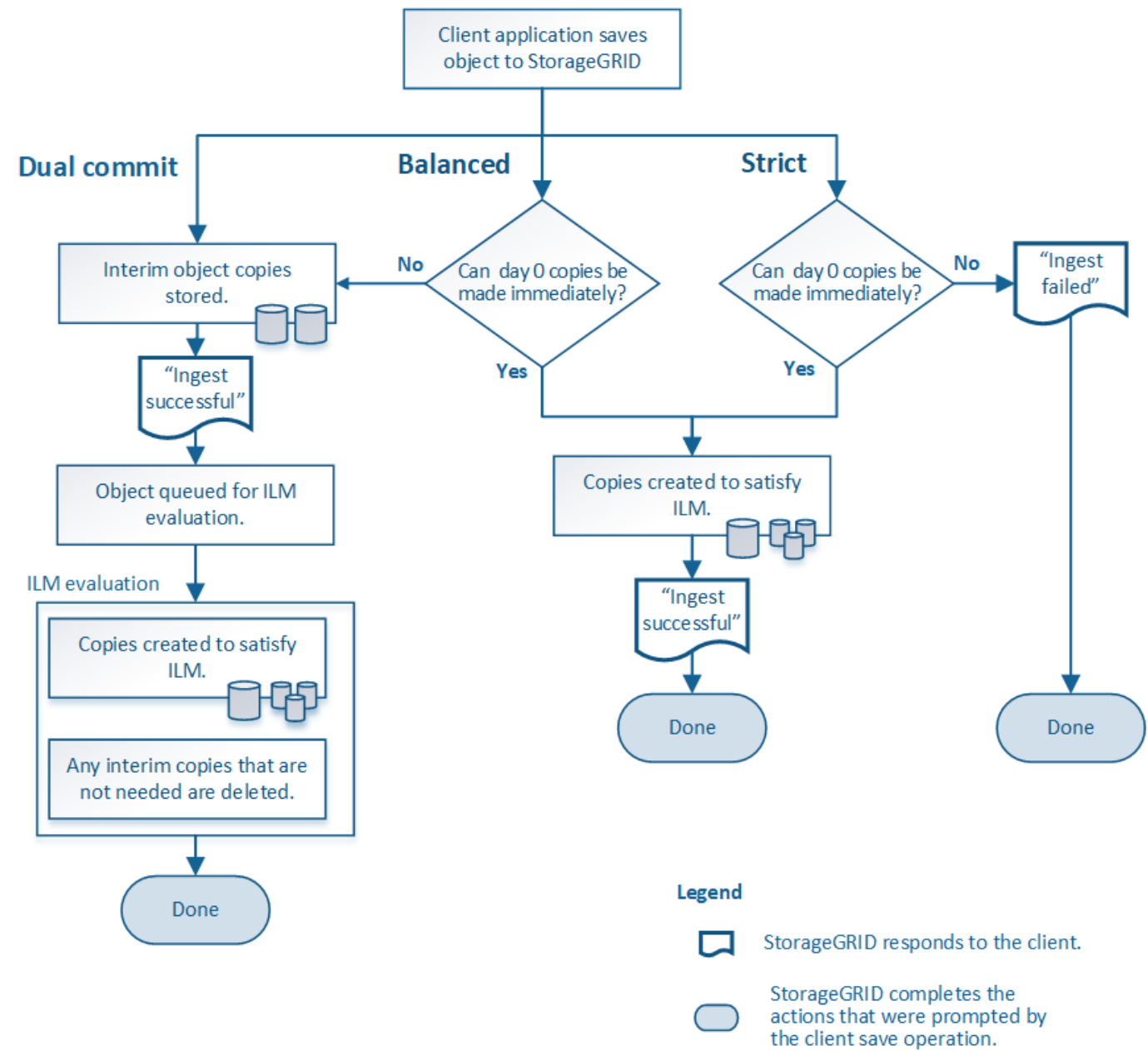
Cuando crea una regla ILM, especifica una de tres opciones para proteger objetos durante la ingesta: Confirmación dual, Estricta o Equilibrada.

Según su elección, StorageGRID realiza copias provisionales y pone en cola los objetos para una evaluación

ILM posterior, o utiliza la ubicación sincrónica y realiza copias inmediatamente para cumplir con los requisitos de ILM.

Diagrama de flujo de opciones de ingesta

El diagrama de flujo muestra lo que sucede cuando los objetos coinciden con una regla ILM que utiliza cada una de las tres opciones de ingesta.



Compromiso dual

Cuando selecciona la opción de confirmación dual, StorageGRID realiza inmediatamente copias de objetos provisionales en dos nodos de almacenamiento diferentes y devuelve un mensaje de "ingesta exitosa" al cliente. El objeto se pone en cola para la evaluación de ILM y luego se realizan copias que cumplen con las instrucciones de ubicación de la regla. Si la política ILM no se puede procesar inmediatamente después de la confirmación dual, la protección contra pérdida del sitio podría llevar tiempo.

Utilice la opción de confirmación dual en cualquiera de estos casos:

- Está utilizando reglas ILM de múltiples sitios y la latencia de ingesta del cliente es su consideración principal. Al usar la confirmación dual, debe asegurarse de que su cuadrícula pueda realizar el trabajo adicional de crear y eliminar las copias de confirmación dual si no satisfacen ILM. Específicamente:
 - La carga en la red debe ser lo suficientemente baja para evitar un retraso en la ILM.
 - La red debe tener recursos de hardware excedentes (IOPS, CPU, memoria, ancho de banda de red, etc.).
- Está utilizando reglas ILM de varios sitios y la conexión WAN entre los sitios generalmente tiene alta latencia o ancho de banda limitado. En este escenario, el uso de la opción de confirmación dual puede ayudar a evitar tiempos de espera del cliente. Antes de elegir la opción de confirmación dual, debe probar la aplicación cliente con cargas de trabajo realistas.

Equilibrado (predeterminado)

Cuando selecciona la opción Equilibrado, StorageGRID también utiliza la ubicación sincrónica en la ingesta y realiza 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 dual en su lugar. Si la política ILM utiliza ubicaciones en varios sitios y no se puede lograr una protección inmediata contra pérdida de sitios, se activa la alerta **Ubicación ILM inalcanzable**.

Utilice la opción Equilibrado para lograr la mejor combinación de protección de datos, rendimiento de la red y éxito de ingesta. Equilibrado es la opción predeterminada en el asistente Crear regla ILM.

Estricto

Cuando selecciona la opción Estricto, StorageGRID utiliza la ubicación sincrónica en la ingesta y realiza inmediatamente todas las copias de objetos especificadas en las instrucciones de ubicación de la regla. La ingesta falla si StorageGRID no puede crear todas las copias, por ejemplo, porque una ubicación de almacenamiento requerida no está disponible temporalmente. El cliente debe volver a intentar la operación.

Utilice la opción Estricto si tiene un requisito operativo o reglamentario para almacenar inmediatamente objetos solo en las ubicaciones descritas en la regla ILM. Por ejemplo, para satisfacer un requisito reglamentario, es posible que necesite utilizar la opción Estricto y un filtro avanzado de Restricción de ubicación para garantizar que los objetos nunca se almacenen en determinados centros de datos.

Ver ["Ejemplo 5: Reglas y políticas de ILM para el comportamiento de ingesta estricto"](#) .

Ventajas, desventajas y limitaciones de las opciones de ingesta

Comprender las ventajas y desventajas de cada una de las tres opciones para proteger datos en la ingesta (equilibrada, estricta o confirmación dual) puede ayudarlo a decidir cuál seleccionar para una regla ILM.

Para obtener una descripción general de las opciones de ingesta, consulte ["Opciones de ingesta"](#) .

Ventajas de las opciones Equilibrada y Estricta

En comparación con la confirmación dual, que crea copias provisionales durante la ingesta, las dos opciones de ubicación sincrónica pueden proporcionar las siguientes ventajas:

- **Mejor seguridad de los datos:** los datos de los objetos se protegen inmediatamente como se especifica en las instrucciones de ubicación de las reglas ILM, que se pueden configurar para proteger contra una amplia variedad de condiciones de falla, incluida la falla de más de una ubicación de almacenamiento. La confirmación dual solo puede proteger contra la pérdida de una única copia local.

- **Operación de red más eficiente:** cada objeto se procesa solo una vez, a medida que se ingiere. Debido a que el sistema StorageGRID no necesita rastrear ni eliminar copias provisionales, hay menos carga de procesamiento y se consume menos espacio de base de datos.
- **(Equilibrado) Recomendado:** La opción Equilibrada proporciona una eficiencia ILM óptima. Se recomienda usar la opción Equilibrada a menos que se requiera un comportamiento de ingesta estricto o la cuadrícula cumpla con todos los criterios para usar la confirmación dual.
- **(Estricta) Certeza sobre las ubicaciones de los objetos:** La opción Estricta garantiza que los objetos se almacenen inmediatamente de acuerdo con las instrucciones de ubicación de la regla ILM.

Desventajas de las opciones equilibrada y estricta

En comparación con la confirmación dual, las opciones equilibrada y estricta tienen algunas desventajas:

- **Ingestas de cliente más prolongadas:** las latencias de ingesta de cliente pueden ser más prolongadas. Cuando se utilizan las opciones Equilibrado o Estricto, no se devuelve un mensaje de "ingesta exitosa" al cliente hasta que se crean y almacenan todos los fragmentos codificados de borrado o copias replicadas. Sin embargo, lo más probable es que los datos de los objetos lleguen a su ubicación final mucho más rápido.
- **(Estricto) Mayores tasas de errores de ingesta:** con la opción Estricto, la ingesta falla siempre que StorageGRID no pueda realizar inmediatamente todas las copias especificadas en la regla ILM. Es posible que observe altas tasas de errores de ingesta si una ubicación de almacenamiento requerida está temporalmente fuera de línea o si los problemas de red causan demoras en la copia de objetos entre sitios.
- **(Estricto) Las ubicaciones de carga multiparte de S3 podrían no ser las esperadas en algunas circunstancias:** con Estricto, se espera que los objetos se coloquen como lo describe la regla ILM o que la ingesta falle. Sin embargo, con una carga multiparte de S3, ILM se evalúa para cada parte del objeto a medida que se ingiere y para el objeto como un todo cuando se completa la carga multiparte. En las siguientes circunstancias, esto podría dar lugar a ubicaciones diferentes a las esperadas:
 - **Si ILM cambia mientras una carga multiparte de S3 está en progreso:** debido a que cada parte se coloca de acuerdo con la regla que está activa cuando se ingiere la parte, es posible que algunas partes del objeto no cumplan con los requisitos actuales de ILM cuando se complete la carga multiparte. En estos casos la ingesta del objeto no falla. En cambio, cualquier pieza que no esté colocada correctamente se pone en cola para una reevaluación de ILM y se mueve a la ubicación correcta más tarde.
 - **Cuando las reglas ILM filtran por tamaño:** al evaluar ILM para una pieza, StorageGRID filtra por el tamaño de la pieza, no por el tamaño del objeto. Esto significa que partes de un objeto pueden almacenarse en ubicaciones que no cumplen los requisitos de ILM para el objeto en su totalidad. 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 momento de la ingesta 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.
- **(Estricto) La ingesta no falla cuando se actualizan las etiquetas o los metadatos de los objetos y no se pueden realizar las nuevas ubicaciones requeridas:** con Estricto, se espera que los objetos se coloquen como lo describe la regla ILM o que la ingesta falle. Sin embargo, cuando se actualizan los metadatos o las etiquetas de un objeto que ya está almacenado en la cuadrícula, el objeto no se vuelve a ingerir. Esto significa que cualquier cambio en la ubicación de los objetos que se active mediante la actualización no se realiza de inmediato. Los cambios de ubicación se realizan cuando el ILM se vuelve a evaluar mediante procesos ILM en segundo plano normales. Si no se pueden realizar los cambios de ubicación requeridos (por ejemplo, porque la nueva ubicación requerida no está disponible), el objeto actualizado conserva su ubicación actual hasta que sea posible realizar los cambios de ubicación.

Limitaciones en la ubicación de objetos con las opciones Equilibrado y Estricto

Las opciones Equilibrado o Estricto no se pueden usar para reglas ILM que tengan alguna de estas instrucciones de ubicación:

- Ubicación en un grupo de almacenamiento en la nube el día 0.
- Ubicaciones en un grupo de almacenamiento en la nube cuando la regla tiene un tiempo de creación definido por el usuario como su tiempo de referencia.

Estas restricciones existen porque StorageGRID no puede realizar copias de manera sincrónica a un grupo de almacenamiento en la nube, y un tiempo de creación definido por el usuario podría resolverse en el presente.

Cómo interactúan las reglas y la consistencia de ILM para afectar la protección de datos

Tanto su regla ILM como su elección de consistencia afectan cómo se protegen los objetos. Estas configuraciones pueden interactuar.

Por ejemplo, el comportamiento de ingesta seleccionado para una regla ILM afecta la ubicación inicial de las copias de objetos, mientras que la consistencia utilizada cuando se almacena un objeto afecta la ubicación inicial de los metadatos del objeto. Debido a que StorageGRID requiere acceso a los datos y metadatos de un objeto para cumplir con las solicitudes de los clientes, seleccionar niveles de protección coincidentes para la consistencia y el comportamiento de ingesta puede brindar una mejor protección de datos inicial y respuestas del sistema más predecibles.

A continuación se muestra un breve resumen de los valores de consistencia disponibles en StorageGRID:

- **Todos:** Todos los nodos reciben metadatos del objeto inmediatamente o la solicitud fallará.
- **Fuerte-global:** Los metadatos de los objetos se distribuyen inmediatamente a todos los sitios. Garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios.
- **Sitio fuerte:** los metadatos del objeto se distribuyen inmediatamente a otros nodos del sitio. Garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes dentro de un sitio.
- **Lectura después de nueva escritura:** proporciona consistencia de lectura después de escritura para nuevos objetos y consistencia eventual para actualizaciones de objetos. Ofrece alta disponibilidad y garantías de protección de datos. Recomendado para la mayoría de los casos.
- **Disponible:** Proporciona consistencia eventual tanto para objetos nuevos como para actualizaciones de objetos. Para los buckets S3, úselo solo cuando sea necesario (por ejemplo, para un bucket que contiene valores de registro que rara vez se leen, o para operaciones HEAD o GET en claves que no existen). No compatible con depósitos S3 FabricPool .



Antes de seleccionar un valor de consistencia, "[Lea la descripción completa de la consistencia](#)". Debe comprender los beneficios y las limitaciones antes de cambiar el valor predeterminado.

Ejemplo de cómo la consistencia y las reglas ILM pueden interactuar

Supongamos que tiene una cuadrícula de dos sitios con la siguiente regla ILM y la siguiente consistencia:

- **Regla ILM:** Crea dos copias de objetos, una en el sitio local y otra en un sitio remoto. Utilice el comportamiento de ingesta estricto.
- **Consistencia:** Fuerte-global (los metadatos del objeto se distribuyen inmediatamente a todos los sitios).

Cuando un cliente almacena un objeto en la red, StorageGRID realiza copias de los objetos y distribuye metadatos a ambos sitios antes de devolver el éxito al cliente.

El objeto está completamente protegido contra pérdida en el momento del mensaje de ingesta exitosa. Por ejemplo, si el sitio local se pierde poco después de la ingesta, aún existen copias de los datos del objeto y de los metadatos del objeto en el sitio remoto. El objeto es completamente recuperable.

Si, en cambio, utilizara la misma regla ILM y la consistencia del sitio fuerte, el cliente podría recibir un mensaje de éxito después de que los datos del objeto se repliquen 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 del objeto no coincide con el nivel de protección de los datos del objeto. Si el sitio local se pierde poco después de la ingesta, se pierden los metadatos del objeto. No se puede recuperar el objeto.

La interrelación entre la consistencia y las reglas ILM puede ser compleja. Comuníquese con NetApp si necesita ayuda.

Información relacionada

["Ejemplo 5: Reglas y políticas de ILM para el comportamiento de ingesta estricto"](#)

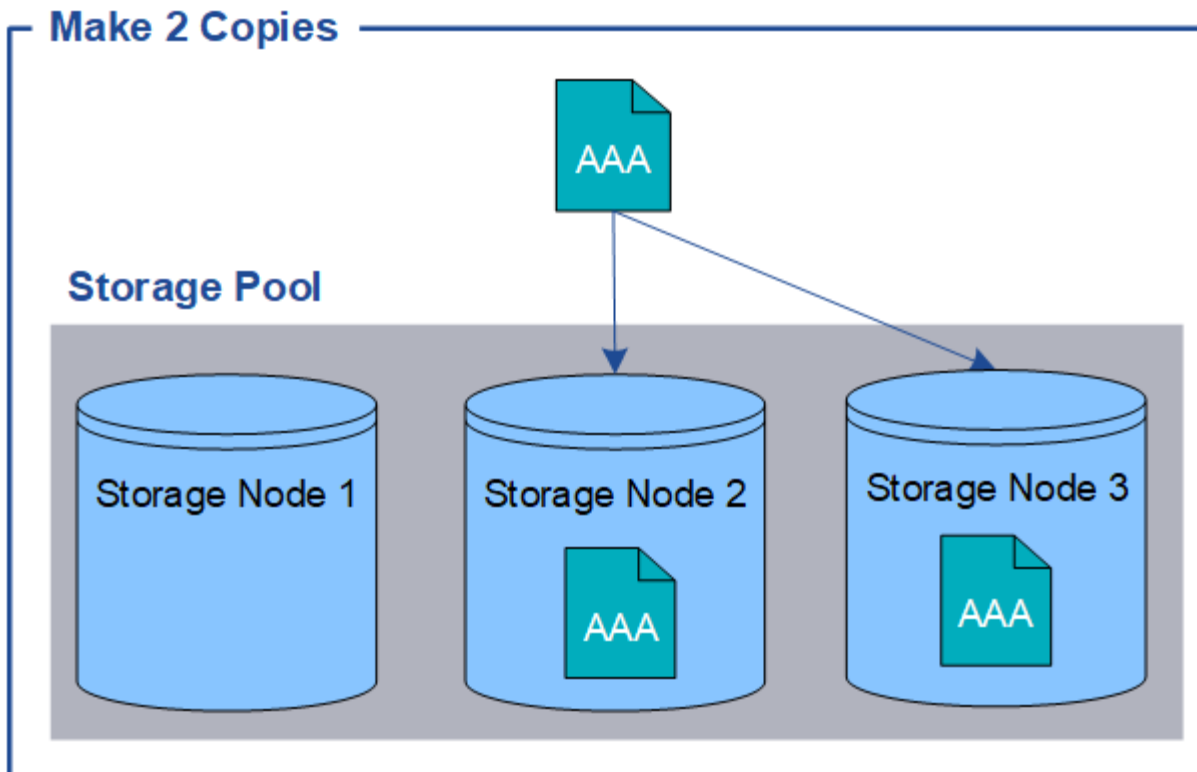
Cómo se almacenan los objetos (codificación de replicación o borrado)

¿Qué es la replicación?

La replicación es uno de los dos métodos utilizados por StorageGRID para almacenar datos de objetos (la codificación de borrado es el otro método). Cuando los objetos coinciden con una regla ILM que utiliza replicación, el sistema crea copias exactas de los datos de los objetos y almacena las copias en los nodos de almacenamiento.

Cuando configura una regla ILM para crear copias replicadas, especifica cuántas copias se deben crear, dónde se deben colocar esas copias y durante cuánto tiempo se deben almacenar las copias en cada ubicación.

En el siguiente ejemplo, la regla ILM especifica que dos copias replicadas de cada objeto se coloquen en un grupo de almacenamiento que contiene tres nodos de almacenamiento.



Cuando StorageGRID hace coincidir objetos con esta regla, crea dos copias del objeto y coloca cada copia en un nodo de almacenamiento diferente en el grupo de almacenamiento. Las dos copias se pueden colocar en cualquiera de los 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. Dado que hay dos copias, el objeto se puede recuperar si alguno de los nodos del grupo de almacenamiento falla.



StorageGRID solo puede almacenar una copia replicada de un objeto en cualquier nodo de almacenamiento determinado. Si su red incluye tres nodos de almacenamiento y crea una regla ILM de 4 copias, solo se realizarán tres copias: una copia para cada nodo de almacenamiento. La alerta **Colocación ILM inalcanzable** se activa para indicar que la regla ILM no se pudo aplicar por completo.

Información relacionada

- ["¿Qué es la codificación de borrado?"](#)
- ["¿Qué es un pool de almacenamiento?"](#)
- ["Habilite la protección contra pérdida de sitios mediante codificación de replicación y borrado"](#)

Por qué no debería utilizar la replicación de copia única

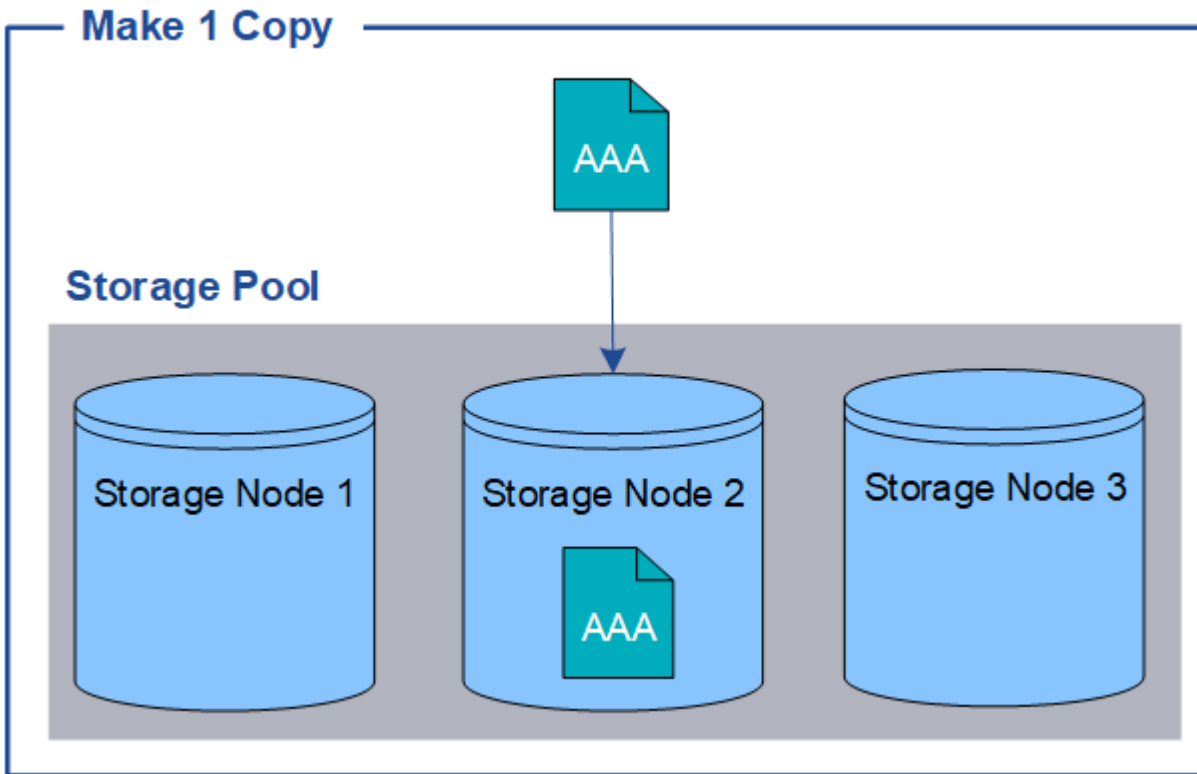
Al crear una regla ILM para crear copias replicadas, siempre debe especificar al menos dos copias para cualquier período de tiempo en las instrucciones de ubicación.



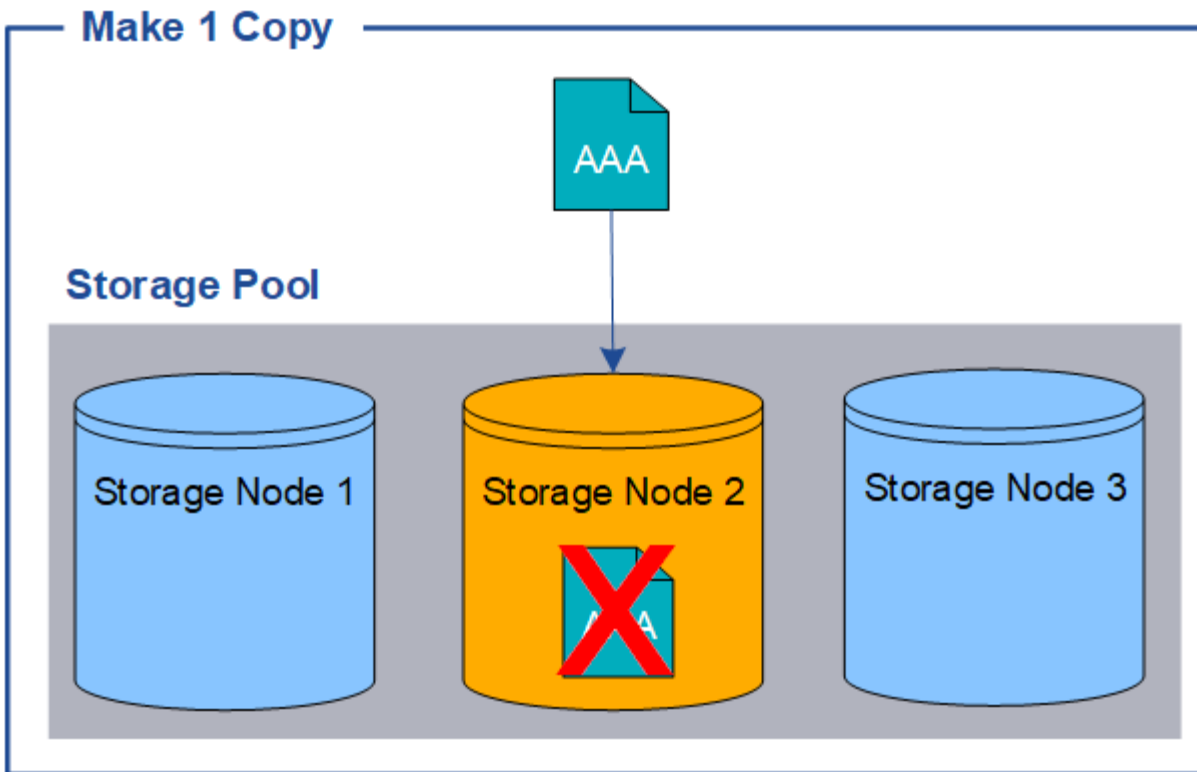
No utilice una regla ILM que cree solo una copia replicada por un período de tiempo determinado. Si solo existe una copia replicada de un objeto, ese objeto se pierde si un nodo de almacenamiento falla o tiene un error significativo. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como actualizaciones.

En el siguiente ejemplo, la regla ILM Realizar 1 copia especifica que una copia replicada de un objeto se

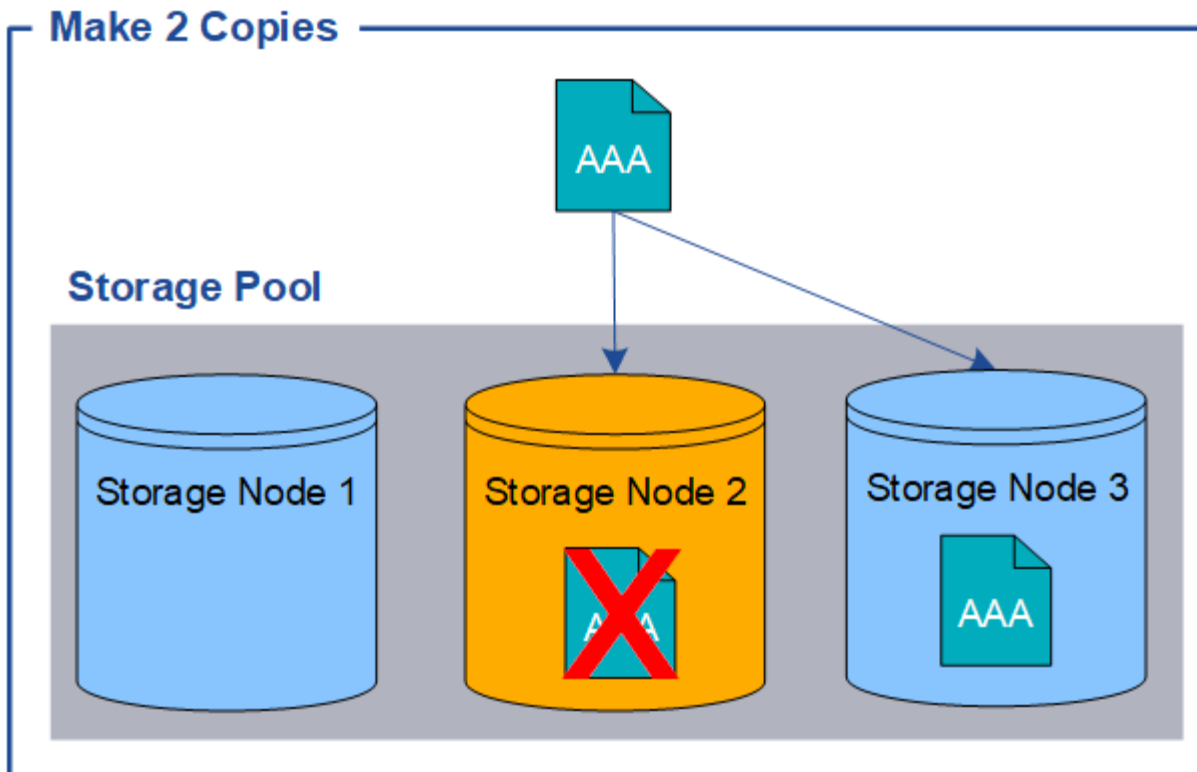
coloque en un grupo de almacenamiento que contenga tres nodos de almacenamiento. Cuando se ingiere un objeto que coincide con esta regla, StorageGRID coloca una única copia en un solo nodo de almacenamiento.



Cuando una regla ILM crea solo una copia replicada de un objeto, el 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 fuera de línea, como durante una actualización u otro procedimiento de mantenimiento. Perderá el objeto AAA por completo si falla el Nodo de almacenamiento 2.



Para evitar perder datos de objetos, siempre debe hacer al menos dos copias de todos los objetos que desee proteger con replicación. Si existen dos o más copias, aún podrá acceder al objeto si un nodo de almacenamiento falla o se desconecta.



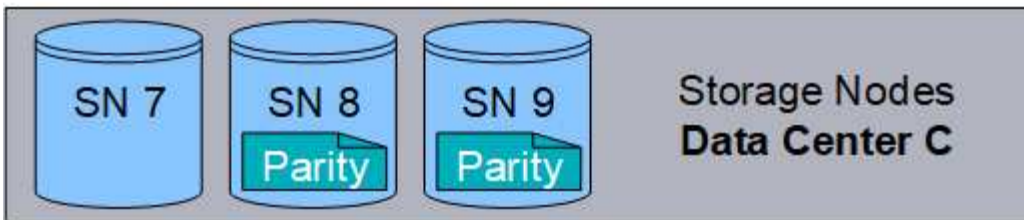
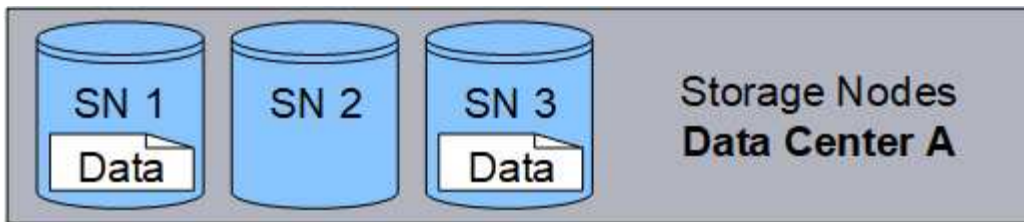
¿Qué es la codificación de borrado?

La codificación de borrado es uno de los dos métodos que utiliza StorageGRID para almacenar datos de objetos (la replicación es el otro método). Cuando los objetos coinciden con una regla ILM que utiliza codificación de borrado, esos objetos se dividen en fragmentos de datos, se calculan fragmentos de paridad adicionales y cada fragmento se almacena en un nodo de almacenamiento diferente.

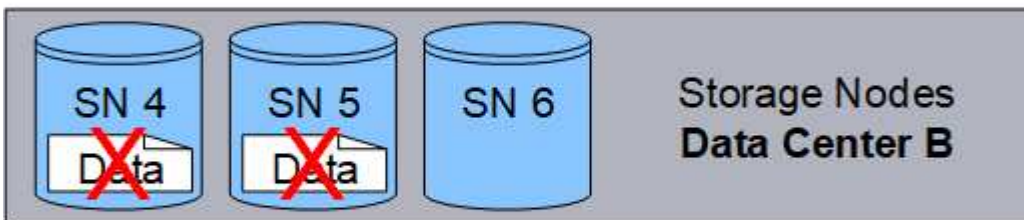
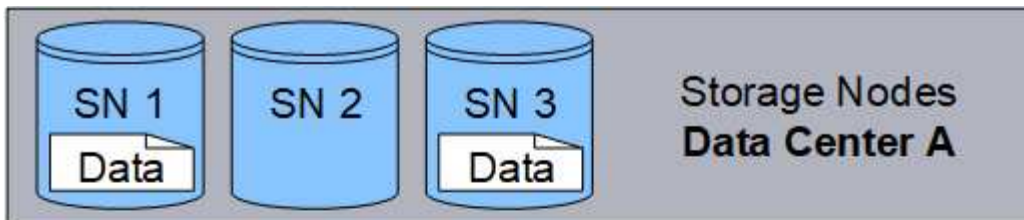
Cuando se accede a un objeto, se vuelve a ensamblar utilizando los fragmentos almacenados. Si un fragmento de datos o de paridad se corrompe o se pierde, el algoritmo de codificación de borrado puede recrear ese fragmento utilizando un subconjunto de los fragmentos de datos y de paridad restantes.

A medida que crea reglas ILM, StorageGRID crea perfiles de codificación de borrado que admiten esas reglas. Puede ver una lista de perfiles de codificación de borrado, ["cambiar el nombre de un perfil de codificación de borrado"](#), o ["Desactivar un perfil de codificación de borrado si no se utiliza actualmente en ninguna regla ILM"](#).

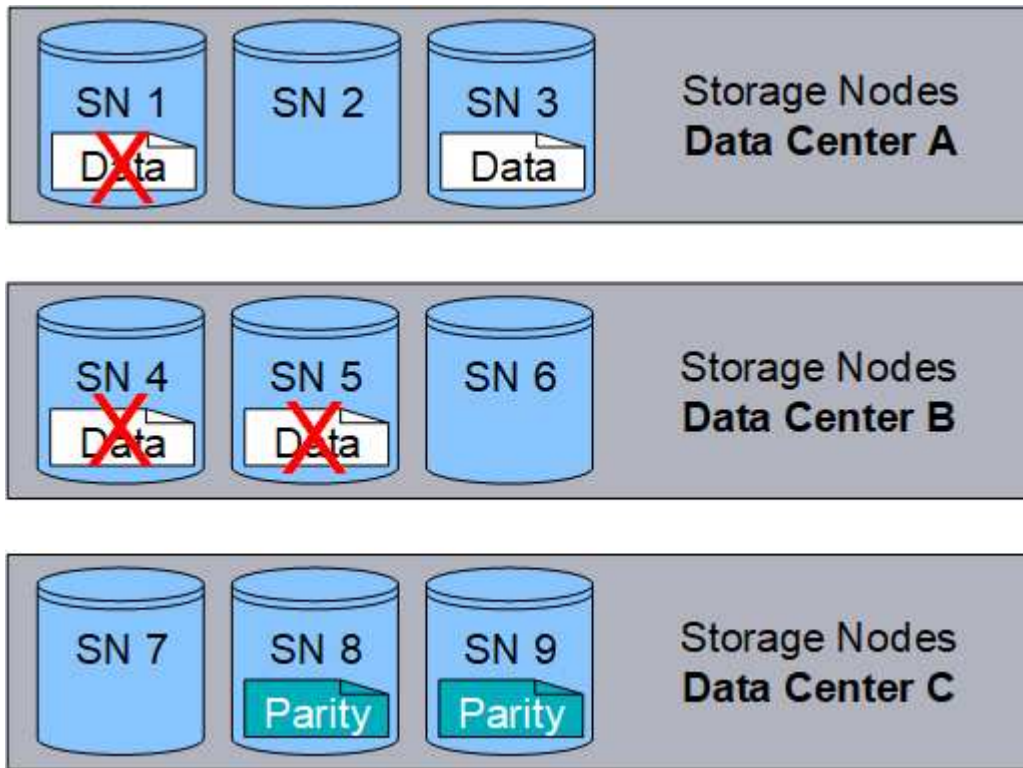
El siguiente ejemplo ilustra el uso de un algoritmo de codificación de borrado en los datos de un objeto. En este ejemplo, la regla ILM utiliza un esquema de codificación de borrado 4+2. Cada objeto se divide en cuatro fragmentos de datos iguales y se calculan dos fragmentos de paridad a partir de los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



El esquema de codificación de borrado 4+2 se puede configurar de varias maneras. Por ejemplo, puede configurar un grupo de almacenamiento de un solo sitio que contenga seis nodos de almacenamiento. Para "protección contra pérdida de sitio", puede utilizar un grupo de almacenamiento que contenga tres sitios con tres nodos de almacenamiento en cada sitio. Se puede recuperar un objeto siempre que cuatro de los seis fragmentos (datos o paridad) permanezcan disponibles. Se pueden perder hasta dos fragmentos sin perder los datos del objeto. Si se pierde un sitio entero, el objeto aún puede recuperarse o repararse, siempre que todos los demás fragmentos permanezcan accesibles.



Si se pierden más de dos nodos de almacenamiento, el objeto no se podrá recuperar.



Información relacionada

- ["¿Qué es la replicación?"](#)
- ["¿Qué es un pool de almacenamiento?"](#)
- ["¿Qué son los esquemas de codificación de borrado?"](#)
- ["Cambiar el nombre de un perfil de codificación de borrado"](#)
- ["Desactivar un perfil de codificación de borrado"](#)

¿Qué son los esquemas de codificación de borrado?

Los esquemas de codificación de borrado controlan cuántos fragmentos de datos y cuántos fragmentos de paridad se crean para cada objeto.

Cuando crea o edita una regla ILM, selecciona un esquema de codificación de borrado disponible. StorageGRID crea automáticamente esquemas de codificación de borrado en función de la cantidad de nodos de almacenamiento y sitios que conforman el grupo de almacenamiento que planea utilizar.

Protección de datos

El sistema StorageGRID utiliza el algoritmo de codificación de borrado Reed-Solomon. El algoritmo divide un objeto en k fragmentos de datos y m fragmentos de paridad.

El $k + m = n$ Los fragmentos se encuentran dispersos en n Nodos de almacenamiento para proporcionar protección de datos de la siguiente manera:

- Para recuperar o reparar un objeto, k Se necesitan fragmentos.
- Un objeto puede soportar hasta m fragmentos perdidos o corruptos. Cuanto mayor sea el valor de m ,

mayor será la tolerancia al fallo.

La mejor protección de datos la proporciona el esquema de codificación de borrado con la mayor tolerancia a fallas de nodo o volumen dentro de un grupo de almacenamiento.

Gastos generales de almacenamiento

La sobrecarga de almacenamiento de un esquema de codificación de borrado se calcula dividiendo el número de fragmentos de paridad(m) por el número de fragmentos de datos(k). Puede utilizar la sobrecarga de almacenamiento para calcular cuánto espacio en disco requiere cada objeto con código de borrado:

$$\text{disk space} = \text{object size} + (\text{object size} * \text{storage overhead})$$

Por ejemplo, si almacena un objeto de 10 MB utilizando el esquema 4+2 (que tiene una sobrecarga de almacenamiento del 50 %), el objeto consume 15 MB de almacenamiento en la red. Si almacena el mismo objeto de 10 MB utilizando el esquema 6+2 (que tiene una sobrecarga de almacenamiento del 33 %), el objeto consume aproximadamente 13,3 MB.

Seleccione el esquema de codificación 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 son computacionalmente más eficientes porque:

- Se crean y distribuyen (o recuperan) menos fragmentos por objeto
- Muestran un mejor rendimiento porque el tamaño del fragmento es mayor
- Pueden requerir que se agreguen menos nodos en un ["expansión cuando se requiere más almacenamiento"](#)

Directrices para los pools de almacenamiento

Al seleccionar el grupo de almacenamiento que se utilizará para una regla que creará una copia con código de borrado, utilice las siguientes pautas para los grupos de almacenamiento:

- El grupo de almacenamiento debe incluir tres o más sitios, o exactamente un sitio.



No se puede utilizar la codificación de borrado si el grupo de almacenamiento incluye dos sitios.

- [Esquemas de codificación de borrado para grupos de almacenamiento que contienen tres o más sitios](#)
- [Esquemas de codificación de borrado para grupos de almacenamiento de un solo sitio](#)

- No utilice un grupo de almacenamiento que incluya el sitio Todos los sitios.
- El grupo de almacenamiento debe incluir al menos $k+m + 1$ Nodos de almacenamiento que pueden almacenar datos de objetos.



Los nodos de almacenamiento se pueden configurar durante la instalación para que contengan solo metadatos de objetos y no datos de objetos. Para obtener más información, consulte ["Tipos de nodos de almacenamiento"](#).

El número mínimo de nodos de almacenamiento requeridos es $k+m$. Sin embargo, tener al menos un nodo de almacenamiento adicional puede ayudar a prevenir fallas de ingesta o retrasos en ILM si un nodo de almacenamiento requerido no está disponible temporalmente.

Esquemas de codificación de borrado para grupos de almacenamiento que contienen tres o más sitios

La siguiente tabla describe los esquemas de codificación de borrado actualmente admitidos por StorageGRID para grupos de almacenamiento que incluyen tres o más sitios. Todos estos esquemas brindan protección contra pérdida de sitio. Se puede perder un sitio y el objeto seguirá siendo accesible.

Para los esquemas de codificación de borrado que brindan protección contra pérdida de sitio, la cantidad recomendada de nodos de almacenamiento en el grupo de almacenamiento excede $k+m + 1$ 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%
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 utilizar cinco nodos de almacenamiento por sitio.

Al seleccionar un esquema de codificación de borrado que proporcione protección del sitio, equilibre la importancia relativa de los siguientes factores:

- **Número de fragmentos:** el rendimiento y la flexibilidad de expansión generalmente son 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 más alto.)
- **Tráfico de red:** Al recuperarse de fallas, se utiliza 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 mayores gastos generales requieren más espacio de almacenamiento por objeto.

Por ejemplo, al decidir entre un esquema 4+2 y un esquema 6+3 (ambos tienen una sobrecarga de almacenamiento del 50 %), seleccione el esquema 6+3 si se requiere tolerancia a fallas 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 utilizar, seleccione 4+2 o 6+3, o comuníquese con el soporte técnico.

Esquemas de codificación de borrado para grupos de almacenamiento de un solo sitio

Un grupo de almacenamiento de un solo sitio admite todos los esquemas de codificación de borrado definidos para tres o más sitios, siempre que el sitio tenga suficientes nodos de almacenamiento.

El número mínimo de nodos de almacenamiento requeridos es $k+m$, pero un grupo de almacenamiento con $k+m +1$ Se recomiendan nodos de almacenamiento. Por ejemplo, el esquema de codificación de borrado 2+1 requiere un grupo de almacenamiento con un mínimo de tres nodos de almacenamiento, pero se recomiendan cuatro nodos de almacenamiento.

Esquema de codificación de borrado ($k+m$)	Número mínimo de nodos de almacenamiento	Número recomendado de nodos de almacenamiento	Gastos generales de almacenamiento
4+2	6	7	50%
6+2	8	9	33%
8+2	10	11	25%
6+3	9	10	50%
9+3	12	13	33%
2+1	3	4	50%
4+1	5	6	25%
6+1	7	8	17%
7+5	12	13	71%

Ventajas, desventajas y requisitos de la codificación de borrado

Antes de decidir si utilizar la codificación de borrado o replicación para proteger los datos de los objetos contra pérdidas, debe comprender las ventajas, desventajas y los requisitos de la codificación de borrado.

Ventajas de la codificación de borrado

En comparación con la replicación, la codificación de borrado ofrece mayor confiabilidad, disponibilidad y

eficiencia de almacenamiento.

- **Confiabilidad:** La confiabilidad se mide en términos de tolerancia a fallas, es decir, la cantidad de fallas simultáneas que pueden mantenerse sin pérdida de datos. Con la replicación, se almacenan múltiples copias idénticas en diferentes nodos y en distintos sitios. Con la codificación de borrado, un objeto se codifica en fragmentos de datos y paridad y se distribuye entre muchos nodos y sitios. Esta dispersión proporciona protección contra fallas tanto del sitio como del nodo. En comparación con la replicación, la codificación de borrado proporciona una confiabilidad mejorada a costos 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 a costos de almacenamiento comparables.
- **Eficiencia de almacenamiento:** para niveles similares de disponibilidad y confiabilidad, los objetos protegidos mediante codificación de borrado consumen menos espacio en disco que los mismos objetos si estuvieran 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 tiene un código de borrado 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 objetos con código de borrado se calcula como el tamaño del objeto más la sobrecarga de almacenamiento. El porcentaje de sobrecarga de almacenamiento es la cantidad de fragmentos de paridad dividida por la cantidad de fragmentos de datos.

Desventajas de la codificación de borrado

En comparación con la replicación, la codificación de borrado tiene las siguientes desventajas:

- Se recomienda un mayor número de nodos y sitios de almacenamiento, según el esquema de codificación de borrado. Por el contrario, si replica datos de objetos, solo necesita un nodo de almacenamiento para cada copia. Ver ["Esquemas de codificación de borrado para grupos de almacenamiento que contienen tres o más sitios"](#) y ["Esquemas de codificación de borrado para grupos de almacenamiento de un solo sitio"](#).
- Aumento del coste y la complejidad de las ampliaciones de almacenamiento. Para expandir una implementación que utiliza replicación, agregue capacidad de almacenamiento en cada ubicación donde se realizan copias de objetos. Para expandir una implementación que utiliza codificación de borrado, debe considerar tanto el esquema de codificación de borrado en uso como qué tan llenos están los nodos de almacenamiento existentes. Por ejemplo, si espera hasta que los nodos existentes estén 100% llenos, debe agregar al menos $k+m$ Nodos de almacenamiento, pero si se expande cuando los nodos existentes están llenos al 70 %, puede agregar dos nodos por sitio y aún así maximizar la capacidad de almacenamiento utilizable. Para obtener más información, consulte ["Añadir capacidad de almacenamiento para objetos con código de borrado"](#).
- Hay mayores latencias de recuperación cuando se utiliza codificación de borrado en sitios distribuidos geográficamente. Los fragmentos de objeto de un objeto codificado para borrado y distribuido en sitios remotos tardan más en recuperarse a través de conexiones WAN que los de un objeto replicado y disponible localmente (el mismo sitio al que se conecta el cliente).
- Cuando se utiliza codificación de borrado en sitios distribuidos geográficamente, hay un mayor uso de tráfico de red WAN para recuperaciones y reparaciones, especialmente para objetos recuperados con frecuencia o para reparaciones de objetos a través de conexiones de red WAN.
- Cuando se utiliza codificación de borrado en varios sitios, el rendimiento máximo de objetos disminuye drásticamente a medida que aumenta la latencia de la red entre los sitios. Esta disminución se debe a la disminución correspondiente en el rendimiento de la red TCP, lo que afecta la rapidez con la que el sistema StorageGRID puede almacenar y recuperar fragmentos de objetos.

- Mayor uso de recursos computacionales.

Cuándo utilizar la codificación de borrado

La codificación de borrado es la más adecuada para los siguientes requisitos:

- Objetos de tamaño superior a 1 MB.



La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado.

- Almacenamiento a largo plazo o en frío para contenido que se recupera con poca frecuencia.
- Alta disponibilidad y confiabilidad de los datos.
- Protección contra fallas completas del sitio y del nodo.
- Eficiencia de almacenamiento.
- Implementaciones de un solo sitio que requieren una protección de datos eficiente con una única copia con código de borrado en lugar de múltiples copias replicadas.
- Implementaciones de múltiples sitios donde la latencia entre sitios es inferior a 100 ms.

Cómo se determina la retención de objetos

StorageGRID ofrece opciones para que los administradores de la red y los usuarios individuales especifiquen durante cuánto tiempo 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 la red.

Cómo los usuarios inquilinos controlan la retención de objetos

Los usuarios inquilinos pueden usar estos métodos para controlar cuánto tiempo se almacenan sus objetos en StorageGRID:

- Si la configuración global de Bloqueo de objetos S3 está habilitada para la red, los usuarios inquilinos de S3 pueden crear depósitos con el Bloqueo de objetos S3 habilitado y luego seleccionar un **Período de retención predeterminado** para cada depósito.
- Si la configuración global de Bloqueo de objetos S3 está habilitada para la red, los usuarios inquilinos de S3 pueden crear depósitos con Bloqueo de objetos S3 habilitado y luego usar la API REST de S3 para especificar configuraciones de retención hasta la fecha y retención legal para cada versión de objeto agregada a ese depósito.
 - Una versión de un objeto que se encuentra bajo retención legal no se puede eliminar mediante ningún método.
 - Antes de que se alcance la fecha de conservación de una versión de un objeto, esa versión no se puede eliminar mediante ningún método.
 - Los objetos en depósitos con el bloqueo de objetos S3 habilitado son retenidos por ILM "para siempre". Sin embargo, una vez alcanzada su fecha de retención, una versión de un objeto puede eliminarse mediante una solicitud del cliente o mediante la expiración del ciclo de vida del depósito. Ver ["Administrar objetos con S3 Object Lock"](#).
- Los usuarios inquilinos de S3 pueden agregar una configuración de ciclo de vida a sus depósitos que

especifique una acción de vencimiento. Si existe un ciclo de vida de depósito, StorageGRID almacena un objeto hasta que se cumpla la fecha o la cantidad de días especificados en la acción Vencimiento, a menos que el cliente elimine el objeto primero. Ver ["Crear la configuración del ciclo de vida de S3"](#).

- Un cliente S3 puede emitir una solicitud de eliminación de objeto. StorageGRID siempre prioriza las solicitudes de eliminación del cliente sobre el ciclo de vida del bucket S3 o ILM al determinar si eliminar o conservar un objeto.

Cómo los administradores de red controlan la retención de objetos

Los administradores de la red pueden utilizar estos métodos para controlar la retención de objetos:

- Establezca un período máximo de retención de bloqueo de objetos S3 para cada inquilino. Luego, los usuarios inquilinos pueden establecer un período de retención predeterminado para cada uno de sus depósitos. El período máximo de retención también se aplica a cualquier objeto recién ingerido para ese depósito (fecha de retención del objeto).
- Cree instrucciones de ubicación de ILM para controlar durante cuánto tiempo se almacenan los objetos. Cuando los objetos coinciden con una regla ILM, StorageGRID almacena esos objetos hasta que transcurra el último período de tiempo de la regla ILM. Los objetos se conservan indefinidamente si se especifica "para siempre" en las instrucciones de ubicación.
- Independientemente de quién controla cuánto tiempo se conservan los objetos, las configuraciones de ILM controlan qué tipos de copias de objetos (replicadas o codificadas por borrado) se almacenan y dónde se ubican las copias (nodos de almacenamiento o grupos de almacenamiento en la nube).

Cómo interactúan el ciclo de vida del bucket S3 y ILM

Cuando se configura un ciclo de vida de un bucket S3, las acciones de vencimiento del ciclo de vida anulan la política ILM para los objetos que coinciden con el filtro del ciclo de vida. Como resultado, un objeto podría permanecer en la cuadrícula incluso después de que hayan transcurrido las instrucciones ILM para colocar el objeto.

Ejemplos de retención de objetos

Para comprender mejor las interacciones entre S3 Object Lock, las configuraciones del ciclo de vida del bucket, las solicitudes de eliminación de clientes e ILM, considere los siguientes ejemplos.

Ejemplo 1: El ciclo de vida del depósito S3 conserva los objetos durante más tiempo que ILM

ILM

Almacenar dos copias durante 1 año (365 días)

Ciclo de vida del bucket

Los objetos expiran en 2 años (730 días)

Resultado

StorageGRID almacena el objeto durante 730 días. StorageGRID utiliza la configuración del ciclo de vida del depósito para determinar si se debe eliminar o conservar un objeto.



Si el ciclo de vida del depósito especifica que los objetos deben conservarse durante más tiempo del especificado por ILM, StorageGRID continúa usando las instrucciones de ubicación de ILM al determinar la cantidad y el tipo de copias a almacenar. En este ejemplo, se continuarán almacenando dos copias del objeto en StorageGRID desde el día 366 al 730.

Ejemplo 2: El ciclo de vida del depósito S3 hace que los objetos caduquen antes que ILM

ILM

Conservar dos copias durante 2 años (730 días)

Ciclo de vida del bucket

Los objetos expiran en 1 año (365 días)

Resultado

StorageGRID elimina ambas copias del objeto después del día 365.

Ejemplo 3: La eliminación del cliente anula el ciclo de vida del depósito y el ILM

ILM

Almacenar dos copias en nodos de almacenamiento "para siempre"

Ciclo de vida del bucket

Los objetos expiran 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 S3

La fecha de conservación hasta para una versión de objeto es 2026-03-31. No está en vigor ninguna retención legal.

Regla ILM compatible

Almacenar dos copias en nodos de almacenamiento "para siempre"

Solicitud de eliminación de cliente

Emitido el 31/03/2024

Resultado

StorageGRID no eliminará la versión del objeto porque la fecha de conservación aún está a 2 años de distancia.

Cómo se eliminan los objetos

StorageGRID puede eliminar objetos ya sea en respuesta directa a una solicitud del cliente o automáticamente como resultado de la expiración del ciclo de vida de un bucket S3 o los requisitos de la política ILM. Comprender las diferentes formas en que se pueden eliminar objetos y cómo StorageGRID maneja las solicitudes de eliminación puede ayudarlo a administrar objetos de manera más efectiva.

StorageGRID puede utilizar uno de dos métodos para eliminar objetos:

- Eliminación sincrónica: cuando StorageGRID recibe una solicitud de eliminación de cliente, todas las copias de objetos se eliminan inmediatamente. Después de eliminar las copias se informa al cliente que la eliminación se realizó correctamente.
- Los objetos se ponen en cola para su eliminación: cuando StorageGRID recibe una solicitud de eliminación, el objeto se pone en cola para su eliminación y se informa inmediatamente al cliente que la eliminación se realizó correctamente. Las copias de objetos se eliminan más tarde mediante el procesamiento ILM en segundo plano.

Al eliminar objetos, StorageGRID utiliza el método que optimiza el rendimiento de la eliminación, minimiza los posibles retrasos en la eliminación y libera espacio más rápidamente.

La tabla resume cuándo StorageGRID utiliza cada método.

Método para realizar la eliminación	Cuando se utiliza
Los objetos se ponen en cola para su eliminación	Cuando cualquiera de las siguientes condiciones sea verdadera: • La eliminación automática de objetos se ha activado por uno de los siguientes eventos: ◦ Se alcanza la fecha de vencimiento o el número de días en la configuración del ciclo de vida de un bucket S3. ◦ Transcurre el último período de tiempo especificado en una regla ILM. Nota: Los objetos en un bucket que tiene habilitado el Bloqueo de objetos S3 no se pueden eliminar si están bajo una retención legal o si se ha especificado una fecha de retención pero aún no se cumple. • Un cliente S3 solicita la eliminación y una o más de estas condiciones son verdaderas: ◦ Las copias no se pueden eliminar en 30 segundos porque, por ejemplo, la ubicación de un objeto no está disponible temporalmente. ◦ Las colas de eliminación en segundo plano están inactivas.
Los objetos se eliminan inmediatamente (eliminación sincrónica)	Cuando un cliente S3 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 para procesar.

Cuando los clientes S3 realizan solicitudes de eliminación, StorageGRID comienza agregando objetos a la cola de eliminación. Luego pasa a realizar la eliminación sincrónica. Asegurarse de que la cola de eliminación en segundo plano tenga objetos para procesar permite que StorageGRID procese las eliminaciones de manera más eficiente, especialmente para clientes de baja concurrencia, al mismo tiempo que ayuda a prevenir retrasos en la eliminación de clientes.

Tiempo necesario para eliminar objetos

La forma en que StorageGRID elimina objetos puede afectar el funcionamiento aparente del sistema:

- Cuando StorageGRID realiza una eliminación sincrónica, puede tardar hasta 30 segundos en devolver un

resultado al cliente. Esto significa que puede parecer que la eliminación ocurre más lentamente, aunque en realidad las copias se eliminan más rápido que cuando StorageGRID pone en cola los objetos para su eliminación.

- Si supervisa de cerca el rendimiento de eliminación durante una eliminación masiva, es posible que observe que la tasa de eliminación parece ser lenta después de que se haya eliminado una cierta cantidad de objetos. Este cambio se produce cuando StorageGRID pasa de poner en cola objetos para su eliminación a realizar una eliminación sincrónica. La aparente reducción en la tasa de eliminación no significa que las copias de objetos se estén eliminando más lentamente. Por el contrario, indica que, en promedio, ahora se está liberando espacio más rápidamente.

Si está eliminando una gran cantidad de objetos y su prioridad es liberar espacio rápidamente, considere usar una solicitud de cliente para eliminar objetos en lugar de eliminarlos mediante ILM u otros métodos. En general, el espacio se libera más rápidamente cuando la eliminación la realizan los clientes porque StorageGRID puede usar la eliminación sincrónica.

La cantidad de tiempo necesaria para liberar espacio después de eliminar un objeto depende de varios factores:

- Si las copias de objetos se eliminan de forma sincrónica o se ponen en cola para su eliminación más tarde (para solicitudes de eliminación del cliente).
- Otros factores, como la cantidad de objetos en la red o la disponibilidad de recursos de la red cuando las copias de objetos se ponen en cola para su eliminación (tanto para eliminaciones de cliente como para otros métodos).

Cómo se eliminan los objetos versionados de S3

Cuando el control de versiones está habilitado para un bucket S3, StorageGRID sigue el comportamiento de Amazon S3 al responder a solicitudes de eliminación, ya sea que dichas solicitudes provengan de un cliente S3, la expiración del ciclo de vida de un bucket S3 o los requisitos de la política ILM.

Cuando los objetos están versionados, las solicitudes de eliminación de objetos no eliminan la versión actual del objeto y no liberan espacio. En cambio, una solicitud de eliminación de objeto crea un marcador de eliminación de cero bytes como la versión actual del objeto, lo que hace que la versión anterior del objeto sea "no actual". Un marcador de eliminación de objeto se convierte en un marcador de eliminación de objeto vencido cuando es la versión actual y no hay versiones no actuales.

Incluso aunque el objeto no se haya eliminado, StorageGRID se comporta como si la versión actual del objeto ya no estuviera disponible. Las solicitudes a ese objeto devuelven 404 Not Found. Sin embargo, debido a que no se han eliminado los datos del objeto no actual, las solicitudes que especifican una versión no actual del objeto pueden tener éxito.

Para liberar espacio al eliminar objetos versionados o para quitar marcadores de eliminación, utilice una de las siguientes opciones:

- **Solicitud de cliente S3:** especifique el ID de la versión del objeto en la solicitud S3 DELETE `Object(DELETE /object?versionId=ID )`. Tenga en cuenta que esta solicitud solo elimina copias de objetos de la versión especificada (las otras versiones aún ocupan espacio).
- **Ciclo de vida del bucket:** utilice el `NoncurrentVersionExpiration` acción en la configuración del ciclo de vida del bucket. Cuando se alcanza la cantidad de `NoncurrentDays` especificada, StorageGRID elimina de forma permanente todas las copias de versiones de objetos no actuales. Estas versiones de objetos no se pueden recuperar.

El `NewerNoncurrentVersions` La acción en la configuración del ciclo de vida del bucket especifica la cantidad de versiones no actuales que se conservan en un bucket S3 versionado. Si hay más versiones

no actuales que `NewerNoncurrentVersions` especifica que StorageGRID elimina las versiones anteriores cuando ha transcurrido el valor `NoncurrentDays`. El `NewerNoncurrentVersions` El umbral anula las reglas del ciclo de vida proporcionadas por ILM, lo que significa que un objeto no actual con una versión dentro del `NewerNoncurrentVersions` El umbral se mantiene si ILM solicita su eliminación.

Para eliminar los marcadores de eliminación de objetos caducados, utilice el `Expiration` acción con una de las siguientes etiquetas: `ExpiredObjectDeleteMarker`, `Days`, o `Date`.

- **ILM:** "Clonar una política activa" y agregue dos reglas ILM a la nueva política:
 - Primera regla: utilice "Tiempo no actual" como tiempo de referencia para que coincida con las versiones no actuales del objeto. En "Paso 1 (Ingresar detalles) del asistente para crear una regla de ILM", seleccione **Sí** para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en depósitos S3 con control de versiones habilitado)?"
 - Segunda regla: utiliza **Tiempo de ingesta** para que coincida con la versión actual. La regla "Hora no actual" debe aparecer en la política encima de la regla **Hora de ingestión**.

Para eliminar marcadores de eliminación de objetos vencidos, utilice una regla de **Tiempo de ingesta** para que coincida con los marcadores de eliminación actuales. Los marcadores de eliminación solo se eliminan cuando ha transcurrido un **Periodo de tiempo de Días** y el creador de eliminación actual ha expirado (no hay versiones no actuales).

- **Eliminar objetos en el depósito:** utilice el administrador de inquilinos para "eliminar todas las versiones de los objetos", incluidos los marcadores de eliminación, de un depósito.

Cuando se elimina un objeto versionado, StorageGRID crea un marcador de eliminación de cero bytes como la versión actual del objeto. Todos los objetos y marcadores de eliminación deben eliminarse antes de poder eliminar un depósito versionado.

- Los marcadores de eliminación creados en StorageGRID 11.7 o versiones anteriores solo se pueden eliminar mediante solicitudes de cliente S3, no se eliminan mediante ILM, reglas de ciclo de vida del bucket ni mediante la eliminación de objetos en operaciones de bucket.
- Los marcadores de eliminación de un depósito creado en StorageGRID 11.8 o posterior se pueden quitar mediante ILM, reglas de ciclo de vida del depósito, operaciones de eliminación de objetos en el depósito o una eliminación explícita del cliente S3.

Información relacionada

- "Utilice la API REST de S3"
- "Ejemplo 4: Reglas y políticas de ILM para objetos versionados de S3"

Crear y asignar grados de almacenamiento

Los grados de almacenamiento identifican el tipo de almacenamiento utilizado por un nodo de almacenamiento. Puede crear grados de almacenamiento si desea que las reglas ILM coloquen determinados objetos en determinados nodos de almacenamiento.

Antes de empezar

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

Acerca de esta tarea

Cuando instala StorageGRID por primera vez, el grado de almacenamiento **Predeterminado** se asigna

automáticamente a cada nodo de almacenamiento en su sistema. Según sea necesario, puede definir opcionalmente grados de almacenamiento personalizados y asignarlos a diferentes nodos de almacenamiento.

El uso de grados de almacenamiento personalizados le permite crear grupos de almacenamiento ILM que contienen solo un tipo específico de nodo de almacenamiento. Por ejemplo, es posible que desee que determinados objetos se almacenen en sus nodos de almacenamiento más rápidos, como los dispositivos de almacenamiento totalmente flash StorageGRID .



Los nodos de almacenamiento se pueden configurar durante la instalación para que contengan solo metadatos de objetos y no datos de objetos. A los nodos de almacenamiento de solo metadatos no se les puede asignar un grado de almacenamiento. Para obtener más información, consulte "[Tipos de nodos de almacenamiento](#)".

Si el grado de almacenamiento no es una preocupación (por ejemplo, todos los nodos de almacenamiento son idénticos), puede omitir este procedimiento y usar la selección **incluye todos los grados de almacenamiento** para el grado de almacenamiento cuando "[crear grupos de almacenamiento](#)". El uso de esta selección garantiza que el grupo de almacenamiento incluirá todos los nodos de almacenamiento del sitio, independientemente de su grado de almacenamiento.



No cree más niveles de almacenamiento de los necesarios. 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. Los grados de almacenamiento asignados a un solo nodo pueden provocar retrasos en ILM si ese nodo deja de estar disponible.

Pasos

1. Seleccione **ILM > Grados de almacenamiento**.
2. Definir grados de almacenamiento personalizados:
 - a. Para cada grado de almacenamiento personalizado que desee agregar, seleccione *Insertar*  para agregar una fila.
 - b. Introduzca una etiqueta descriptiva.



Storage Grades

Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	disk	

Storage Grades

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes

c. Seleccione **Aplicar cambios**.

d. Opcionalmente, si necesita modificar una etiqueta guardada, seleccione **Editar*** y seleccione ***Aplicar cambios**.



No se pueden eliminar los niveles de almacenamiento.

3. Asignar nuevos grados de almacenamiento a los nodos de almacenamiento:

a. Localice el nodo de almacenamiento en la lista LDR y seleccione su ícono ***Editar*** .

b. Seleccione el grado de almacenamiento apropiado de la lista.



LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default disk	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes



Asignar un grado de almacenamiento a un nodo de almacenamiento determinado solo una vez. Un nodo de almacenamiento recuperado de una falla mantiene el grado de almacenamiento asignado previamente. No cambie esta asignación después de que se active la política ILM. Si se cambia la asignación, los datos se almacenan según el nuevo grado de almacenamiento.

- Seleccione **Aplicar cambios**.

Utilice grupos de almacenamiento

¿Qué es un pool de almacenamiento?

Un grupo de almacenamiento es una agrupación lógica de nodos de almacenamiento.

Cuando instala StorageGRID, se crea automáticamente un grupo de almacenamiento por sitio. Puede configurar grupos de almacenamiento adicionales según sea necesario para sus requisitos de almacenamiento.



Los nodos de almacenamiento se pueden configurar durante la instalación para contener datos de objetos y metadatos de objetos, o solo metadatos de objetos. Los nodos de almacenamiento de solo metadatos no se pueden usar en grupos de almacenamiento. Para obtener más información, consulte "[Tipos de nodos de almacenamiento](#)".

Los grupos de almacenamiento tienen dos atributos:

- **Grado de almacenamiento:** para los nodos de almacenamiento, el rendimiento relativo del almacenamiento de respaldo.
- **Sitio:** El centro de datos donde se almacenarán los objetos.

Los grupos de almacenamiento se utilizan en las reglas ILM para determinar dónde se almacenan los datos de los objetos y el tipo de almacenamiento utilizado. Cuando configura las reglas de ILM para la replicación, selecciona uno o más grupos de almacenamiento.

Pautas para la creación de grupos de almacenamiento

Configure y utilice grupos de almacenamiento para protegerse contra la pérdida de datos mediante la distribución de datos en varios sitios. Las copias replicadas y las copias con código de borrado requieren diferentes configuraciones de grupo de almacenamiento.

Ver ["Ejemplos de habilitación de la protección contra pérdida de sitios mediante codificación de replicación y borrado"](#).

Directrices para todos los grupos de almacenamiento

- Mantenga las configuraciones del grupo de almacenamiento lo más simples posible. No cree más grupos de almacenamiento de los necesarios.
- Cree grupos de almacenamiento con tantos nodos como sea posible. Cada grupo de almacenamiento debe contener dos o más nodos. Un grupo de almacenamiento con nodos insuficientes puede provocar retrasos en ILM si un nodo deja de estar disponible.
- Evite crear o utilizar grupos de almacenamiento que se superpongan (que contengan uno o más de los mismos nodos). Si los grupos de almacenamiento se superponen, es posible que se guarden más de una copia de datos de objetos en el mismo nodo.
- En general, no utilice el grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores) ni el sitio Todos los sitios. Estos elementos se actualizan automáticamente para incluir cualquier sitio nuevo que agregue en una expansión, lo que podría no ser el comportamiento deseado.

Directrices para los grupos de almacenamiento utilizados para copias replicadas

- Para la protección contra pérdida de sitios utilizando ["replicación"](#), especifique uno o más grupos de almacenamiento específicos del sitio en el ["Instrucciones de colocación para cada regla ILM"](#).

Durante la instalación de StorageGRID se crea automáticamente un grupo de almacenamiento para cada sitio.

El uso de un grupo de almacenamiento para cada sitio garantiza que las copias de objetos replicados se coloquen exactamente donde usted espera (por ejemplo, una copia de cada objeto en cada sitio para protección contra pérdida del sitio).

- Si agrega un sitio en una expansión, cree un nuevo grupo de almacenamiento que contenga solo el nuevo sitio. Entonces, ["actualizar las reglas de ILM"](#) para controlar qué objetos se almacenan en el nuevo sitio.
- Si la cantidad de copias es menor que la cantidad de grupos de almacenamiento, el sistema distribuye las copias para equilibrar el uso del disco entre los grupos.
- Si los grupos de almacenamiento se superponen (contienen los mismos nodos de almacenamiento), todas las copias del objeto podrían guardarse en un solo sitio. Debe asegurarse de que los grupos de almacenamiento seleccionados no contengan los mismos nodos de almacenamiento.

Directrices para los grupos de almacenamiento utilizados para copias con código de borrado

- Para la protección contra pérdida de sitios utilizando ["codificación de borrado"](#), cree grupos de almacenamiento que consten de al menos tres sitios. Si un grupo de almacenamiento incluye solo dos sitios, no podrá utilizar ese grupo de almacenamiento para la codificación de borrado. No hay esquemas de codificación de borrado disponibles para un grupo de almacenamiento que tiene dos sitios.
- La cantidad de nodos de almacenamiento y sitios contenidos en el grupo de almacenamiento determinan qué ["esquemas de codificación de borrado"](#) están disponibles.

- Si es posible, un grupo de almacenamiento debe incluir más que 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 tener al menos nueve nodos de almacenamiento. Sin embargo, se recomienda tener al menos un nodo de almacenamiento adicional por sitio.
- Distribuya los nodos de almacenamiento en los sitios de la manera más uniforme posible. Por ejemplo, para admitir un esquema de codificación de borrado 6+3, configure un grupo de almacenamiento que incluya al menos tres nodos de almacenamiento en tres sitios.
- Si tiene requisitos de alto rendimiento, no se recomienda utilizar un grupo de almacenamiento que incluya varios sitios si la latencia de red entre 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 drásticamente debido a la disminución del rendimiento de la red TCP.

La disminución del rendimiento afecta las tasas máximas alcanzables de ingesta y recuperación de objetos (cuando se selecciona Equilibrado o Estricto como comportamiento de ingesta) o podría generar retrasos en la cola de ILM (cuando se selecciona Confirmación dual como comportamiento de ingesta). Ver "[Comportamiento de ingesta de reglas ILM](#)".



Si su red incluye solo un sitio, no podrá utilizar el grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores) ni el sitio Todos los sitios en un perfil de codificación de borrado. Este comportamiento evita que el perfil se vuelva inválido si se agrega un segundo sitio.

Habilitar la protección contra pérdida de sitios

Si su implementación de StorageGRID incluye más de un sitio, puede usar codificación de replicación y borrado con grupos de almacenamiento configurados adecuadamente para habilitar la protección contra pérdida de sitios.

La codificación de replicación y borrado requiere diferentes configuraciones de grupo de almacenamiento:

- Para utilizar la replicación para la protección contra pérdida del sitio, utilice los grupos de almacenamiento específicos del sitio que se crean automáticamente durante la instalación de StorageGRID. Luego crea reglas ILM con "[instrucciones de colocación](#)" que especifican múltiples grupos de almacenamiento para que se coloque una copia de cada objeto en cada sitio.
- Para utilizar la codificación de borrado para la protección contra pérdida del sitio, "[crear grupos de almacenamiento que consten de varios sitios](#)". Luego, cree reglas ILM que utilicen un grupo de almacenamiento compuesto por varios sitios y cualquier esquema de codificación de borrado disponible.



Al configurar su implementación de StorageGRID para la protección contra pérdida de sitios, también debe tener en cuenta los efectos de "[opciones de ingesta](#)" y "[consistencia](#)".

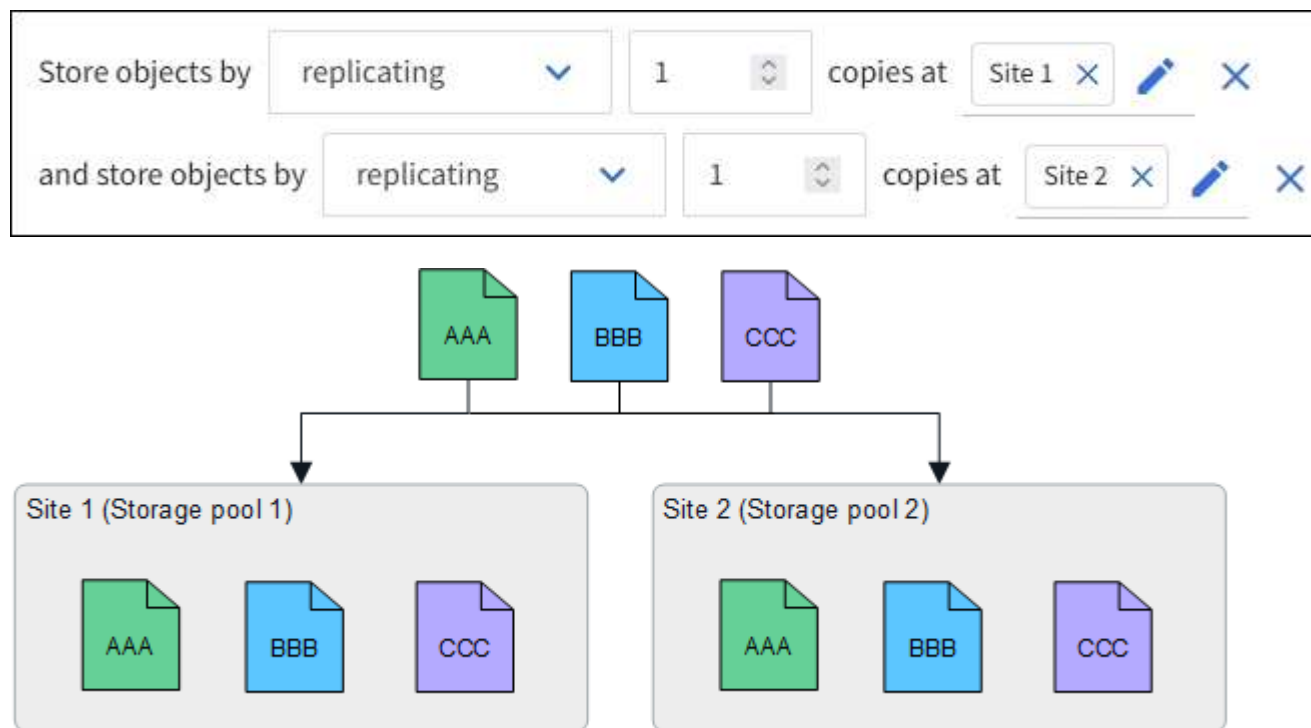
Ejemplo de replicación

De forma predeterminada, se crea un grupo de almacenamiento para cada sitio durante la instalación de StorageGRID. Tener grupos de almacenamiento que constan de un solo sitio le permite configurar reglas ILM que utilizan la replicación para la protección contra pérdida del sitio. En este ejemplo:

- El grupo de almacenamiento 1 contiene el Sitio 1
- El grupo de almacenamiento 2 contiene el Sitio 2
- La regla ILM contiene dos colocaciones:

- Almacenar objetos replicando 1 copia en el Sitio 1
- Almacenar objetos replicando 1 copia en el Sitio 2

Ubicación de las reglas de ILM:



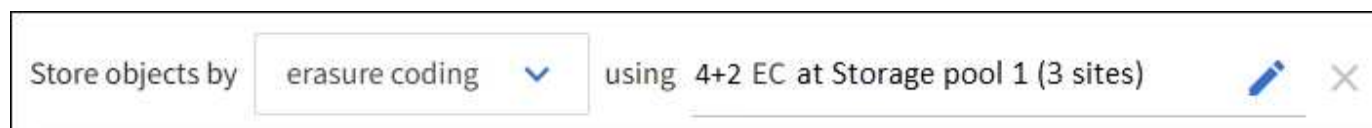
Si se pierde un sitio, hay copias de los objetos disponibles en el otro sitio.

Ejemplo de codificación de borrado

Tener grupos de almacenamiento que constan de más de un sitio por grupo de almacenamiento le permite configurar reglas ILM que utilizan codificación de borrado para la protección contra pérdida de sitios. En este ejemplo:

- El grupo de almacenamiento 1 contiene los sitios 1 a 3
- La regla ILM contiene una ubicación: almacenar objetos mediante codificación de borrado utilizando un esquema EC 4+2 en el grupo de almacenamiento 1, que contiene tres sitios

Ubicación de las reglas de ILM:



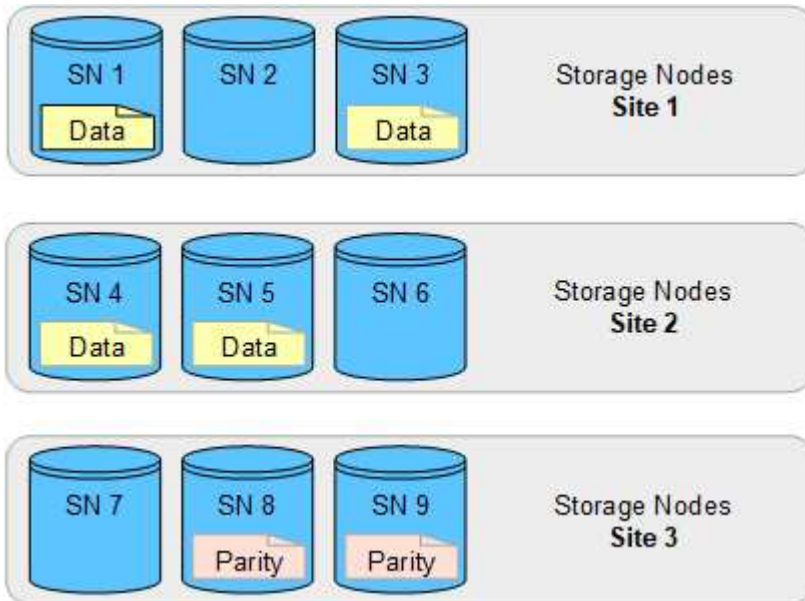
En este ejemplo:

- La regla ILM utiliza un esquema de codificación de borrado 4+2.
- Cada objeto se divide en cuatro fragmentos de datos iguales y se calculan dos fragmentos de paridad a partir de los datos del objeto.
- Cada uno de los seis fragmentos se almacena en un nodo diferente en tres sitios de centros de datos para brindar protección de datos ante fallas de nodos o pérdidas de sitios.

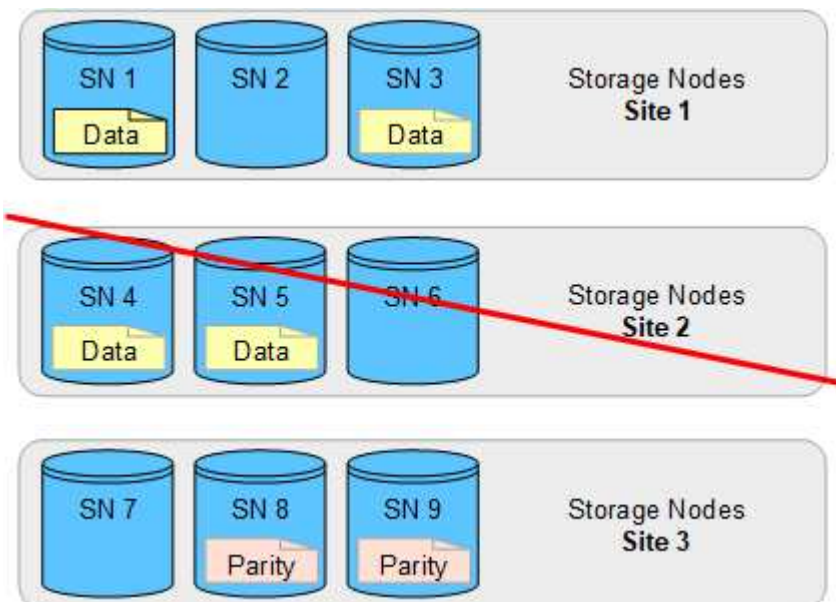


Se permite la codificación de borrado en grupos de almacenamiento que contengan cualquier cantidad de sitios *excepto* dos sitios.

Regla ILM que utiliza el esquema de codificación de borrado 4+2:



Si se pierde un sitio, aún se pueden recuperar los datos:



Crear un grupo de almacenamiento

Crea grupos de almacenamiento para determinar dónde el sistema StorageGRID almacena los datos de los objetos y el tipo de almacenamiento utilizado. Cada grupo de almacenamiento incluye uno o más sitios y uno o más grados de almacenamiento.



Cuando instala StorageGRID 11.9 en una nueva red, se crean automáticamente grupos de almacenamiento para cada sitio. Sin embargo, si instaló inicialmente StorageGRID 11.6 o una versión anterior, los grupos de almacenamiento no se crean automáticamente para cada sitio.

Si desea crear grupos de almacenamiento en la nube para almacenar datos de objetos fuera de su sistema StorageGRID , consulte la ["Información sobre el uso de grupos de almacenamiento en la nube"](#) .

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Ha revisado las pautas para crear grupos de almacenamiento.

Acerca de esta tarea

Los grupos de almacenamiento determinan dónde se almacenan los datos de los objetos. La cantidad de grupos de almacenamiento que necesita depende de la cantidad de sitios en su red y de los tipos de copias que desea: replicadas o con código de borrado.

- Para la replicación y la codificación de borrado de un solo sitio, cree un grupo de almacenamiento para cada sitio. Por ejemplo, si desea almacenar copias de objetos replicados en tres sitios, cree tres grupos de almacenamiento.
- Para la codificación de borrado en tres o más sitios, cree un grupo de almacenamiento que incluya una entrada para cada sitio. Por ejemplo, si desea borrar objetos de código en tres sitios, cree un grupo de almacenamiento.



No incluya el sitio Todos los sitios en un grupo de almacenamiento que se utilizará en un perfil de codificación de borrado. En su lugar, agregue una entrada separada al grupo de almacenamiento para cada sitio que almacenará datos codificados con borrado. Ver [este paso](#) por ejemplo.

- Si tiene más de un grado de almacenamiento, no cree un grupo de almacenamiento que incluya diferentes grados de almacenamiento en un solo sitio. Ver el ["Pautas para la creación de grupos de almacenamiento"](#) .

Pasos

1. Seleccione **ILM > Grupos de almacenamiento**.

La pestaña Grupos de almacenamiento enumera todos los grupos de almacenamiento definidos.



Para las nuevas instalaciones de StorageGRID 11.6 o anteriores, el grupo de almacenamiento Todos los nodos de almacenamiento se actualiza automáticamente cada vez que agrega nuevos sitios de centros de datos. No utilice este grupo en las reglas de ILM.

2. Para crear un nuevo grupo de almacenamiento, seleccione **Crear**.
3. Introduzca un nombre único para el grupo de almacenamiento. Utilice un nombre que sea fácil de identificar cuando configure perfiles de codificación de borrado y reglas ILM.
4. En la lista desplegable **Sitio**, seleccione un sitio para este grupo de almacenamiento.

Cuando selecciona un sitio, la cantidad de nodos de almacenamiento en la tabla se actualiza automáticamente.

En general, no utilice el sitio Todos los sitios en ningún grupo de almacenamiento. Las reglas ILM que utilizan un grupo de almacenamiento de todos los sitios colocan los objetos en cualquier sitio disponible, lo que le brinda menos control sobre la ubicación de los objetos. Además, un grupo de almacenamiento de todos los sitios utiliza los nodos de almacenamiento en un nuevo sitio de inmediato, 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 ILM usa este grupo de almacenamiento.

El grado de almacenamiento, *incluye todos los grados de almacenamiento*, incluye todos los nodos de almacenamiento en el sitio seleccionado. Si creó grados de almacenamiento adicionales para los nodos de almacenamiento en su cuadrícula, aparecerán en el menú desplegable.

6. Si desea utilizar el grupo de almacenamiento en un perfil de codificación de borrado de varios sitios, seleccione **Agregar más nodos** para agregar una entrada para cada sitio al grupo de almacenamiento.



Se le advertirá si agrega más de una entrada con diferentes grados de almacenamiento para un sitio.

Para eliminar una entrada, seleccione el icono de eliminar .

7. Cuando esté satisfecho con sus selecciones, seleccione **Guardar**.

El nuevo grupo de almacenamiento se agrega a la lista.

Ver detalles del grupo de almacenamiento

Puede ver los detalles de un grupo de almacenamiento para determinar dónde se utiliza y ver qué nodos y grados de almacenamiento están incluidos.

Antes de empezar

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

Pasos

1. Seleccione **ILM > Grupos de almacenamiento**.

La tabla de grupos de almacenamiento incluye la siguiente información para cada grupo de almacenamiento que incluye nodos de almacenamiento:

- **Nombre:** el nombre para mostrar único del grupo de almacenamiento.
- **Recuento de nodos:** la cantidad de nodos en el grupo de almacenamiento.
- **Uso de almacenamiento:** el porcentaje del espacio utilizable total que se ha utilizado para datos de objetos en este nodo. Este valor no incluye metadatos del objeto.
- **Capacidad total:** el tamaño del grupo de almacenamiento, que equivale a la cantidad total de espacio utilizable para datos de objetos para todos los nodos del grupo de almacenamiento.
- **Uso de ILM:** cómo se utiliza actualmente el grupo de almacenamiento. Es posible que un grupo de almacenamiento no se utilice o que se utilice en una o más reglas ILM, perfiles de codificación de borrado o ambos.

2. Para ver los detalles de un grupo de almacenamiento específico, seleccione su nombre.

Aparece la página de detalles del grupo de almacenamiento.

3. Consulte la pestaña **Nodos** para obtener información sobre los nodos de almacenamiento incluidos en el grupo de almacenamiento.

La tabla incluye la siguiente información para cada nodo:

- Nombre del nodo
- Nombre del sitio
- Grado de almacenamiento
- Uso de almacenamiento: el porcentaje del espacio total utilizable para los datos de objetos que se ha utilizado para el nodo de almacenamiento.



El mismo valor de uso de almacenamiento (%) también se muestra en el gráfico Almacenamiento utilizado - Datos de objeto para cada nodo de almacenamiento (seleccione **NODOS** > **Nodo de almacenamiento** > **Almacenamiento**).

4. Vea la pestaña **Uso de ILM** para determinar si el grupo de almacenamiento se está utilizando actualmente en alguna regla de ILM o perfil de codificación de borrado.
5. Opcionalmente, vaya a la **página de reglas de ILM** para conocer y administrar las reglas que utilizan el grupo de almacenamiento.

Ver el "[Instrucciones para trabajar con reglas ILM](#)".

Editar grupo de almacenamiento

Puede editar un grupo de almacenamiento para cambiar su nombre o actualizar sitios y grados de almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tienes "[permisos de acceso específicos](#)".
- Usted ha revisado el "[Pautas para la creación de grupos de almacenamiento](#)".
- Si planea editar un grupo de almacenamiento que se utiliza en una regla de la política ILM activa, debe considerar cómo sus cambios afectarán la ubicación de los datos de los objetos.

Acerca de esta tarea

Si está agregando un nuevo sitio o grado de almacenamiento a un grupo de almacenamiento que se utiliza en la política ILM activa, tenga en cuenta que los nodos de almacenamiento en el nuevo sitio o grado de almacenamiento no se utilizarán automáticamente. Para forzar a StorageGRID a usar un nuevo sitio o grado de almacenamiento, debe activar una nueva política ILM después de guardar el grupo de almacenamiento editado.

Pasos

1. Seleccione **ILM** > **Grupos de almacenamiento**.
2. Seleccione la casilla de verificación del grupo de almacenamiento que desea editar.

No se puede editar el grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores).

3. Seleccione **Editar**.
4. Según sea necesario, cambie el nombre del grupo de almacenamiento.
5. Según sea necesario, seleccione otros sitios y grados de almacenamiento.

No se le permite cambiar el sitio o el grado de almacenamiento si el grupo de almacenamiento se utiliza en un perfil de codificación de borrado y el cambio provocaría que el esquema de codificación de borrado se vuelva inválido. Por ejemplo, si un grupo de almacenamiento utilizado en un perfil de codificación de borrado actualmente incluye un grado de almacenamiento con un solo sitio, no podrá utilizar un grado de almacenamiento con dos sitios porque el cambio haría que el esquema de codificación de borrado no sea válido.



Agregar o eliminar sitios de un grupo de almacenamiento existente no moverá ningún dato codificado de borrado existente. Si desea mover los datos existentes del sitio, debe crear un nuevo grupo de almacenamiento y un perfil EC para volver a codificar los datos.

6. Seleccione **Guardar**.

Después de terminar

Si agregó un nuevo sitio o grado de almacenamiento a un grupo de almacenamiento utilizado en la política ILM activa, active una nueva política ILM para forzar a StorageGRID a usar el nuevo sitio o grado de almacenamiento. Por ejemplo, clone su política ILM existente y luego active el clon. Ver ["Trabajar con las reglas y políticas de ILM"](#).

Eliminar un grupo de almacenamiento

Puedes eliminar un grupo de almacenamiento que no esté en uso.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["permisos de acceso necesarios"](#).

Pasos

1. Seleccione **ILM > Grupos de almacenamiento**.
2. Mire la columna de uso de ILM en la tabla para determinar si puede eliminar el grupo de almacenamiento.

No se puede eliminar un grupo de almacenamiento si se está utilizando en una regla ILM o en un perfil de codificación de borrado. Según sea necesario, seleccione **nombre del grupo de almacenamiento > uso de ILM** para determinar dónde se utiliza el grupo de almacenamiento.

3. Si el grupo de almacenamiento que desea eliminar no está en uso, seleccione la casilla de verificación.
4. Seleccione **Eliminar**.
5. Seleccione **Aceptar**.

Utilice grupos de almacenamiento en la nube

¿Qué es un pool de almacenamiento en la nube?

Un grupo de almacenamiento en la nube le permite usar ILM para mover datos de objetos fuera de su sistema StorageGRID. Por ejemplo, es posible que desee mover objetos a los que se accede con poca frecuencia a un almacenamiento en la nube de menor costo, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o el nivel de acceso de archivo en el almacenamiento de blobs de Microsoft Azure. O bien, es posible que desee mantener una copia de seguridad en la nube de los objetos

StorageGRID para mejorar la recuperación ante desastres.

Desde una perspectiva ILM, un grupo de almacenamiento en la nube es similar a un grupo de almacenamiento. Para almacenar objetos en cualquiera de las ubicaciones, seleccione el grupo al crear las instrucciones de ubicación para una regla ILM. Sin embargo, mientras que los grupos de almacenamiento constan de nodos de almacenamiento dentro del sistema StorageGRID, un grupo de almacenamiento en la nube consta de un depósito externo (S3) o contenedor (almacenamiento de blobs de Azure).

La tabla compara los grupos de almacenamiento con los grupos de almacenamiento en la nube y muestra las similitudes y diferencias de alto nivel.

	Pool de almacenamiento	Grupo de almacenamiento en la nube
¿Cómo se crea?	Usando la opción ILM > Grupos de almacenamiento en el Administrador de Grid.	Usando la opción ILM > Grupos de almacenamiento > Grupos de almacenamiento en la nube en Grid Manager. Debe configurar el contenedor o depósito externo antes de poder crear el grupo de almacenamiento en la nube.
¿Cuántos pools puedes crear?	Ilimitado.	Hasta 10.
¿Dónde se almacenan los objetos?	En uno o más nodos de almacenamiento dentro de StorageGRID.	En un bucket de Amazon S3, un contenedor de almacenamiento de blobs de Azure o un Google Cloud externo al sistema StorageGRID. Si el grupo de almacenamiento en la nube es un bucket de Amazon S3: • Opcionalmente, puede configurar un ciclo de vida de depósito para trasladar objetos a un almacenamiento a largo plazo y de bajo costo, como Amazon S3 Glacier o S3 Glacier Deep Archive. El sistema de almacenamiento externo debe ser compatible con la clase de almacenamiento Glacier y la API S3 RestoreObject. • Puede crear grupos de almacenamiento en la nube para usar con AWS Commercial Cloud Services (C2S), que admite la región secreta de AWS. Si el grupo de almacenamiento en la nube es un contenedor de almacenamiento de blobs de Azure, StorageGRID traslada el objeto al nivel de archivo. Nota: En general, no configure la administración del ciclo de vida del almacenamiento de blobs de Azure para el contenedor utilizado para un grupo de almacenamiento en la nube. Las operaciones de restauración de objetos en el grupo de almacenamiento en la nube pueden verse afectadas por el ciclo de vida configurado.

	Pool de almacenamiento	Grupo de almacenamiento en la nube
¿Qué controla la ubicación de los objetos?	Una regla ILM en las políticas ILM activas.	Una regla ILM en las políticas ILM activas.
¿Qué método de protección de datos se utiliza?	Codificación de replicación o borrado.	Replicación.
¿Cuántas copias de cada objeto están permitidas?	Múltiple.	Una copia en el grupo de almacenamiento en la nube y, opcionalmente, una o más copias en StorageGRID. Nota: No es posible almacenar un objeto en más de un grupo de almacenamiento en la nube al mismo tiempo.
¿Cuales son las ventajas?	Los objetos son accesibles rápidamente en cualquier momento.	Almacenamiento de bajo coste. Nota: Los datos de FabricPool no se pueden agrupar en grupos de almacenamiento en la nube.

Ciclo de vida de un objeto de grupo de almacenamiento en la nube

Antes de implementar grupos de almacenamiento en la nube, revise el ciclo de vida de los objetos que se almacenan en cada tipo de grupo de almacenamiento en la nube.

S3: Ciclo de vida de un objeto de grupo de almacenamiento en la nube

Los pasos describen las etapas del ciclo de vida de un objeto almacenado en un grupo de almacenamiento en la nube S3.



"Glacier" se refiere tanto a la clase de almacenamiento Glacier como a la clase de almacenamiento Glacier Deep Archive, con una excepción: la clase de almacenamiento Glacier Deep Archive no admite el nivel de restauración acelerada. Solo se admite la recuperación masiva o estándar.



Google Cloud Platform (GCP) admite la recuperación de objetos del almacenamiento a largo plazo sin necesidad de una operación de restauración POST.

1. Objeto almacenado en StorageGRID

Para iniciar el ciclo de vida, una aplicación cliente almacena un objeto en StorageGRID.

2. Objeto movido al pool de almacenamiento en la nube S3

- Cuando el objeto coincide con una regla ILM que utiliza un grupo de almacenamiento en la nube S3 como su ubicación, StorageGRID mueve el objeto al depósito S3 externo especificado por el grupo de almacenamiento en la nube.

- Cuando el objeto se ha movido al grupo de almacenamiento en la nube S3, la aplicación cliente puede recuperarlo mediante una solicitud GetObject de S3 desde StorageGRID, a menos que el objeto se haya transferido al almacenamiento Glacier.

3. Objeto en transición a Glacier (estado no recuperable)

- Opcionalmente, el objeto puede trasladarse al almacenamiento de Glacier. Por ejemplo, el depósito S3 externo podría usar la configuración del ciclo de vida para trasladar un objeto al almacenamiento de Glacier inmediatamente o después de una cierta cantidad de días.



Si desea realizar la transición de objetos, debe crear una configuración de ciclo de vida para el depósito S3 externo y debe utilizar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y admita la API S3 RestoreObject.

- Durante la transición, la aplicación cliente puede utilizar una solicitud S3 HeadObject para monitorear el estado del objeto.

4. Objeto restaurado del almacenamiento del glaciar

Si un objeto se ha transferido al almacenamiento de Glacier, la aplicación cliente puede emitir una solicitud S3 RestoreObject para restaurar una copia recuperable al grupo de almacenamiento en la nube S3. La solicitud especifica cuántos días debe estar disponible la copia en el grupo de almacenamiento en la nube y el nivel de acceso a datos que se utilizará para la operación de restauración (acelerada, estándar o masiva). Cuando se alcanza la fecha de vencimiento de la copia recuperable, la copia vuelve automáticamente a un estado no recuperable.



Si también existen una o más copias del objeto en los nodos de almacenamiento dentro de StorageGRID, no es necesario restaurar el objeto desde Glacier emitiendo una solicitud RestoreObject. En cambio, la copia local se puede recuperar directamente, mediante una solicitud GetObject.

5. Objeto recuperado

Una vez que se ha restaurado un objeto, la aplicación cliente puede emitir una solicitud GetObject para recuperar el objeto restaurado.

Azure: ciclo de vida de un objeto de grupo de almacenamiento en la nube

Los pasos describen las etapas del ciclo de vida de un objeto almacenado en un grupo de almacenamiento en la nube de Azure.

1. Objeto almacenado en StorageGRID

Para iniciar el ciclo de vida, una aplicación cliente almacena un objeto en StorageGRID.

2. Objeto movido al grupo de almacenamiento en la nube de Azure

Cuando el objeto coincide con una regla ILM que usa un grupo de almacenamiento en la nube de Azure como su ubicación, StorageGRID mueve el objeto al contenedor de almacenamiento de blobs de Azure externo especificado por el grupo de almacenamiento en la nube.

3. Objeto en transición al nivel de archivo (estado no recuperable)

Inmediatamente después de mover el objeto al grupo de almacenamiento en la nube de Azure, StorageGRID transfiere automáticamente el objeto al nivel de archivo de almacenamiento de blobs de

Azure.

4. Objeto restaurado desde el nivel de archivo

Si un objeto se ha trasladado al nivel de archivo, la aplicación cliente puede emitir una solicitud S3 RestoreObject para restaurar una copia recuperable en el grupo de almacenamiento en la nube de Azure.

Cuando StorageGRID recibe RestoreObject, transfiere temporalmente el objeto al nivel Esporádico de almacenamiento de blobs de Azure. Tan pronto como se alcanza la fecha de vencimiento en la solicitud RestoreObject, StorageGRID transfiere el objeto nuevamente al nivel de archivo.



Si una o más copias del objeto también existen en los nodos de almacenamiento dentro de StorageGRID, no es necesario restaurar el objeto desde el nivel de acceso de archivo emitiendo una solicitud RestoreObject. En cambio, la copia local se puede recuperar directamente, mediante una solicitud GetObject.

5. Objeto recuperado

Una vez que se ha restaurado un objeto en el grupo de almacenamiento en la nube de Azure, la aplicación cliente puede emitir una solicitud GetObject para recuperar el objeto restaurado.

Información relacionada

["Utilice la API REST de S3"](#)

Cuándo utilizar grupos de almacenamiento en la nube

Al utilizar grupos de almacenamiento en la nube, puede realizar copias de seguridad o agrupar datos en niveles en una ubicación externa. Además, puedes realizar copias de seguridad o agrupar datos en más de una nube.

Realizar una copia de seguridad de los datos de StorageGRID en una ubicación externa

Puede utilizar un grupo de almacenamiento en la nube para realizar copias de seguridad de objetos StorageGRID en una ubicación externa.

Si las copias en StorageGRID son inaccesibles, los datos de los objetos en el grupo de almacenamiento en la nube se pueden usar para atender las solicitudes de los clientes. Sin embargo, es posible que necesite emitir una solicitud S3 RestoreObject para acceder a la copia del objeto de respaldo en el grupo de almacenamiento en la nube.

Los datos de objetos en un grupo de almacenamiento en la nube también se pueden usar para recuperar datos perdidos de StorageGRID debido a una falla del volumen de almacenamiento o del nodo de almacenamiento. Si la única copia restante de un objeto está en un grupo de almacenamiento en la nube, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el nodo de almacenamiento recuperado.

Para implementar una solución de respaldo:

1. Crear un único grupo de almacenamiento en la nube.
2. Configure una regla ILM que almacene simultáneamente copias de objetos en nodos de almacenamiento (como copias replicadas o codificadas por borrado) y una única copia de objeto en el grupo de almacenamiento en la nube.

3. Añade la regla a tu política ILM. Luego, simule y active la política.

Datos de niveles desde StorageGRID a una ubicación externa

Puede utilizar un grupo de almacenamiento en la nube para almacenar objetos fuera del sistema StorageGRID . Por ejemplo, supongamos que tiene una gran cantidad de objetos que necesita conservar, pero espera acceder a ellos en raras ocasiones, o nunca. Puede utilizar un grupo de almacenamiento en la nube para organizar los objetos en un almacenamiento de menor costo y liberar espacio en StorageGRID.

Para implementar una solución de niveles:

1. Crear un único grupo de almacenamiento en la nube.
2. Configure una regla ILM que mueva objetos rara vez utilizados desde los nodos de almacenamiento al grupo de almacenamiento en la nube.
3. Añade la regla a tu política ILM. Luego, simule y active la política.

Mantener múltiples puntos finales en la nube

Puede configurar varios puntos finales de Cloud Storage Pool si desea organizar en niveles o realizar copias de seguridad de datos de objetos en más de una nube. Los filtros en sus reglas ILM le permiten especificar qué objetos se almacenan en cada grupo de almacenamiento en la nube. Por ejemplo, es posible que desee almacenar objetos de algunos inquilinos o buckets en Amazon S3 Glacier y objetos de otros inquilinos o buckets en Azure Blob Storage. O bien, es posible que desee mover datos entre Amazon S3 Glacier y Azure Blob Storage.



Al utilizar varios puntos finales de un grupo de almacenamiento en la nube, tenga en cuenta que un objeto solo se puede almacenar en un grupo de almacenamiento en la nube a la vez.

Para implementar múltiples puntos finales en la nube:

1. Crea hasta 10 grupos de almacenamiento en la nube.
2. Configure las reglas de ILM para almacenar los datos de objetos adecuados en el momento adecuado en cada grupo de almacenamiento en la nube. Por ejemplo, almacene objetos del depósito A en el grupo de almacenamiento en la nube A y almacene objetos del depósito B en el grupo de almacenamiento en la nube B. O bien, almacene objetos en el grupo de almacenamiento en la nube A durante un período de tiempo y luego muévalos al grupo de almacenamiento en la nube B.
3. Añade las reglas a tu política de ILM. Luego, simule y active la política.

Consideraciones para los grupos de almacenamiento en la nube

Si planea utilizar un grupo de almacenamiento en la nube para mover objetos fuera del sistema StorageGRID , debe revisar las consideraciones para configurar y usar grupos de almacenamiento en la nube.

Consideraciones generales

- En general, el almacenamiento de archivo en la nube, como Amazon S3 Glacier o Azure Blob Storage, es un lugar económico para almacenar datos de objetos. Sin embargo, los costos de recuperar datos del almacenamiento de archivos en la nube son relativamente altos. Para lograr el costo general más bajo, debe considerar cuándo y con qué frecuencia accederá a los objetos en el grupo de almacenamiento en la nube. Se recomienda utilizar un grupo de almacenamiento en la nube solo para contenido al que se espera acceder con poca frecuencia.

- No se admite el uso de grupos de almacenamiento en la nube con FabricPool debido a la latencia adicional para recuperar un objeto del destino del grupo de almacenamiento en la nube.
- Los objetos que tienen habilitado el bloqueo de objetos S3 no se pueden colocar en grupos de almacenamiento en la nube.
- Si el depósito S3 de destino de un grupo de almacenamiento en la nube tiene habilitado el bloqueo de objetos S3, el intento de configurar la replicación del depósito (PutBucketReplication) fallará con un error AccessDenied.
- Las siguientes combinaciones de plataforma, autenticación y protocolo con bloqueo de objetos S3 no son compatibles con los grupos de almacenamiento en la nube:
 - **Plataformas:** Google Cloud Platform y Azure
 - **Tipos de autenticación:** Roles de IAM en cualquier lugar y acceso anónimo
 - **Protocolo:** HTTP

Consideraciones sobre los puertos utilizados para los grupos de almacenamiento en la nube

Para garantizar que las reglas ILM puedan mover objetos hacia y desde el grupo de almacenamiento en la nube especificado, debe configurar la red o las redes que contienen los nodos de almacenamiento de su sistema. Debe asegurarse de que los siguientes puertos puedan comunicarse con el grupo de almacenamiento en la nube.

De forma predeterminada, los grupos de almacenamiento en la nube utilizan los siguientes puertos:

- **80:** Para URI de punto final que comienzan con http
- **443:** Para URI de puntos finales que comienzan con https

Puede especificar un puerto diferente al crear o editar un grupo de almacenamiento en la nube.

Si utiliza un servidor proxy no transparente, también debe ["configurar un proxy de almacenamiento"](#) para permitir que se envíen mensajes a puntos finales externos, como un punto final en Internet.

Consideraciones sobre los costos

El acceso al almacenamiento en la nube mediante un Cloud Storage Pool requiere conectividad de red a la nube. Debe considerar el costo de la infraestructura de red que utilizará para acceder a la nube y aprovisionarla adecuadamente, en función de la cantidad de datos que espera mover entre StorageGRID y la nube mediante el grupo de almacenamiento en la nube.

Cuando StorageGRID se conecta al punto final del grupo de almacenamiento en la nube externo, emite varias solicitudes para monitorear la conectividad y garantizar que pueda realizar las operaciones necesarias. Si bien estas solicitudes implicarán algunos costos adicionales, el costo de monitorear un grupo de almacenamiento en la nube debería ser solo una pequeña fracción del costo total de almacenar objetos en S3 o Azure.

Es posible que se produzcan costos más significativos si necesita mover objetos desde un punto final de un grupo de almacenamiento en la nube externo a StorageGRID. Los objetos se pueden mover nuevamente a StorageGRID en cualquiera de estos casos:

- La única copia del objeto está en un grupo de almacenamiento en la nube y usted decide almacenar el objeto en StorageGRID. En este caso, reconfigura tus reglas y políticas de ILM. Cuando se produce la evaluación de ILM, StorageGRID emite varias solicitudes para recuperar el objeto del grupo de almacenamiento en la nube. Luego, StorageGRID crea localmente la cantidad especificada de copias replicadas o codificadas por borrado. Una vez que el objeto se mueve nuevamente a StorageGRID, se elimina la copia en el grupo de almacenamiento en la nube.

- Los objetos se pierden debido a una falla del nodo de almacenamiento. Si la única copia restante de un objeto está en un grupo de almacenamiento en la nube, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el nodo de almacenamiento recuperado.



Cuando los objetos se mueven nuevamente a StorageGRID desde un grupo de almacenamiento en la nube, StorageGRID emite múltiples solicitudes al punto final del grupo de almacenamiento en la nube para cada objeto. Antes de mover grandes cantidades de objetos, comuníquese con el soporte técnico para obtener ayuda para estimar el tiempo y los costos asociados.

S3: Permisos necesarios para el depósito del grupo de almacenamiento en la nube

Las políticas para el depósito S3 externo utilizado para un grupo de almacenamiento en la nube deben otorgarle a StorageGRID permiso para mover un objeto al depósito, obtener el estado de un objeto, restaurar un objeto desde el almacenamiento de Glacier cuando sea necesario, etc. Idealmente, StorageGRID debería tener acceso de control total al depósito.(s3: *); sin embargo, si esto no es posible, la política del bucket debe otorgar 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 depósito externo

El movimiento de objetos entre StorageGRID y el depósito S3 externo especificado en el grupo de almacenamiento en la nube está controlado por las reglas de ILM y las políticas de ILM activas en StorageGRID. Por el contrario, la transición de objetos del depósito S3 externo especificado en el grupo de almacenamiento en la nube a Amazon S3 Glacier o S3 Glacier Deep Archive (o a una solución de almacenamiento que implementa la clase de almacenamiento Glacier) está controlada por la configuración del ciclo de vida de ese depósito.

Si desea realizar la transición de objetos desde el grupo de almacenamiento en la nube, debe crear la configuración de ciclo de vida adecuada en el depósito S3 externo y debe utilizar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y admita la API S3 RestoreObject.

Por ejemplo, supongamos que desea que todos los objetos que se mueven desde StorageGRID al grupo de almacenamiento en la nube se transfieran al almacenamiento de Amazon S3 Glacier de inmediato. Debe crear una configuración de ciclo de vida en el depósito S3 externo que especifique una única acción (**Transición**) de la siguiente manera:

```
<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 trasladaría todos los objetos de bucket a Amazon S3 Glacier el día en que se crearon (es decir, el día en que se trasladaron de StorageGRID al Cloud Storage Pool).



Al configurar el ciclo de vida del depósito externo, nunca utilice acciones **Expiración** para definir cuándo expiran los objetos. Las acciones de expiración hacen que el sistema de almacenamiento externo elimine los objetos expirados. Si posteriormente intenta acceder a un objeto caducado desde StorageGRID, no se encontrará el objeto eliminado.

Si desea transferir objetos del grupo de almacenamiento en la nube a S3 Glacier Deep Archive (en lugar de a Amazon S3 Glacier), especifique `<StorageClass>DEEP_ARCHIVE</StorageClass>` en el ciclo de vida del bucket. Sin embargo, tenga en cuenta que no puede utilizar el Expedited Nivel para restaurar objetos del Archivo S3 Glacier Deep.

Azure: Consideraciones para el nivel de acceso

Al configurar una cuenta de almacenamiento de Azure, puede establecer el nivel de acceso predeterminado en Activo o Esporádico. Al crear una cuenta de almacenamiento para usarla con un grupo de almacenamiento en la nube, debe utilizar el nivel Activo como nivel predeterminado. Si bien StorageGRID establece inmediatamente el nivel en Archivo cuando mueve objetos al grupo de almacenamiento en la nube, el uso de una configuración predeterminada de Activo garantiza que no se le cobrará una tarifa de eliminación anticipada por los objetos eliminados del nivel Fresco antes del mínimo de 30 días.

Azure: No se admite la gestión del ciclo de vida

No utilice la administración del ciclo de vida del almacenamiento de blobs de Azure para el contenedor utilizado con un grupo de almacenamiento en la nube. Las operaciones del ciclo de vida podrían interferir con las operaciones del grupo de almacenamiento en la nube.

Información relacionada

["Crear un grupo de almacenamiento en la nube"](#)

Comparar los grupos de almacenamiento en la nube y la replicación de CloudMirror

A medida que comience a utilizar los grupos de almacenamiento en la nube, puede resultar útil comprender las similitudes y diferencias entre los grupos de almacenamiento

en la nube y el servicio de replicación StorageGRID CloudMirror.

	Grupo de almacenamiento en la nube	Servicio de replicación CloudMirror
¿Cuál es el propósito principal?	Actúa como un objetivo de archivo. La copia del objeto en el grupo de almacenamiento en la nube puede ser la única copia del objeto o puede ser una copia adicional. Es decir, en lugar de mantener dos copias en el sitio, puede mantener una copia dentro de StorageGRID y enviar una copia al grupo de almacenamiento en la nube.	Permite que un inquilino replique automáticamente objetos desde un depósito en StorageGRID (origen) a un depósito S3 externo (destino). Crea una copia independiente de un objeto en una infraestructura S3 independiente.
¿Cómo está configurado?	Se define de la misma manera que los grupos de almacenamiento, utilizando Grid Manager o la API de administración de Grid. Se puede seleccionar como ubicación de colocación en una regla ILM. Mientras que un grupo de almacenamiento consta de un grupo de nodos de almacenamiento, un grupo de almacenamiento en la nube se define mediante un punto final remoto de S3 o Azure (dirección IP, credenciales, etc.).	Un usuario inquilino "configura la replicación de CloudMirror" definiendo un punto final de CloudMirror (dirección IP, credenciales, etc.) mediante el Administrador de inquilinos o la API S3. Una vez configurado el punto final de CloudMirror, cualquier depósito propiedad de esa cuenta de inquilino se puede configurar para apuntar al punto final de CloudMirror.
¿Quién es responsable de configurarlo?	Por lo general, un administrador de red	Normalmente, un usuario inquilino
¿Cual es el destino?	• Cualquier infraestructura S3 compatible (incluido Amazon S3) • Nivel de archivo de blobs de Azure • Plataforma de Google Cloud (GCP)	• Cualquier infraestructura S3 compatible (incluido Amazon S3) • Plataforma de Google Cloud (GCP)
¿Qué hace que los objetos se muevan al destino?	Una o más reglas ILM en las políticas ILM activas. Las reglas de ILM definen qué objetos StorageGRID mueve al grupo de almacenamiento en la nube y cuándo se mueven los objetos.	El acto de ingerir un nuevo objeto en un depósito de origen que se ha configurado con un punto final de CloudMirror. Los objetos que existían en el depósito de origen antes de que este se configurara con el punto final de CloudMirror no se replican, a menos que se modifiquen.

	Grupo de almacenamiento en la nube	Servicio de replicación CloudMirror
¿Cómo se recuperan los objetos?	Las aplicaciones deben realizar solicitudes a StorageGRID para recuperar objetos que se han movido a un grupo de almacenamiento en la nube. Si la única copia de un objeto se ha transferido al almacenamiento de archivo, StorageGRID administra el proceso de restauración del objeto para que pueda recuperarse.	Dado que la copia reflejada en el depósito de destino es una copia independiente, las aplicaciones pueden recuperar el objeto realizando solicitudes a StorageGRID o al destino S3. Por ejemplo, supongamos que utiliza la replicación de CloudMirror para reflejar objetos en una organización asociada. El socio puede utilizar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario utilizar StorageGRID .
¿Puedes leer desde el destino directamente?	No. Los objetos trasladados a un grupo de almacenamiento en la nube son administrados por StorageGRID. Las solicitudes de lectura deben dirigirse a StorageGRID (y StorageGRID será responsable de la recuperación del grupo de almacenamiento en la nube).	Sí, porque la copia reflejada es una copia independiente.
¿Qué sucede si se elimina un objeto de la fuente?	El objeto también se elimina del grupo de almacenamiento en la nube.	La acción de eliminar no se replica. Un objeto eliminado ya no existe en el depósito StorageGRID , pero continúa existiendo en el depósito de destino. De manera similar, los objetos en el depósito de destino se pueden eliminar sin afectar el origen.
¿Cómo acceder a los objetos después de un desastre (el sistema StorageGRID no está operativo)?	Los nodos StorageGRID fallidos deben recuperarse. Durante este proceso, se pueden restaurar copias de objetos replicados utilizando las copias en el grupo de almacenamiento en la nube.	Las copias de objetos en el destino CloudMirror son independientes de StorageGRID, por lo que se puede acceder a ellas directamente antes de que se recuperen los nodos de StorageGRID .

Crear un grupo de almacenamiento en la nube

Un grupo de almacenamiento en la nube especifica un único depósito externo de Amazon S3 u otro proveedor compatible con S3 o un contenedor de almacenamiento de blobs de Azure.

Cuando se crea un grupo de almacenamiento en la nube, se especifica el nombre y la ubicación del contenedor o depósito externo que StorageGRID usará para almacenar objetos, el tipo de proveedor de nube (Amazon S3/GCP o Azure Blob Storage) y la información que StorageGRID necesita para acceder al contenedor o depósito externo.

StorageGRID valida el grupo de almacenamiento en la nube tan pronto como lo guarda, por lo que debe asegurarse de que el depósito o contenedor especificado en el grupo de almacenamiento en la nube exista y

sea accesible.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["permisos de acceso necesarios"](#) .
- Usted ha revisado el ["Consideraciones para los grupos de almacenamiento en la nube"](#) .
- El contenedor o depósito externo al que hace referencia el grupo de almacenamiento en la nube ya existe y usted tiene la [información del punto final del servicio](#) .
- Para acceder al cubo o contenedor, tienes el [Información de la cuenta para el tipo de autenticación](#) Tú elegirás.

Pasos

1. Seleccione **ILM > Grupos de almacenamiento > Grupos de almacenamiento en la nube**.
2. Seleccione **Crear**, luego ingrese la siguiente información:

Campo	Descripción
Nombre del grupo de almacenamiento en la nube	Un nombre que describe brevemente el grupo de almacenamiento en la nube y su propósito. Utilice un nombre que sea fácil de identificar cuando configure las reglas de ILM.
Tipo de proveedor	¿Qué proveedor de nube utilizará para este grupo de almacenamiento en la nube? • Amazon S3/GCP: seleccione esta opción para un proveedor de Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) u otro proveedor compatible con S3. • Almacenamiento de blobs de Azure
Cubo o contenedor	El nombre del depósito S3 externo o del contenedor de Azure. No es posible cambiar este valor una vez guardado el grupo de almacenamiento en la nube.

3. Según su selección del tipo de proveedor, ingrese la información del punto final del servicio.

Amazon S3/GCP

- a. Para el protocolo, seleccione HTTPS o HTTP.



No utilice conexiones HTTP para datos confidenciales.

- b. Introduzca el nombre del host. Ejemplo:

`s3-aws-region.amazonaws.com`

- c. Seleccione el estilo de URL:

Opción	Descripción
Detección automática	Intente detectar automáticamente qué estilo de URL utilizar, según la información proporcionada. Por ejemplo, si especifica una dirección IP, StorageGRID utilizará una URL de estilo ruta. Seleccione esta opción solo si no sabe qué estilo específico usar.
Estilo alojado virtualmente	Utilice una URL de estilo alojado virtualmente para acceder al depósito. Las URL de estilo alojado virtualmente incluyen el nombre del depósito como parte del nombre de dominio. Ejemplo: <code>https://bucket-name.s3.company.com/key-name</code>
Estilo de ruta	Utilice una URL de estilo de ruta para acceder al depósito. Las URL de estilo de ruta incluyen el nombre del depósito al final. Ejemplo: <code>https://s3.company.com/bucket-name/key-name</code> Nota: La opción de URL de estilo de ruta no se recomienda y quedará obsoleta en una versión futura de StorageGRID.

- d. Opcionalmente, ingrese el número de puerto o utilice el puerto predeterminado: 443 para HTTPS o 80 para HTTP.

Almacenamiento de blobs de Azure

- a. Utilice uno de los siguientes formatos para ingresar el URI del punto final del servicio.

- `https://host:port`
- `http://host:port`

Ejemplo: `https://myaccount.blob.core.windows.net:443`

Si no especifica un puerto, de manera predeterminada se utiliza el puerto 443 para HTTPS y el puerto 80 para HTTP.

4. Seleccione **Continuar**. Luego, seleccione el tipo de autenticación e ingrese la información requerida para el punto final del grupo de almacenamiento en la nube:

Tecla de acceso

Para Amazon S3/GCP u otro proveedor compatible con S3

- a. **ID de clave de acceso:** Ingrese el ID de clave de acceso para la cuenta que posee el depósito externo.
- b. **Clave de acceso secreta:** Ingrese la clave de acceso secreta.

Roles de IAM en cualquier lugar

Para el servicio AWS IAM Roles Anywhere

StorageGRID utiliza el Servicio de token de seguridad de AWS (STS) para generar dinámicamente un token de corta duración para acceder a los recursos de AWS.

- a. **Región de AWS IAM Roles Anywhere:** seleccione la región para el grupo de almacenamiento en la nube. Por ejemplo, `us-east-1`.
- b. **URN de ancla de confianza:** ingrese la URN del ancla de confianza que valida las solicitudes de credenciales STS de corta duración. Puede ser una CA raíz o intermedia.
- c. **URN de perfil:** ingrese la URN del perfil de IAM Roles Anywhere que enumera los roles que pueden asumirse para cualquier persona de confianza.
- d. **URN de rol:** Ingrese el URN del rol de IAM que puede asumir cualquier persona de confianza.
- e. **Duración de la sesión:** Ingrese la duración de las credenciales de seguridad temporales y la sesión del rol. Ingrese al menos 15 minutos y no más de 12 horas.
- f. **Certificado de CA del servidor** (opcional): Uno o más certificados de CA confiables, en formato PEM, para verificar el servidor de IAM Roles Anywhere. Si se omite, el servidor no se verificará.
- g. **Certificado de entidad final:** La clave pública, en formato PEM, del certificado X509 firmado por el ancla de confianza. AWS IAM Roles Anywhere utiliza esta clave para emitir un token STS.
- h. **Clave privada de entidad final:** la clave privada para el certificado de entidad final.

CAP (portal de acceso C2S)

Para el servicio S3 de Servicios de Nube Comercial (C2S)

- a. **URL de credenciales temporales:** ingrese la URL completa que StorageGRID utilizará para obtener las credenciales temporales del servidor CAP, incluidos todos los parámetros de API obligatorios y opcionales asignados a su cuenta C2S.
- b. **Certificado CA del servidor:** seleccione **Explorar** y cargue el certificado CA que StorageGRID utilizará para verificar el servidor CAP. El certificado debe estar codificado en PEM y ser emitido por una autoridad de certificación gubernamental (CA) apropiada.
- c. **Certificado de cliente:** seleccione **Explorar** y cargue el certificado que StorageGRID utilizará para identificarse en el servidor CAP. El certificado del cliente debe estar codificado en PEM, emitido por una autoridad de certificación gubernamental (CA) apropiada y tener acceso a su cuenta C2S.
- d. **Clave privada del cliente:** seleccione **Explorar** y cargue la clave privada codificada en PEM para el certificado del cliente.
- e. Si la clave privada del cliente está cifrada, ingrese la contraseña para descifrarla. De lo contrario, deje el campo **Frase de contraseña de clave privada del cliente** en blanco.



Si se va a cifrar el certificado del cliente, utilice el formato tradicional para el cifrado. El formato cifrado PKCS #8 no es compatible.

Almacenamiento de blobs de Azure

Para Azure Blob Storage, solo clave compartida

- Nombre de la cuenta:** Ingrese el nombre de la cuenta de almacenamiento que posee el contenedor externo
- Clave de cuenta:** Ingrese la clave secreta para la cuenta de almacenamiento

Puede utilizar el portal de Azure para encontrar estos valores.

Anónimo

No se requiere información adicional

5. Seleccione **Continuar**. A continuación, elija el tipo de verificación de servidor que desea utilizar:

Opción	Descripción
Usar certificados de CA raíz en el sistema operativo del nodo de almacenamiento	Utilice los certificados CA de Grid instalados en el sistema operativo para proteger las conexiones.
Utilice un certificado CA personalizado	Utilice un certificado CA personalizado. Seleccione Explorar y cargue el certificado codificado en PEM.
No verificar el certificado	Seleccionar esta opción significa que las conexiones TLS al grupo de almacenamiento en la nube no son seguras.

6. Seleccione **Guardar**.

Cuando guarda un grupo de almacenamiento en la nube, StorageGRID hace lo siguiente:

- Valida que el depósito o contenedor y el punto final del servicio existan y que se pueda acceder a ellos utilizando las credenciales que usted especificó.
- Escribe un archivo de marcador en el depósito o contenedor para identificarlo como un grupo de almacenamiento en la nube. Nunca elimine este archivo, que se llama `x-ntap-sgws-cloud-pool-uuid`.

Si falla la validación del grupo de almacenamiento en la nube, recibirá un mensaje de error que explica por qué falló la validación. Por ejemplo, se podría informar un error si hay un error de certificado o si el depósito o contenedor especificado aún no existe.

7. Si se produce un error, consulte la "[Instrucciones para solucionar problemas de grupos de almacenamiento en la nube](#)", resuelva cualquier problema y luego intente guardar el grupo de almacenamiento en la nube nuevamente.

Ver detalles del grupo de almacenamiento en la nube

Puede ver los detalles de un grupo de almacenamiento en la nube para determinar

dónde se utiliza y ver qué nodos y grados de almacenamiento están incluidos.

Antes de empezar

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

Pasos

1. Seleccione **ILM > Grupos de almacenamiento > Grupos de almacenamiento en la nube**.

La tabla de grupos de almacenamiento en la nube incluye la siguiente información para cada grupo de almacenamiento en la nube que incluye nodos de almacenamiento:

- **Nombre:** el nombre para mostrar único del grupo.
- **URI:** El identificador uniforme de recursos del grupo de almacenamiento en la nube.
- **Tipo de proveedor:** ¿Qué proveedor de nube se utiliza para este grupo de almacenamiento en la nube?
- **Contenedor:** el nombre del depósito utilizado para el grupo de almacenamiento en la nube.
- **Uso de ILM:** cómo se utiliza actualmente el pool. Es posible que un grupo de almacenamiento en la nube no se utilice o que se utilice en una o más reglas ILM, perfiles de codificación de borrado o ambos.
- **Último error:** el último error detectado durante una verificación del estado de este grupo de almacenamiento en la nube.

2. Para ver los detalles de un grupo de almacenamiento en la nube específico, seleccione su nombre.

Aparece la página de detalles del grupo.

3. Consulte la pestaña **Autenticación** para obtener información sobre el tipo de autenticación para este grupo de almacenamiento en la nube y para editar los detalles de autenticación.
4. Vea la pestaña **Verificación del servidor** para obtener información sobre los detalles de verificación, editar la verificación, descargar un nuevo certificado o copiar el certificado PEM.
5. Vea la pestaña **Uso de ILM** para determinar si el grupo de almacenamiento en la nube se está utilizando actualmente en alguna regla de ILM o perfil de codificación de borrado.
6. Opcionalmente, vaya a la **página de reglas de ILM** para ["Conozca y administre cualquier regla"](#) que utilizan el grupo de almacenamiento en la nube.

Editar un grupo de almacenamiento en la nube

Puede editar un grupo de almacenamiento en la nube para cambiar su nombre, punto final de servicio u otros detalles; sin embargo, no puede cambiar el depósito S3 ni el contenedor de Azure de un grupo de almacenamiento en la nube.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Usted ha revisado el ["Consideraciones para los grupos de almacenamiento en la nube"](#) .

Pasos

1. Seleccione **ILM > Grupos de almacenamiento > Grupos de almacenamiento en la nube**.

La tabla Grupos de almacenamiento en la nube enumera los grupos de almacenamiento en la nube existentes.

2. Seleccione la casilla de verificación del grupo de almacenamiento en la nube que desea editar y luego seleccione **Acciones > Editar**.

Alternativamente, seleccione el nombre del grupo de almacenamiento en la nube y luego seleccione **Editar**.

3. Según sea necesario, cambie el nombre del grupo de almacenamiento en la nube, el punto final del servicio, las credenciales de autenticación o el método de verificación del certificado.



No se puede cambiar el tipo de proveedor ni el bucket S3 ni el contenedor de Azure para un grupo de almacenamiento en la nube.

Si anteriormente cargó un certificado de servidor o cliente, puede expandir el acordeón **Detalles del certificado** para revisar el certificado que está actualmente en uso.

4. Seleccione **Guardar**.

Cuando guarda un grupo de almacenamiento en la nube, StorageGRID valida que el depósito o contenedor y el punto final del servicio existan y que se pueda acceder a ellos mediante las credenciales que usted especificó.

Si falla la validación del grupo de almacenamiento en la nube, se muestra un mensaje de error. Por ejemplo, se podría informar un error si hay un error de certificado.

Vea las instrucciones para "[Solución de problemas de grupos de almacenamiento en la nube](#)", resuelva el problema y luego intente guardar el grupo de almacenamiento en la nube nuevamente.

Eliminar un grupo de almacenamiento en la nube

Puede eliminar un grupo de almacenamiento en la nube si no se utiliza en una regla ILM y no contiene datos de objetos.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tú tienes el "[permisos de acceso necesarios](#)".

Si es necesario, utilice ILM para mover datos de objetos

Si el grupo de almacenamiento en la nube que desea eliminar contiene datos de objetos, debe usar ILM para mover los datos a una ubicación diferente. Por ejemplo, puede mover los datos a nodos de almacenamiento en su red o a un grupo de almacenamiento en la nube diferente.

Pasos

1. Seleccione **ILM > Grupos de almacenamiento > Grupos de almacenamiento en la nube**.

2. Mire la columna de uso de ILM en la tabla para determinar si puede eliminar el grupo de almacenamiento en la nube.

No se puede eliminar un grupo de almacenamiento en la nube si se está utilizando en una regla ILM o en un perfil de codificación de borrado.

3. Si se está utilizando el grupo de almacenamiento en la nube, seleccione **nombre del grupo de almacenamiento en la nube > uso de ILM**.
4. ["Clonar cada regla ILM"](#) que actualmente coloca objetos en el grupo de almacenamiento en la nube que desea eliminar.
5. Determina dónde quieres mover los objetos existentes administrados por cada regla que clones.

Puede utilizar uno o más grupos de almacenamiento o un grupo de almacenamiento en la nube diferente.

6. Edite cada una de las reglas que clonó.

Para el paso 2 del asistente para crear reglas de ILM, seleccione la nueva ubicación en el campo **copias en**.

7. ["Crear una nueva política de ILM"](#) y reemplazar cada una de las reglas antiguas con una regla clonada.
8. Activar la nueva política.
9. Espere a que ILM elimine objetos del grupo de almacenamiento en la nube y los coloque en la nueva ubicación.

Eliminar grupo de almacenamiento en la nube

Cuando el grupo de almacenamiento en la nube esté vacío y no se utilice en ninguna regla de ILM, puedes eliminarlo.

Antes de empezar

- Ha eliminado todas las reglas ILM que podrían haber utilizado el grupo.
- Ha confirmado que el bucket S3 o el contenedor de Azure no contiene ningún objeto.

Se produce un error si intenta eliminar un grupo de almacenamiento en la nube si contiene objetos. Ver ["Solucionar problemas de grupos de almacenamiento en la nube"](#).



Cuando se crea un grupo de almacenamiento en la nube, StorageGRID escribe un archivo marcador en el depósito o contenedor para identificarlo como un grupo de almacenamiento en la nube. No elimine este archivo, que se llama `x-ntap-sgws-cloud-pool-uuid`.

Pasos

1. Seleccione **ILM > Grupos de almacenamiento > Grupos de almacenamiento en la nube**.
2. Si la columna de uso de ILM indica que no se está utilizando el grupo de almacenamiento en la nube, seleccione la casilla de verificación.
3. Seleccione **Acciones > Eliminar**.
4. Seleccione **Aceptar**.

Solucionar problemas de grupos de almacenamiento en la nube

Utilice estos pasos de solución de problemas para ayudar a resolver errores que pueda encontrar al crear, editar o eliminar un grupo de almacenamiento en la nube.

Determinar si se ha producido un error

StorageGRID realiza una comprobación de estado simple en cada grupo de almacenamiento en la nube leyendo el objeto conocido `x-ntap-sgws-cloud-pool-uuid` para garantizar que se pueda acceder al grupo de almacenamiento en la nube y que funcione correctamente. Cuando StorageGRID detecta un error en el punto final, realiza una comprobación del estado cada minuto desde cada nodo de almacenamiento. Cuando se resuelve el error, las comprobaciones de estado se detienen. Si una verificación de estado detecta un problema, se muestra un mensaje en la columna **Último error** de la tabla **Grupos de almacenamiento** en la nube en la página **Grupos de almacenamiento**.

La tabla muestra el error más reciente detectado para cada grupo de almacenamiento en la nube e indica cuánto tiempo hace que ocurrió el error.

Además, se activa una alerta de **Error de conectividad del Cloud Storage Pool** si la comprobación de estado detecta que se han producido uno o más errores nuevos del Cloud Storage Pool en los últimos 5 minutos. Si recibe una notificación por correo electrónico para esta alerta, vaya a la página **Grupos de almacenamiento** (seleccione **ILM > Grupos de almacenamiento**), revise los mensajes de error en la columna **Último error** y consulte las pautas de solución de problemas a continuación.

Comprobar si se ha resuelto un error

Después de resolver cualquier problema subyacente, puede determinar si se ha resuelto el error. Desde la página **Grupo de almacenamiento en la nube**, seleccione el punto final y seleccione **Borrar error**. Un mensaje de confirmación indica que StorageGRID ha solucionado el error del grupo de almacenamiento en la nube.

Si se ha resuelto el problema subyacente, el mensaje de error ya no se muestra. Sin embargo, si el problema subyacente no se ha solucionado (o si se encuentra un error diferente), el mensaje de error se mostrará en la columna **Último error** dentro de unos minutos.

Error: Error en la comprobación de salud. Error del punto final

Es posible que encuentre este error cuando habilite el bloqueo de objetos S3 con retención predeterminada para su depósito de Amazon S3 después de comenzar a usar este depósito para un grupo de almacenamiento en la nube. Este error ocurre cuando la operación PUT no tiene un encabezado HTTP con un valor de suma de comprobación de carga útil como `Content-MD5`. AWS requiere este valor de encabezado para operaciones PUT en buckets con el bloqueo de objetos S3 habilitado.

Para corregir este problema, siga los pasos que se indican en ["Editar un grupo de almacenamiento en la nube"](#) sin realizar ningún cambio. Esta acción activa la validación de la configuración del grupo de almacenamiento en la nube que detecta y actualiza automáticamente el indicador de bloqueo de objetos S3 en una configuración de punto final del grupo de almacenamiento en la nube.

Error: Este grupo de almacenamiento en la nube contiene contenido inesperado

Es posible que encuentre este error cuando intente crear, editar o eliminar un grupo de almacenamiento en la nube. Este error se produce si el depósito o contenedor incluye el `x-ntap-sgws-cloud-pool-uuid` archivo marcador, pero ese archivo no tiene el campo de metadatos con el UUID esperado.

Por lo general, solo verá este error si está creando un nuevo grupo de almacenamiento en la nube y otra instancia de StorageGRID ya está usando el mismo grupo de almacenamiento en la nube.

Pruebe uno de estos pasos para corregir el problema:

- Si está configurando un nuevo grupo de almacenamiento en la nube y el depósito contiene el `x-ntap-sgws-cloud-pool-uuid` archivo y claves de objeto adicionales similares al siguiente ejemplo, cree un

nuevo depósito y use este nuevo depósito en su lugar.

Ejemplo de una clave de objeto adicional: `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- Si el `x-ntap-sgws-cloud-pool-uuid` el archivo es el único objeto en el depósito, elimine este archivo.

Si estos pasos no se aplican a su situación, comuníquese con el soporte técnico.

Error: No se pudo crear o actualizar el grupo de almacenamiento en la nube. Error del punto final

Es posible que encuentre este error en las siguientes circunstancias:

- Cuando intenta crear o editar un grupo de almacenamiento en la nube.
- Cuando selecciona una plataforma, autenticación o combinación de protocolo no compatible con S3 Object Lock durante la configuración de un nuevo grupo de almacenamiento en la nube. Ver ["Consideraciones para los grupos de almacenamiento en la nube"](#).

Este error indica que un problema de conectividad o configuración impide que StorageGRID escriba en el grupo de almacenamiento en la nube.

Para corregir el problema, revise el mensaje de error del punto final.

- Si el mensaje de error contiene `Get url: EOF` Verifique que el punto final del servicio utilizado para el grupo de almacenamiento en la nube no utilice HTTP para un contenedor o depósito que requiera HTTPS.
- Si el mensaje de error contiene `Get url: net/http: request canceled while waiting for connection`, verifique que la configuración de la red permita que los nodos de almacenamiento accedan al punto final de servicio utilizado para el grupo de almacenamiento en la nube.
- Si el error se debe a una plataforma, autenticación o protocolo no compatible, cambie a una configuración compatible con S3 Object Lock e intente guardar nuevamente el nuevo grupo de almacenamiento en la nube.
- Para todos los demás mensajes de error de punto final, pruebe una o más de las siguientes opciones:
 - Cree un contenedor o depósito externo con el mismo nombre que ingresó para el grupo de almacenamiento en la nube e intente guardar el nuevo grupo de almacenamiento en la nube nuevamente.
 - Corrija el nombre del contenedor o depósito que especificó para el grupo de almacenamiento en la nube e intente guardar el nuevo grupo de almacenamiento en la nube nuevamente.

Error: No se pudo analizar el certificado de CA

Es posible que encuentre este error cuando intente crear o editar un grupo de almacenamiento en la nube. El error ocurre si StorageGRID no pudo analizar el certificado ingresado al configurar el grupo de almacenamiento en la nube.

Para corregir el problema, verifique el certificado CA que proporcionó para ver si hay problemas.

Error: No se encontró un grupo de almacenamiento en la nube con este ID

Es posible que encuentre este error cuando intente editar o eliminar un grupo de almacenamiento en la nube. Este error ocurre si el punto final devuelve una respuesta 404, que puede significar cualquiera de las siguientes cosas:

- Las credenciales utilizadas para el grupo de almacenamiento en la nube no tienen permiso de lectura para el depósito.
- El depósito utilizado para el grupo de almacenamiento en la nube no incluye el `x-ntap-sgws-cloud-pool-uuid` archivo de marcador.

Pruebe uno o más de estos pasos para corregir el problema:

- Verifique que el usuario asociado a la clave de acceso configurada tenga los permisos necesarios.
- Edite el grupo de almacenamiento en la nube con credenciales que tengan los permisos necesarios.
- Si los permisos son correctos, comuníquese con el soporte.

Error: No se pudo comprobar el contenido del grupo de almacenamiento en la nube. Error del punto final

Es posible que encuentre este error cuando intente eliminar un grupo de almacenamiento en la nube. Este error indica que algún tipo de problema de conectividad o configuración impide que StorageGRID lea el contenido del depósito de Cloud Storage Pool.

Para corregir el problema, revise el mensaje de error del punto final.

Error: Ya se han colocado objetos en este depósito

Es posible que encuentre este error cuando intente eliminar un grupo de almacenamiento en la nube. No puedes eliminar un grupo de almacenamiento en la nube si contiene datos que ILM movió allí, datos que estaban en el depósito antes de configurar el grupo de almacenamiento en la nube o datos que alguna otra fuente colocó en el depósito después de que se creó el grupo de almacenamiento en la nube.

Pruebe uno o más de estos pasos para corregir el problema:

- Siga las instrucciones para mover objetos nuevamente a StorageGRID en "Ciclo de vida de un objeto de grupo de almacenamiento en la nube".
- Si está seguro de que ILM no colocó los objetos restantes en el grupo de almacenamiento en la nube, elimine manualmente los objetos del depósito.



Nunca elimine manualmente objetos de un grupo de almacenamiento en la nube que ILM pueda haber colocado allí. Si posteriormente intenta acceder a un objeto eliminado manualmente desde StorageGRID, no se encontrará el objeto eliminado.

Error: el proxy encontró un error externo al intentar acceder al grupo de almacenamiento en la nube

Es posible que encuentre este error si ha configurado un proxy de almacenamiento no transparente entre los nodos de almacenamiento y el punto final S3 externo utilizado para el grupo de almacenamiento en la nube. Este error se produce si el servidor proxy externo no puede acceder al punto final del grupo de almacenamiento en la nube. Por ejemplo, es posible que el servidor DNS no pueda resolver el nombre de host o que haya un problema de red externa.

Pruebe uno o más de estos pasos para corregir el problema:

- Verifique la configuración del grupo de almacenamiento en la nube (**ILM > Grupos de almacenamiento**).
- Verifique la configuración de red del servidor proxy de almacenamiento.

Error: el certificado X.509 está fuera del período de validez

Es posible que encuentre este error cuando intente eliminar un grupo de almacenamiento en la nube. Este error ocurre cuando la autenticación requiere un certificado X.509 para garantizar que se valide el grupo de almacenamiento en la nube externo correcto y el grupo externo está vacío antes de que se elimine la configuración del grupo de almacenamiento en la nube.

Pruebe estos pasos para corregir el problema:

- Actualice el certificado configurado para la autenticación en el grupo de almacenamiento en la nube.
- Asegúrese de que se haya resuelto cualquier alerta de vencimiento de certificado en este grupo de almacenamiento en la nube.

Información relacionada

["Ciclo de vida de un objeto de grupo de almacenamiento en la nube"](#)

Administrar perfiles de codificación de borrado

Puede ver los detalles de un perfil de codificación de borrado y cambiar el nombre de un perfil si es necesario. Puede desactivar un perfil de codificación de borrado si no se utiliza actualmente en ninguna regla ILM.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["permisos de acceso necesarios"](#).

Ver detalles del perfil de codificación de borrado

Puede ver los detalles de un perfil de codificación de borrado para determinar su estado, el esquema de codificación de borrado utilizado y otra información.

Pasos

1. Seleccione **CONFIGURACIÓN > Sistema > Codificación de borrado**.
2. Seleccione el perfil. Aparece la página de detalles del perfil.
3. Opcionalmente, consulte la pestaña de reglas de ILM para obtener una lista de las reglas de ILM que usan el perfil y las políticas de ILM que usan esas reglas.
4. Opcionalmente, consulte la pestaña Nodos de almacenamiento para obtener detalles sobre cada nodo de almacenamiento en el grupo de almacenamiento del perfil, como el sitio donde está ubicado y el uso del almacenamiento.

Cambiar el nombre de un perfil de codificación de borrado

Es posible que desees cambiar el nombre de un perfil de codificación de borrado para que sea más obvio lo que hace el perfil.

Pasos

1. Seleccione **CONFIGURACIÓN > Sistema > Codificación de borrado**.
2. Seleccione el perfil que desea renombrar.
3. Seleccione **Cambiar nombre**.

4. Introduzca un nombre único para el perfil de codificación de borrado.

El nombre del perfil de codificación de borrado se agrega al nombre del grupo de almacenamiento en la instrucción de ubicación de una regla ILM.



Los nombres de los perfiles de codificación 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 codificación de borrado

Puede desactivar un perfil de codificación de borrado si ya no planea usarlo y si el perfil no se utiliza actualmente en ninguna regla de ILM.



Confirme que no haya operaciones de reparación de datos con código de borrado ni procedimientos de desmantelamiento en proceso. Se devuelve un mensaje de error si intenta desactivar un perfil de codificación de borrado mientras alguna de estas operaciones está en progreso.

Acerca de esta tarea

StorageGRID le impide desactivar un perfil de codificación de borrado si se cumple alguna de las siguientes condiciones:

- Actualmente, el perfil de codificación de borrado se utiliza en una regla ILM.
- El perfil de codificación de borrado ya no se utiliza en ninguna regla ILM, pero los datos de objetos y los fragmentos de paridad para el perfil aún existen.

Pasos

1. Seleccione **CONFIGURACIÓN > Sistema > Codificación de borrado**.
2. En la pestaña Activo, revise la columna **Estado** para confirmar que el perfil de codificación de borrado que desea desactivar no se utiliza en ninguna regla de ILM.

No se puede desactivar un perfil de codificación de borrado si se utiliza en alguna regla ILM. En el ejemplo, el perfil 2+1 del centro de datos 1 se utiliza en al menos una regla ILM.

☐	Profile name 	Status 	Storage pool 	Erasure-coding scheme 
☐	2+1 Data Center 1	Used in <u>5 rules</u>	Data Center 1	2+1
☐	New profile	Deactivated	Data Center 1	2+1

3. Si el perfil se utiliza en una regla ILM, siga estos pasos:
 - a. Seleccione **ILM > Reglas**.
 - b. Seleccione cada regla y revise el diagrama de retención para determinar si la regla utiliza el perfil de codificación de borrado que desea desactivar.
 - c. Si la regla ILM utiliza el perfil de codificación de borrado que desea desactivar, determine si la regla se

utiliza en alguna política ILM.

d. Complete los pasos adicionales de la tabla, según dónde se utilice el perfil de codificación de borrado.

¿Dónde se ha utilizado el perfil?	Pasos adicionales a realizar antes de desactivar el perfil	Consulte estas instrucciones adicionales
Nunca se utiliza en ninguna regla ILM	No se requieren pasos adicionales. Continúe con este procedimiento.	<i>Ninguno</i>
En una regla ILM que nunca se ha utilizado en ninguna política ILM	i. Editar o eliminar todas las reglas ILM afectadas. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de codificación de borrado. ii. Continúe con este procedimiento.	"Trabajar con las reglas y políticas de ILM"
En una regla ILM que actualmente se encuentra en una política ILM activa	i. Clonar la política. ii. Eliminar la regla ILM que utiliza el perfil de codificación de borrado. iii. Agregue una o más reglas ILM nuevas para garantizar que los objetos estén protegidos. iv. Guarde, simule y active la nueva política. v. Espere a que se aplique la nueva política y a que los objetos existentes se muevan a nuevas ubicaciones según las nuevas reglas que agregó. Nota: Dependiendo de la cantidad de objetos y el tamaño de su sistema StorageGRID , las operaciones de ILM podrían tardar semanas o incluso meses en mover los objetos a nuevas ubicaciones, según las nuevas reglas de ILM. Si bien puede intentar desactivar de forma segura un perfil de codificación de borrado mientras aún esté 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 quitó de la política. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de codificación de borrado. vii. Continúe con este procedimiento.	"Crear una política ILM" "Trabajar con las reglas y políticas de ILM"

¿Dónde se ha utilizado el perfil?	Pasos adicionales a realizar antes de desactivar el perfil	Consulte estas instrucciones adicionales
En una regla ILM que actualmente se encuentra en una política ILM	i. Editar la política. ii. Eliminar la regla ILM que utiliza el perfil de codificación de borrado. iii. Agregue una o más reglas ILM nuevas para garantizar que todos los objetos estén protegidos. iv. Guardar la política. v. Edite o elimine la regla que quitó de la política. Si edita la regla, elimine todas las ubicaciones que utilicen el perfil de codificación de borrado. vi. Continúe con este procedimiento.	"Crear una política ILM" "Trabajar con las reglas y políticas de ILM"

e. Actualice la página Perfiles de codificación de borrado para asegurarse de que el perfil no se utilice en una regla ILM.

4. Si el perfil no se utiliza en una regla ILM, seleccione el botón de opción y seleccione **Desactivar**. Aparece el cuadro de diálogo Desactivar perfil de codificación de borrado.



Puede seleccionar varios perfiles para desactivarlos al mismo tiempo, siempre que cada perfil no se utilice en ninguna regla.

5. Si está seguro de que desea desactivar el perfil, seleccione **Desactivar**.

Resultados

- Si StorageGRID puede desactivar el perfil de codificación de borrado, su estado es Desactivado. Ya no puedes seleccionar este perfil para ninguna regla ILM. No es posible reactivar un perfil desactivado.
- Si StorageGRID no puede desactivar el perfil, aparecerá un mensaje de error. Por ejemplo, aparece un mensaje de error si los datos del objeto aún están asociados con este perfil. Es posible que tengas que esperar varias semanas antes de intentar nuevamente el proceso de desactivación.

Configurar regiones (opcional y solo S3)

Las reglas ILM pueden filtrar objetos según las regiones donde se crean los buckets S3, lo que le permite almacenar objetos de diferentes regiones en diferentes ubicaciones de almacenamiento.

Si desea utilizar una región de bucket S3 como filtro en una regla, primero debe crear las regiones que los buckets pueden usar en su sistema.



No es posible cambiar la región de un depósito una vez creado el mismo.

Antes de empezar

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

- Tienes "permisos de acceso específicos" .

Acerca de esta tarea

Al crear un depósito S3, puede especificar que el depósito se cree en una región específica. Al especificar una región, el bucket puede estar geográficamente cerca de sus usuarios, lo que puede ayudar a optimizar la latencia, minimizar los costos y abordar los requisitos regulatorios.

Al crear una regla ILM, es posible que desee utilizar la región asociada con un depósito S3 como filtro avanzado. Por ejemplo, puede diseñar una regla que se aplique únicamente a los objetos en los depósitos S3 creados en el `us-west-2` región. Luego, puede especificar que se coloquen copias de esos objetos en nodos de almacenamiento en un sitio del centro de datos dentro de esa región para optimizar la latencia.

Al configurar regiones, siga estas pautas:

- De forma predeterminada, se considera que todos los depósitos pertenecen a la `us-east-1` región.
- Debe crear las regiones usando Grid Manager antes de poder especificar una región no predeterminada al crear depósitos usando Tenant Manager o Tenant Management API o con el elemento de solicitud `LocationConstraint` para solicitudes de API de depósito PUT de S3. Se produce un error si una solicitud PUT Bucket utiliza una región que no se ha definido en StorageGRID.
- Debes utilizar el nombre exacto de la región al crear el bucket S3. Los nombres de las regiones distinguen entre mayúsculas y minúsculas. Los caracteres válidos son números, letras y guiones.



EU no se considera un alias de eu-west-1. Si desea utilizar la región UE o eu-west-1, debe utilizar el nombre exacto.

- No se puede eliminar ni modificar una región si se utiliza en una regla asignada a cualquier política (activa o inactiva).
- Si utiliza una región no válida como filtro avanzado en una regla ILM, no podrá agregar esa regla a una política.

Puede obtenerse una región no válida si utiliza una región como filtro avanzado en una regla ILM pero luego elimina esa región, o si utiliza la API de administración de cuadrícula para crear una regla y especificar una región que no ha definido.

- Si elimina una región después de usarla para crear un depósito S3, deberá volver a agregar la región si alguna vez desea utilizar el filtro avanzado de Restricción de ubicación para buscar objetos en ese depósito.

Pasos

1. Seleccione **ILM > Regiones**.

Aparece la página Regiones, con una lista de las regiones definidas actualmente. **Región 1** muestra la región predeterminada, `us-east-1`, que no se puede modificar ni eliminar.

2. Para agregar una región:

- a. Seleccione **Agregar otra región**.
- b. Ingrese el nombre de la región que desea utilizar al crear depósitos S3.

Debe utilizar este nombre de región exacto como elemento de solicitud `LocationConstraint` cuando cree el bucket S3 correspondiente.

3. Para eliminar una región no utilizada, seleccione el icono de eliminar  .

Aparece un mensaje de error si intenta eliminar una región que se utiliza actualmente en cualquier política (activa o inactiva).

4. Cuando haya terminado de realizar cambios, seleccione **Guardar**.

Ahora puede seleccionar estas regiones desde la sección Filtros avanzados en el paso 1 del asistente Crear regla ILM. Ver "[Utilice filtros avanzados en las reglas de ILM](#)".

Crear regla ILM

Utilice reglas ILM para administrar objetos

Para administrar objetos, debe crear un conjunto de reglas de administración del ciclo de vida de la información (ILM) y organizarlas en una política ILM.

Cada objeto ingerido en el sistema se evalúa en función de la política activa. Cuando una regla en la política coincide con los metadatos de un objeto, las instrucciones en la regla determinan qué acciones realiza StorageGRID para copiar y almacenar ese objeto.



Los metadatos de los objetos no son administrados por las reglas ILM. En cambio, los metadatos de los objetos se almacenan en una base de datos de Cassandra en lo que se conoce como un almacén de metadatos. Se mantienen automáticamente tres copias de los metadatos de los objetos en cada sitio para proteger los datos contra pérdidas.

Elementos de una regla ILM

Una regla ILM tiene 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 objetos especificadas en las instrucciones de ubicación de la regla.
- **Instrucciones de ubicación:** Las instrucciones de ubicación de una regla definen el número, tipo y ubicación de las copias de objetos. Cada regla puede incluir una secuencia de instrucciones de ubicación para cambiar la cantidad, el tipo y la ubicación de las copias de objetos a lo largo del tiempo. Cuando expira el plazo para una colocación, las instrucciones de la siguiente colocación se aplican automáticamente en la siguiente evaluación de ILM.
- **Comportamiento de ingesta:** el comportamiento de ingesta de una regla le permite elegir cómo se protegen los objetos filtrados por la regla a medida que se ingieren (cuando un cliente S3 guarda un objeto en la cuadrícula).

Filtrado de reglas ILM

Cuando se crea una regla ILM, se especifican filtros para identificar a qué objetos se aplica la regla.

En el caso más simple, 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) en una política ILM. La regla predeterminada proporciona instrucciones de almacenamiento para los objetos que no coinciden con los filtros de otra regla.

- Los filtros básicos le permiten aplicar diferentes reglas a grupos grandes y distintos de objetos. Estos

filtros le permiten aplicar una regla a cuentas de inquilinos específicos, depósitos S3 específicos o ambos.

Los filtros básicos le brindan una forma sencilla de aplicar diferentes reglas a un gran número de objetos. Por ejemplo, es posible que sea necesario almacenar los registros financieros de su empresa para cumplir con los requisitos reglamentarios, mientras que es posible que sea necesario almacenar los datos del departamento de marketing para facilitar las operaciones diarias. Después de crear cuentas de inquilinos independientes para cada departamento o después de segregar datos de los diferentes departamentos en grupos S3 separados, puede crear fácilmente una regla que se aplique a todos los registros financieros y una segunda regla que se aplique a todos los datos de marketing.

- Los filtros avanzados le brindan un control granular. Puede crear filtros para seleccionar objetos según las siguientes propiedades del objeto:
 - Tiempo de ingesta
 - Hora del último acceso
 - Todo o parte del nombre del objeto (Clave)
 - Restricción de ubicación (solo S3)
 - Tamaño del objeto
 - Metadatos del usuario
 - Etiqueta de objeto (solo S3)

Puede filtrar objetos según criterios muy específicos. Por ejemplo, los objetos almacenados por el departamento de imágenes de un hospital pueden usarse con frecuencia cuando tienen menos de 30 días y con poca frecuencia después, mientras que los objetos que contienen información de visitas de pacientes pueden necesitar copiarse al departamento de facturación en la sede central de la red de salud. Puede crear filtros que identifiquen cada tipo de objeto según el nombre del objeto, el tamaño, las etiquetas de objeto S3 o cualquier otro criterio relevante y luego crear reglas independientes para almacenar cada conjunto de objetos de forma adecuada.

Puede combinar filtros según sea necesario en una sola regla. Por ejemplo, el departamento de marketing podría querer almacenar archivos de imágenes grandes de forma diferente a sus registros de proveedores, mientras que el departamento de Recursos Humanos podría necesitar almacenar registros de personal en una geografía específica e información de políticas de forma centralizada. En este caso, puede crear reglas que filtren por cuenta de inquilino para segregar los registros de cada departamento, mientras utiliza filtros en cada regla para identificar el tipo específico de objetos a los que se aplica la regla.

Instrucciones de colocación de reglas ILM

Las instrucciones de ubicación determinan dónde, cuándo y cómo se almacenan los datos de los objetos. Una regla ILM puede incluir una o más instrucciones de ubicación. Cada instrucción de colocación se aplica a un único período de tiempo.

Al crear instrucciones de ubicación:

- Comienza especificando el tiempo de referencia, que determina cuándo comienzan las instrucciones de colocación. El tiempo de referencia puede ser cuando se ingiere un objeto, cuando se accede a un objeto, cuando un objeto versionado deja de ser actual o un tiempo definido por el usuario.
- A continuación, especifica cuándo se aplicará la ubicación, en relación con el tiempo de referencia. Por ejemplo, una ubicación podría comenzar el día 0 y continuar durante 365 días, en relación con el momento en que se ingirió el objeto.
- Por último, se especifica el tipo de copias (codificación de replicación o borrado) y la ubicación donde se almacenan las copias. Por ejemplo, es posible que desee almacenar dos copias replicadas en dos sitios

diferentes.

Cada regla puede definir múltiples ubicaciones para un solo período de tiempo y diferentes ubicaciones para diferentes períodos de tiempo.

- Para colocar objetos en varias ubicaciones durante un solo período de tiempo, seleccione **Agregar otro tipo o ubicación** para agregar más de una línea para ese período de tiempo.
- Para colocar objetos en diferentes ubicaciones en diferentes períodos de tiempo, seleccione **Agregar otro período de tiempo** para agregar el siguiente período de tiempo. Luego, especifique una o más líneas dentro del período de tiempo.

El ejemplo muestra dos instrucciones de ubicación en la página Definir ubicaciones del asistente Crear regla de ILM.

Time period and placements [Sort by start date](#)

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1 From Day 0 store for 365 days

Store objects by replicating 2 copies at Data Center 1, Data Center 2

and store objects by erasure coding using 6+3 EC scheme at all sites

[Add other type or location](#)

Time period 2 From Day 365 store forever

Store objects by replicating 2 copies at Data Center 3

[Add other type or location](#)

La primera instrucción de colocación ¹ tiene dos líneas para el primer año:

- La primera línea crea dos copias de objetos replicados en dos sitios de centros de datos.
- La segunda línea crea una copia con código de borrado 6+3 utilizando todos los sitios del centro de datos.

La segunda instrucción de colocación ² crea dos copias después de un año y conserva esas copias para siempre.

Al definir el conjunto de instrucciones de ubicación para una regla, debe asegurarse de que al menos una instrucción de ubicación comience en el día 0, que no haya espacios entre los períodos de tiempo que haya definido y que la instrucción de ubicación final continúe para siempre o hasta que ya no necesite copias de objetos.

A medida que expira cada período de tiempo de la regla, se aplican las instrucciones de ubicación de contenido para el siguiente período de tiempo. Se crean nuevas copias de objetos y se eliminan las copias innecesarias.

Comportamiento de ingesta de reglas ILM

El comportamiento de ingesta controla si las copias de objetos se colocan inmediatamente de acuerdo con las instrucciones de la regla, o si se realizan copias provisionales y las instrucciones de ubicación se aplican más tarde. Los siguientes comportamientos de ingesta están disponibles para las reglas ILM:

- **Equilibrado:** StorageGRID intenta realizar todas las copias especificadas en la regla ILM en la ingesta; si esto no es posible, se realizan copias provisionales y se devuelve el resultado exitoso al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.
- **Estricto:** Se deben realizar todas las copias especificadas en la regla ILM antes de devolver el resultado exitoso al cliente.
- **Confirmación dual:** StorageGRID realiza inmediatamente copias provisionales del objeto y devuelve el éxito al cliente. Cuando sea posible se realizarán las copias especificadas en la regla ILM.

Información relacionada

- ["Opciones de ingesta"](#)
- ["Ventajas, desventajas y limitaciones de las opciones de ingesta"](#)
- ["Cómo interactúan la consistencia y las reglas ILM para afectar la protección de datos"](#)

Ejemplo de regla ILM

A modo de ejemplo, una regla ILM podría especificar lo siguiente:

- Aplicar únicamente a los objetos pertenecientes al Inquilino A.
- Haga dos copias replicadas de esos objetos y almacene cada copia en un sitio diferente.
- Conserve las dos copias "para siempre", lo que significa que StorageGRID no las eliminará automáticamente. En su lugar, StorageGRID conservará estos objetos hasta que sean eliminados por una solicitud de eliminación del cliente o hasta que expire el ciclo de vida de un depósito.
- Utilice la opción Equilibrado para el comportamiento de ingesta: la instrucción de ubicación de dos sitios se aplica tan pronto como el Inquilino A guarda un objeto en StorageGRID, a menos que no sea posible realizar inmediatamente ambas copias requeridas.

Por ejemplo, si no se puede acceder al Sitio 2 cuando el Inquilino A guarda un objeto, StorageGRID hará dos copias provisionales en los Nodos de almacenamiento del Sitio 1. Tan pronto como el Sitio 2 esté disponible, StorageGRID hará la copia requerida en ese sitio.

Información relacionada

- ["¿Qué es un pool de almacenamiento?"](#)
- ["¿Qué es un pool de almacenamiento en la nube?"](#)

Acceda al asistente para crear una regla ILM

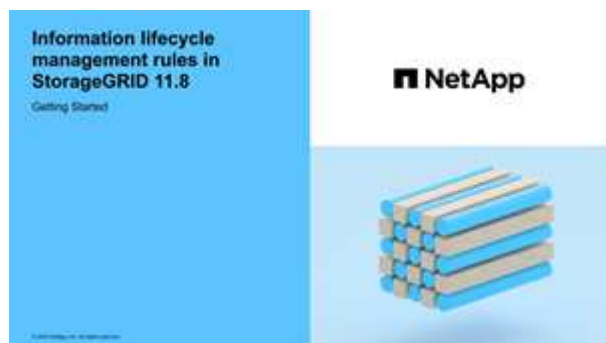
Las reglas ILM le permiten administrar la ubicación de los datos de los objetos a lo largo del tiempo. Para crear una regla ILM, utilice el asistente Crear una regla ILM.



Si desea crear la regla ILM predeterminada para una política, siga las ["Instrucciones para crear una regla ILM predeterminada"](#) en cambio.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Si desea especificar a qué cuentas de inquilino se aplica esta regla, tiene la ["Permiso de cuentas de inquilinos"](#) o conoce el ID de cuenta para cada cuenta.
- Si desea que la regla filtre objetos según los metadatos de la hora del último acceso, las actualizaciones de la hora del último acceso deben estar habilitadas por el bucket S3.
- Ha configurado todos los grupos de almacenamiento en la nube que planea utilizar. Ver ["Crear un grupo de almacenamiento en la nube"](#) .
- Estás familiarizado con el ["opciones de ingesta"](#) .
- Si necesita crear una regla compatible para usarla con S3 Object Lock, está familiarizado con el ["Requisitos para el bloqueo de objetos S3"](#) .
- Opcionalmente has visto el vídeo: ["Vídeo: Resumen de las reglas de ILM"](#) .



Acerca de esta tarea

Al crear reglas ILM:

- Tenga en cuenta la topología y las configuraciones de almacenamiento del sistema StorageGRID .
- Considere qué tipos de copias de objetos desea realizar (replicadas o codificadas por borrado) y la cantidad de copias de cada objeto que se requieren.
- Determinar qué tipos de metadatos de objetos se utilizan en las aplicaciones que se conectan al sistema StorageGRID . Las reglas ILM filtran objetos según sus metadatos.
- Considere dónde desea que se coloquen las copias de objetos a lo largo del tiempo.
- Decide qué opción de ingesta utilizar (equilibrada, estricta o confirmación dual).

Pasos

1. Seleccione **ILM > Reglas**.
2. Seleccione **Crear**. ["Paso 1 \(Ingresar detalles\)"](#) Aparece el asistente Crear una regla ILM.

Paso 1 de 3: Ingrese los detalles

El paso **Ingresar detalles** del asistente Crear una regla ILM le permite ingresar un nombre y una descripción para la regla y definir filtros para la regla.

Ingresar una descripción y definir filtros para la regla son opcionales.

Acerca de esta tarea

Al evaluar un objeto frente a un ["Regla 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 una o más cuentas de inquilino o nombres de depósito, o filtros avanzados, como el tamaño del objeto o los metadatos del usuario.

Pasos

1. Introduzca un nombre único para la regla en el campo **Nombre**.
2. Opcionalmente, ingrese una breve descripción de la regla en el campo **Descripción**.

Debes describir el propósito o función de la regla para poder reconocerla más adelante.

3. Opcionalmente, seleccione una o más cuentas de inquilino S3 a las que se aplica esta regla. Si esta regla se aplica a todos los inquilinos, deje este campo en blanco.

Si no tiene el permiso de acceso de raíz o el permiso de cuentas de inquilino, no podrá seleccionar inquilinos de la lista. En su lugar, ingrese el ID del inquilino o ingrese varios ID como una cadena delimitada por comas.

4. De manera opcional, especifique los buckets S3 a los que se aplica esta regla.

Si se selecciona **se aplica a todos los buckets** (predeterminado), la regla se aplica a todos los buckets S3.

5. Para los inquilinos de S3, seleccione opcionalmente **Sí** para aplicar la regla solo a versiones de objetos más antiguas en depósitos de S3 que tengan habilitada la función de control de versiones.

Si selecciona **Sí**, se seleccionará automáticamente "Hora no actual" para la hora de referencia en ["Paso 2 del asistente para crear una regla ILM"](#).



El tiempo no actual se aplica únicamente a objetos S3 en depósitos con control de versiones habilitado. Ver ["Operaciones en buckets, PutBucketVersioning"](#) y ["Administrar objetos con S3 Object Lock"](#).

Puede utilizar esta opción para reducir el impacto de almacenamiento de los objetos versionados filtrando las versiones de objetos no actuales. Ver ["Ejemplo 4: Reglas y políticas de ILM para objetos versionados de S3"](#).

6. Opcionalmente, seleccione **Agregar un filtro avanzado** para especificar filtros adicionales.

Si no configura el filtrado avanzado, la regla se aplica a todos los objetos que coincidan con los filtros básicos. Para obtener más información sobre el filtrado avanzado, consulte [Utilice filtros avanzados en las reglas de ILM](#) y [Especificar múltiples tipos y valores de metadatos](#).

7. Seleccione **Continuar**. ["Paso 2 \(Definir ubicaciones\)"](#) Aparece el asistente Crear una regla ILM.

Utilice filtros avanzados en las reglas de ILM

El filtrado avanzado le permite crear reglas ILM que se aplican solo a objetos específicos en función de sus metadatos. Cuando configura el filtrado avanzado para una regla, selecciona el tipo de metadatos que desea que coincidan, selecciona un operador y especifica un valor de metadatos. Cuando se evalúan objetos, la regla ILM se aplica solo a aquellos objetos que tienen metadatos que coinciden con el filtro avanzado.

La tabla muestra los tipos de metadatos que puede especificar en los filtros avanzados, los operadores que puede utilizar para cada tipo de metadatos y los valores de metadatos esperados.

Tipo de metadatos	Operadores compatibles	Valor de metadatos
Tiempo de ingesta	• es • no es • es antes • está en o antes • es despues • está en o después	Hora y fecha en que se ingirió el objeto. Nota: Para evitar problemas de recursos al activar una nueva política ILM, puede usar el filtro avanzado Tiempo de ingesta en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establezca el tiempo de ingesta para que sea mayor o igual al tiempo aproximado en que entrará en vigencia la nueva política para garantizar que los objetos existentes no se muevan innecesariamente.
Llave	• es igual • no es igual • contiene • no contiene • comienza con • no empieza con • termina con • no termina con	Toda o parte de una clave de objeto S3 única. Por ejemplo, es posible que desees hacer coincidir objetos que terminen con <code>.txt</code> o empezar con <code>test-object/</code>.
Hora del último acceso	• es • no es • es antes • está en o antes • es despues • está en o después	Hora y fecha en que se recuperó (leyó o vio) el objeto por última vez. Nota: Si planeas "utilizar la hora del último acceso" Como filtro avanzado, se deben habilitar las actualizaciones de la última hora de acceso para el bucket S3.
Restricción de ubicación (solo S3)	• es igual • no es igual	La región donde se creó un depósito S3. Utilice ILM > Regiones para definir las regiones que se muestran. Nota: Un valor de <code>us-east-1</code> coincidirá con objetos en depósitos creados en la región <code>us-east-1</code>, así como con objetos en depósitos que no tienen ninguna región especificada. Ver "Configurar regiones (opcional y solo S3)".

Tipo de metadatos	Operadores compatibles	Valor de metadatos
Tamaño del objeto	• es igual • no es igual • menos que • menor o igual a • más que • mayor o igual a	El tamaño del objeto. La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado.
Metadatos del usuario	• contiene • termina con • es igual • existe • comienza con • no contiene • no termina con • no es igual • no existe • no empieza con	Par clave-valor, donde Nombre de metadatos del usuario es la clave y Valor de metadatos es el valor. Por ejemplo, para filtrar objetos que tienen metadatos de usuario de <code>color=blue</code>, especificar <code>color</code> para Nombre de metadatos de usuario, <code>equals</code> para el operador, y <code>blue</code> para Valor de metadatos. Nota: Los nombres de metadatos del usuario no distinguen entre mayúsculas y minúsculas; los valores de metadatos del usuario sí distinguen entre mayúsculas y minúsculas.
Etiqueta de objeto (solo S3)	• contiene • termina con • es igual • existe • comienza con • no contiene • no termina con • no es igual • no existe • no empieza 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 <code>Image=True</code>, especificar <code>Image</code> para Nombre de etiqueta de objeto, <code>equals</code> para el operador, y <code>True</code> 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. Debes ingresar estos elementos exactamente como fueron definidos para el objeto.

Especificar múltiples tipos y valores de metadatos

Al definir el filtrado avanzado, puede especificar múltiples tipos de metadatos y múltiples valores de metadatos. Por ejemplo, si desea que una regla coincida con objetos entre 10 MB y 100 MB de tamaño, deberá seleccionar el tipo de metadatos **Tamaño del 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 menores o iguales a 100 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size	greater than or equal to	10	MB	✕
and				
Object size	less than or equal to	100	MB	✕

El uso de múltiples entradas le permite tener un control preciso sobre qué objetos coinciden. En el siguiente ejemplo, la regla se aplica a los objetos que tienen Marca A o Marca B como valor de los metadatos de usuario camera_type. Sin embargo, la regla sólo se aplica a aquellos objetos de la marca B que tengan un tamaño inferior a 10 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

User metadata	camera_type	equals	Brand A	✕

[Add another advanced filter](#)

or **Filter group 2** Objects with all of following metadata will be evaluated by this rule: ✕

User metadata	camera_type	equals	Brand B	✕
and				
Object size	less than or equal to	10	MB	✕

[Add another advanced filter](#)

Paso 2 de 3: Definir ubicaciones

El paso **Definir ubicaciones** del asistente Crear regla ILM le permite definir las instrucciones de ubicación que determinan durante cuánto tiempo se almacenan los objetos, el tipo de copias (replicadas o con código de borrado), la ubicación de almacenamiento y la cantidad de copias.



Las capturas de pantalla que se muestran son ejemplos. Los resultados pueden variar según la versión de StorageGRID .

Acerca de esta tarea

Una regla ILM puede incluir una o más instrucciones de ubicación. Cada instrucción de colocación se aplica a un único período de tiempo. Cuando se utiliza más de una instrucción, los períodos de tiempo deben ser contiguos y al menos una instrucción debe comenzar el día 0. Las instrucciones pueden continuar indefinidamente o hasta que ya no necesite ninguna copia de objeto.

Cada instrucción de ubicación puede tener varias líneas si desea crear diferentes tipos de copias o utilizar diferentes ubicaciones durante ese período de tiempo.

En este ejemplo, la regla ILM almacena una copia replicada en el Sitio 1 y una copia replicada en el Sitio 2 durante el primer año. Después de un año, se realiza una copia con código de borrado 2+1 y se guarda en un solo sitio.

Pasos

1. Para **Hora de referencia**, seleccione el tipo de hora que se utilizará al calcular la hora de inicio de una instrucción de ubicación.

Opción	Descripción
Tiempo de ingesta	El momento en que se ingirió el objeto.
Hora del último acceso	La hora en que se recuperó el objeto por última vez (se leyó o se vio). Para utilizar esta opción, las actualizaciones de la hora del último acceso deben estar habilitadas para el bucket S3. Consulte "Utilice la hora del último acceso en las reglas de ILM" .
Hora de creación definida por el usuario	Un tiempo especificado en metadatos definidos por el usuario.
Tiempo no actual	"Hora no actual" se selecciona automáticamente si seleccionó Sí para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en buckets S3 con control de versiones habilitado)?" en "Paso 1 del asistente para crear una regla de ILM" .

Si desea crear una regla *compatible*, debe seleccionar **Tiempo de ingesta**. Consulte ["Administrar objetos con S3 Object Lock"](#) .

2. En la sección **Período de tiempo y ubicaciones**, ingrese una hora 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 (*Desde el día 0 almacenar durante 365 días*). Al menos una instrucción debe comenzar en el día 0.

3. Si desea crear copias replicadas:

- a. En la lista desplegable **Almacenar objetos por**, seleccione **replicando**.
- b. Seleccione el número de copias que desea realizar.

Aparece una advertencia si cambia el número de copias a 1. Una regla ILM que crea solo una copia replicada por cada período de tiempo pone los datos en riesgo de pérdida permanente. Consulte ["Por qué no debería utilizar la replicación de copia única"](#) .

Para evitar el riesgo, realice una o más de las siguientes acciones:

- Aumentar el número de copias para el período de tiempo.
- Agregue copias a otros grupos de almacenamiento o a un grupo de almacenamiento en la nube.
- Seleccione **codificación de borrado** en lugar de **replicación**.

Puede ignorar esta advertencia de forma segura si esta regla ya crea múltiples copias para todos los períodos de tiempo.

- c. En el campo **copias en**, seleccione los grupos de almacenamiento que desea agregar.

Si especifica solo un grupo de almacenamiento, tenga en cuenta que StorageGRID solo puede

almacenar una copia replicada de un objeto en cualquier nodo de almacenamiento determinado. Si su red incluye tres nodos de almacenamiento y selecciona 4 como número de copias, solo se realizarán tres copias: una copia para cada nodo de almacenamiento.

La alerta **Colocación ILM inalcanzable** se activa para indicar que la regla ILM no se pudo aplicar por completo.

Si especifica más de un grupo de almacenamiento, tenga en cuenta estas reglas:

- La cantidad de copias no puede ser mayor que la cantidad de grupos de almacenamiento.
- Si la cantidad de copias es igual a la cantidad de grupos de almacenamiento, se almacena una copia del objeto en cada grupo de almacenamiento.
- Si la cantidad de copias es menor que la cantidad de grupos de almacenamiento, se almacena una copia en el sitio de ingesta y luego el sistema distribuye las copias restantes para mantener equilibrado el uso del disco entre los grupos y, al mismo tiempo, garantizar que ningún sitio obtenga más de una copia de un objeto.
- Si los grupos de almacenamiento se superponen (contienen los mismos nodos de almacenamiento), todas las copias del objeto podrían guardarse en un solo sitio. Por este motivo, no especifique el grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores) y otro grupo de almacenamiento.

4. Si desea crear una copia con código de borrado:

a. En la lista desplegable **Almacenar objetos por**, seleccione **codificación de borrado**.



La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado.

b. Si no agregó un filtro de tamaño de objeto para un valor mayor a 200 KB, seleccione **Anterior** para regresar al Paso 1. Luego, seleccione **Agregar un filtro avanzado** y configure un filtro de **Tamaño de objeto** en cualquier valor mayor a 200 KB.

c. Seleccione el grupo de almacenamiento que desea agregar y el esquema de codificación de borrado que desea utilizar.

La ubicación de almacenamiento de una copia con código de borrado incluye el nombre del esquema de codificación de borrado, seguido del nombre del grupo de almacenamiento.

Los esquemas de codificación de borrado disponibles están limitados por la cantidad de nodos de almacenamiento en el grupo de almacenamiento que seleccione. A Recommended La insignia aparece junto a los esquemas que proporcionan el "[La mejor protección o la menor sobrecarga de almacenamiento](#)".

5. Opcionalmente:

- a. Seleccione **Agregar otro tipo o ubicación** para crear copias adicionales en diferentes ubicaciones.
- b. Seleccione **Agregar otro período de tiempo** para agregar diferentes períodos de tiempo.



Las eliminaciones de objetos se producen según las siguientes configuraciones:

- Los objetos se eliminan automáticamente al final del período de tiempo final, a menos que otro período de tiempo finalice **para siempre**.
- Dependiendo de "[Configuración del período de retención de depósitos e inquilinos](#)" Es posible que los objetos no se eliminen incluso si finaliza el período de retención de ILM.

6. Si desea almacenar objetos en un grupo de almacenamiento en la nube:

- a. En la lista desplegable **Almacenar objetos por**, seleccione **replicando**.
- b. Seleccione el campo **copias en** y luego seleccione un grupo de almacenamiento en la nube.

Al utilizar grupos de almacenamiento en la nube, tenga en cuenta estas reglas:

- No puede seleccionar más de un grupo de almacenamiento en la nube en una sola instrucción de ubicación. De manera similar, no es posible seleccionar un grupo de almacenamiento en la nube y un grupo de almacenamiento en la misma instrucción de ubicación.
- Solo puedes almacenar una copia de un objeto en un grupo de almacenamiento en la nube determinado. Aparece un mensaje de error si configura **Copias** en 2 o más.
- No es posible almacenar más de una copia de objeto en ningún grupo de almacenamiento en la nube al mismo tiempo. Aparece un mensaje de error si varias ubicaciones que utilizan un grupo de almacenamiento en la nube tienen fechas superpuestas o si varias líneas en la misma ubicación utilizan un grupo de almacenamiento en la nube.
- Puede almacenar un objeto en un grupo de almacenamiento en la nube al mismo tiempo que ese objeto se almacena como copias replicadas o con código de borrado en StorageGRID. Sin embargo, debe incluir más de una línea en la instrucción de ubicación para el período de tiempo, de modo que pueda especificar la cantidad y los tipos de copias para cada ubicación.

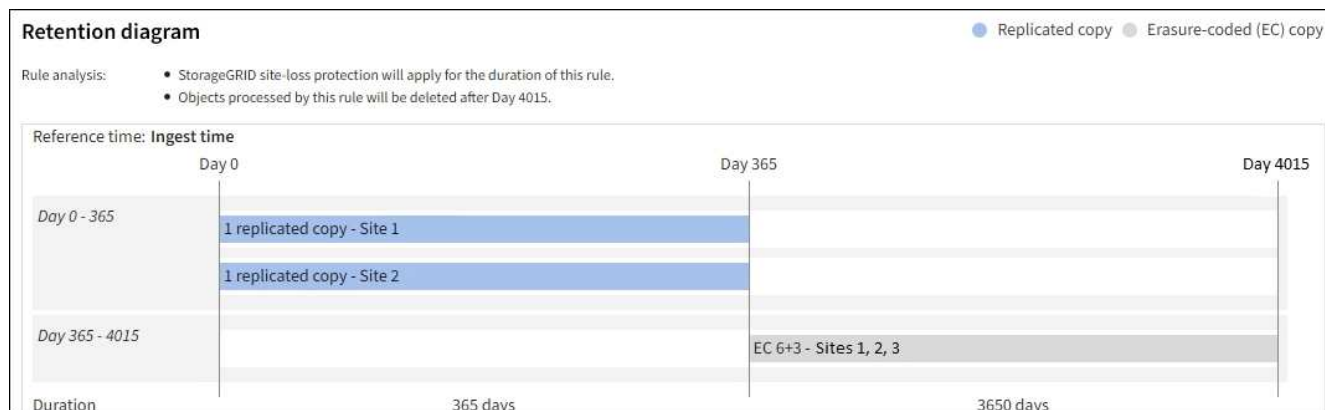
7. En el diagrama de retención, confirme sus instrucciones de ubicación.

En este ejemplo, la regla ILM almacena una copia replicada en el Sitio 1 y una copia replicada en el Sitio 2 durante el primer año. Después de un año y durante 10 años más, se guardará una copia con código de borrado 6+3 en tres sitios. Después de 11 años en total, los objetos se eliminarán de StorageGRID.

La sección de análisis de reglas del diagrama de retención establece:

- La protección contra pérdida de sitios de StorageGRID se aplicará mientras dure esta regla.
- Los objetos procesados por esta regla se eliminarán después del día 4015.

Consulte "[Habilitar la protección contra pérdida del sitio.](#)"



8. Seleccione **Continuar**. "[Paso 3 \(Seleccionar el comportamiento de ingesta\)](#)" Aparece el asistente Crear una regla ILM.

Utilice la hora del último acceso en las reglas de ILM

Puede utilizar la hora del último acceso como hora de referencia en una regla ILM. Por ejemplo, es posible que desee dejar objetos que se hayan visto en los últimos tres meses en nodos de almacenamiento locales, mientras que mueve objetos que no se hayan visto recientemente a una ubicación externa. También puede utilizar Hora del último acceso como filtro avanzado si desea que una regla ILM se aplique solo a los objetos a los que se accedió por última vez en una fecha específica.

Acerca de esta tarea

Antes de utilizar la hora del último acceso en una regla ILM, revise las siguientes consideraciones:

- Al utilizar la hora del último acceso como tiempo de referencia, tenga en cuenta que cambiar la hora del último acceso de un objeto no activa una evaluación ILM inmediata. En su lugar, se evalúan las ubicaciones del objeto y el objeto se mueve según sea necesario cuando ILM en segundo plano evalúa el objeto. Esto podría tomar dos semanas o más después de acceder al objeto.

Tenga en cuenta esta latencia al crear reglas ILM basadas en el último tiempo de acceso y evite ubicaciones que utilicen períodos de tiempo cortos (menos de un mes).

- Al utilizar la Hora del último acceso como filtro avanzado o como hora de referencia, debe habilitar las actualizaciones de la Hora del último acceso para los buckets S3. Puedes utilizar el "[Administrador de inquilinos](#)" o el "[API de gestión de inquilinos](#)".



Las actualizaciones del último tiempo de acceso están deshabilitadas de manera predeterminada para los buckets S3.



Tenga en cuenta que habilitar actualizaciones de la última hora de 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 nuevas marcas de tiempo cada vez que se recuperan los objetos.

La siguiente tabla resume si la hora del último acceso se actualiza para todos los objetos en el depósito para diferentes tipos de solicitudes.

Tipo de solicitud	Si la hora del último acceso se actualiza cuando las actualizaciones de la hora del último acceso están deshabilitadas	Si la hora del último acceso se actualiza cuando se habilitan las actualizaciones de la hora del último 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
Solicitud para copiar un objeto de un depósito a otro	• No, para la copia fuente • Sí, para la copia de destino	• Sí, para la copia fuente • Sí, para la copia de destino
Solicitud para completar una carga de varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Paso 3 de 3: Seleccionar el comportamiento de ingesta

El paso **Seleccionar comportamiento de ingesta** del asistente Crear regla de ILM le permite elegir cómo se protegen los objetos filtrados por esta regla a medida que se ingieren.

Acerca de esta tarea

StorageGRID puede hacer copias provisionales y poner en cola los objetos para una evaluación ILM posterior, o puede hacer copias para cumplir con las instrucciones de ubicación de la regla de inmediato.

Pasos

1. Seleccione el ["comportamiento de ingestión"](#) Para utilizar.

Para obtener más información, consulte ["Ventajas, desventajas y limitaciones de las opciones de ingesta"](#).



No puedes usar la opción Equilibrado o Estricto si la regla utiliza una de estas ubicaciones:

- Un grupo de almacenamiento en la nube en el día 0
- Un grupo de almacenamiento en la nube cuando la regla utiliza un tiempo de creación definido por el usuario como tiempo de referencia

Ver ["Ejemplo 5: Reglas y políticas de ILM para el comportamiento de ingesta estricto"](#).

2. Seleccione **Crear**.

Se crea la regla ILM. La regla no se activa hasta que se agrega a una ["Política de ILM"](#) y esa política se activa.

Para ver los detalles de la regla, seleccione el nombre de la regla en la página de reglas de ILM.

Crear una regla ILM predeterminada

Antes de crear una política ILM, debe crear una regla predeterminada para colocar cualquier objeto que no coincida con otra regla en la política. La regla predeterminada no puede utilizar ningún filtro. Debe aplicarse a todos los inquilinos, todos los depósitos y todas las versiones de objetos.

Antes de empezar

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

Acerca de esta tarea

La regla predeterminada es la última regla que se evalúa en una política ILM, por lo que no puede usar ningún filtro. Las instrucciones de ubicación de la regla predeterminada se aplican a cualquier objeto que no coincida con otra regla en la política.

En esta política de ejemplo, la primera regla se aplica solo a los objetos que pertenecen a test-tenant-1. La regla predeterminada, que es la última, se aplica a los objetos que pertenecen a todas las demás cuentas de inquilino.

Proposed policy name

Example ILM policy

Reason for change

Example

Manage rules

1. Select the rules you want to add to the policy.

2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	↕ EC for test-tenant-1	Tenant is test-tenant-1
Default	Default rule	—

Al crear la regla predeterminada, tenga en cuenta estos requisitos:

- La regla predeterminada se colocará automáticamente como última regla cuando la agregue a una política.
- La regla predeterminada no puede utilizar ningún filtro básico o avanzado.
- La regla predeterminada debe aplicarse a todas las versiones del objeto.
- La regla predeterminada debería 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 utilizar un filtro avanzado para evitar que se codifiquen por borrado objetos más pequeños.

- En general, la regla predeterminada debería conservar los objetos para siempre.
- Si está utilizando (o planea habilitar) la configuración global de bloqueo de objetos S3, la regla predeterminada debe ser compatible.

Pasos

1. Seleccione **ILM > Reglas**.
2. Seleccione **Crear**.

Aparece el paso 1 (Ingresar detalles) del asistente Crear regla ILM.

3. Introduzca un nombre único para la regla en el campo **Nombre de la regla**.
4. Opcionalmente, ingrese una breve descripción de la regla en el campo **Descripción**.
5. Deje el campo **Cuentas de inquilinos** en blanco.

La regla predeterminada debe aplicarse a todas las cuentas de inquilinos.

6. Deje la selección desplegable del nombre del depósito como **se aplica a todos los depósitos**.

La regla predeterminada debe aplicarse a todos los buckets S3.

7. Mantenga la respuesta predeterminada, **No**, para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en depósitos S3 con control de versiones habilitado)?"
8. No agregue filtros avanzados.

La regla predeterminada no puede especificar ningún filtro.

9. Seleccione **Siguiente**.

Aparece el paso 2 (Definir ubicaciones).

10. Para el tiempo de referencia, seleccione cualquier opción.

Si mantuvo la respuesta predeterminada, **No**, para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores?" La hora no actual no se incluirá en la lista desplegable. La regla predeterminada debe aplicarse a todas las versiones del objeto.

11. Especifique las instrucciones de ubicación para la regla predeterminada.
 - La regla predeterminada debería conservar los objetos para siempre. Aparece una advertencia cuando se activa una nueva política si la regla predeterminada no retiene los objetos para siempre. Debes confirmar que este es el comportamiento que esperas.
 - La regla predeterminada debería crear copias replicadas.



No utilice una regla que cree copias con código de borrado como regla predeterminada para una política. Las reglas de codificación de borrado deben incluir el filtro avanzado **Tamaño de objeto (MB) mayor a 200 KB** para evitar que se codifiquen objetos más pequeños.

- Si está utilizando (o planea habilitar) la configuración global de Bloqueo de objetos S3, la regla predeterminada debe ser compatible:
 - Debe crear al menos dos copias del objeto replicado o una copia con código de borrado.
 - Estas copias deben existir en los nodos de almacenamiento durante toda la duración de cada línea en las instrucciones de ubicación.
 - Las copias de objetos no se pueden guardar en un grupo de almacenamiento en la nube.
 - Al menos una línea de las instrucciones de ubicación debe comenzar en el día 0, utilizando el tiempo de ingesta como tiempo de referencia.
 - Al menos una línea de las instrucciones de colocación debe ser "para siempre".

12. Mire el diagrama de retención para confirmar sus instrucciones de ubicación.

13. Seleccione **Continuar**.

Aparece el paso 3 (Seleccionar comportamiento de ingesta).

14. Seleccione la opción de ingesta que desea utilizar y seleccione **Crear**.

Administrar políticas de ILM

Utilice las políticas de ILM

Una política de gestión del ciclo de vida de la información (ILM) es un conjunto ordenado de reglas ILM que determina cómo el sistema StorageGRID gestiona los datos de los objetos a lo largo del tiempo.



Una política ILM que se haya configurado incorrectamente puede provocar una pérdida irreparable de datos. Antes de activar una política ILM, revise cuidadosamente la política ILM y sus reglas ILM y luego simule la política ILM. Confirme siempre que la política ILM funcionará según lo previsto.

Política ILM predeterminada

Cuando instala StorageGRID y agrega sitios, se crea automáticamente una política ILM predeterminada, de la siguiente manera:

- Si su cuadrícula contiene un sitio, la política predeterminada contiene una regla predeterminada que replica dos copias de cada objeto en ese sitio.
- Si su cuadrícula contiene más de un sitio, la regla predeterminada replica una copia de cada objeto en cada sitio.

Si la política predeterminada no cumple con sus requisitos de almacenamiento, puede crear sus propias reglas y políticas. Ver ["Crear una regla ILM"](#) y ["Crear una política ILM"](#).

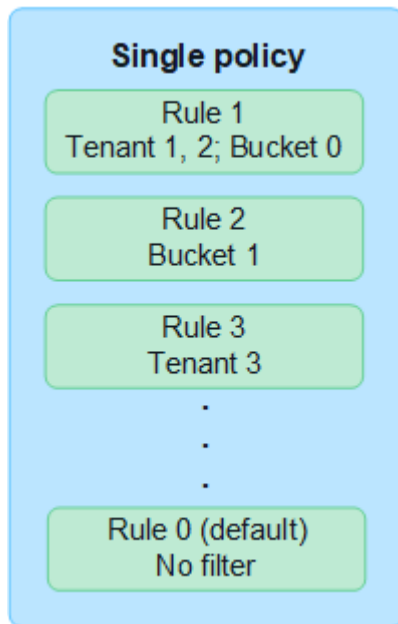
¿Una o varias políticas ILM activas?

Puede tener una o más políticas ILM activas a la vez.

Una política

Si su red utilizará un esquema de protección de datos simple con pocas reglas específicas para cada inquilino y cada depósito, utilice una única política ILM activa. Las reglas de ILM pueden contener filtros para

administrar diferentes grupos o inquilinos.



Cuando solo tiene una política y cambian los requisitos de un inquilino, debe crear una nueva política ILM o clonar la política existente para aplicar los cambios, simular y luego activar la nueva política ILM. Los cambios en la política de ILM podrían generar movimientos de objetos que podrían demorar muchos días y causar latencia del sistema.

Múltiples políticas

Para brindar diferentes opciones de calidad de servicio a los inquilinos, puede tener más de una política activa a la vez. Cada política puede administrar inquilinos, depósitos S3 y objetos específicos. Cuando se aplica o cambia una política para un conjunto específico de inquilinos u objetos, las políticas aplicadas a otros inquilinos y objetos no se ven afectadas.

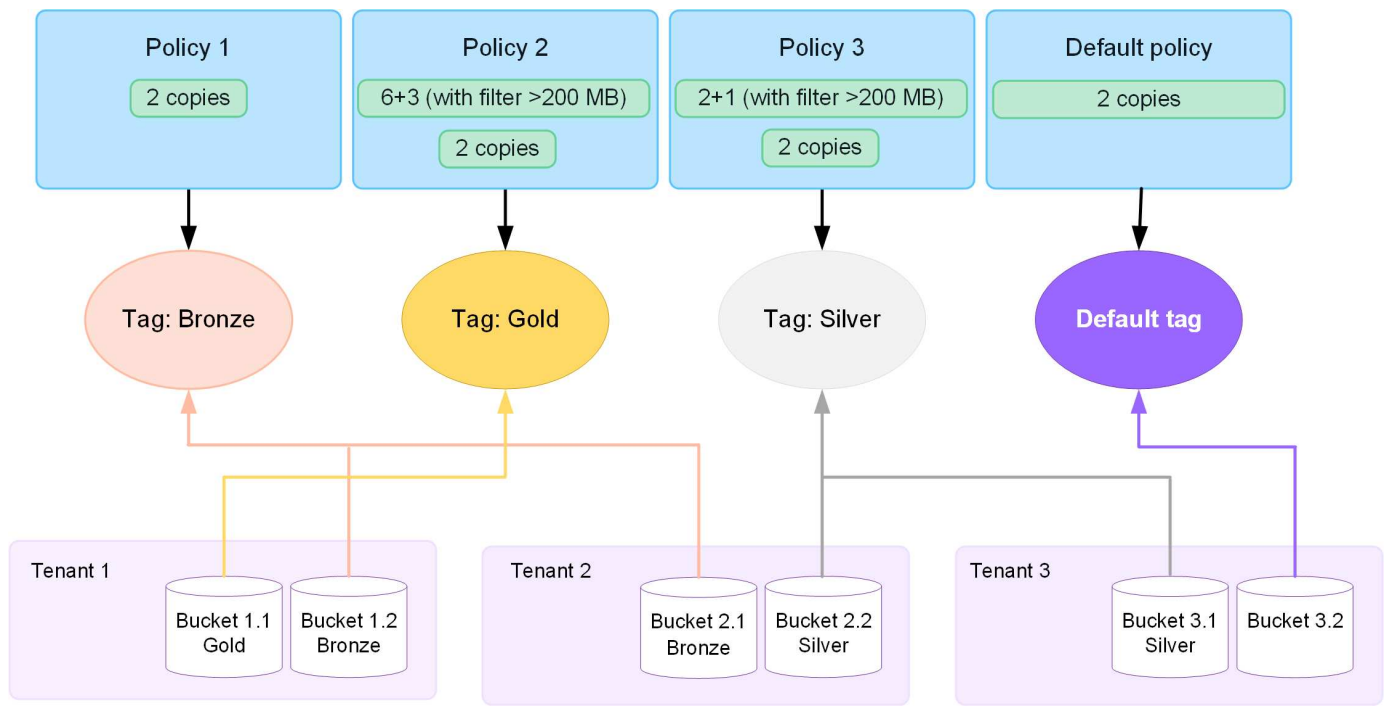
Etiquetas de política de ILM

Si desea permitir que los inquilinos cambien fácilmente entre múltiples políticas de protección de datos por depósito, utilice múltiples políticas ILM con *etiquetas de política ILM*. Asigna cada política de ILM a una etiqueta y luego los inquilinos etiquetan un depósito para aplicar la política a ese depósito. Puede configurar etiquetas de política ILM solo en depósitos S3.

Por ejemplo, podría tener tres etiquetas denominadas Oro, Plata y Bronce. Puede asignar una política ILM a cada etiqueta, en función de cuánto tiempo y dónde esa política almacena los objetos. Los inquilinos pueden elegir qué política utilizar etiquetando sus áreas. Un depósito etiquetado como Oro es administrado por la política Oro y recibe el nivel Oro de protección de datos y rendimiento.

Etiqueta de política ILM predeterminada

Se crea automáticamente una etiqueta de política ILM predeterminada cuando instala StorageGRID. Cada cuadrícula debe tener una política activa asignada a la etiqueta Predeterminada. La política predeterminada se aplica a cualquier depósito S3 sin etiquetar.



¿Cómo evalúa una política ILM los objetos?

Una política ILM activa controla la ubicación, la duración y la protección de datos de los objetos.

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

1. Si los filtros de la primera regla de la política coinciden con un objeto, el objeto se ingiere de acuerdo con el comportamiento de ingesta de esa regla y se almacena de acuerdo con las instrucciones de ubicación de esa regla.
2. Si los filtros de la primera regla no coinciden con el objeto, este se evalúa en relación con cada regla posterior de la política hasta que se encuentre una coincidencia.
3. Si ninguna regla coincide con un objeto, se aplican el comportamiento de ingesta y las instrucciones de ubicación de la regla predeterminada en la política. La regla predeterminada es la última regla de una política. La regla predeterminada debe aplicarse a todos los inquilinos, todos los depósitos S3 y todas las versiones de objetos, y no puede usar ningún filtro avanzado.

Ejemplo de política ILM

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

- **Regla 1: Copias replicadas para el inquilino A**

- Empareja todos los objetos que pertenecen al inquilino A.
- Almacene estos objetos como tres copias replicadas en tres sitios.
- Los objetos que pertenecen a otros inquilinos no coinciden con la Regla 1, por lo que se evalúan según la Regla 2.

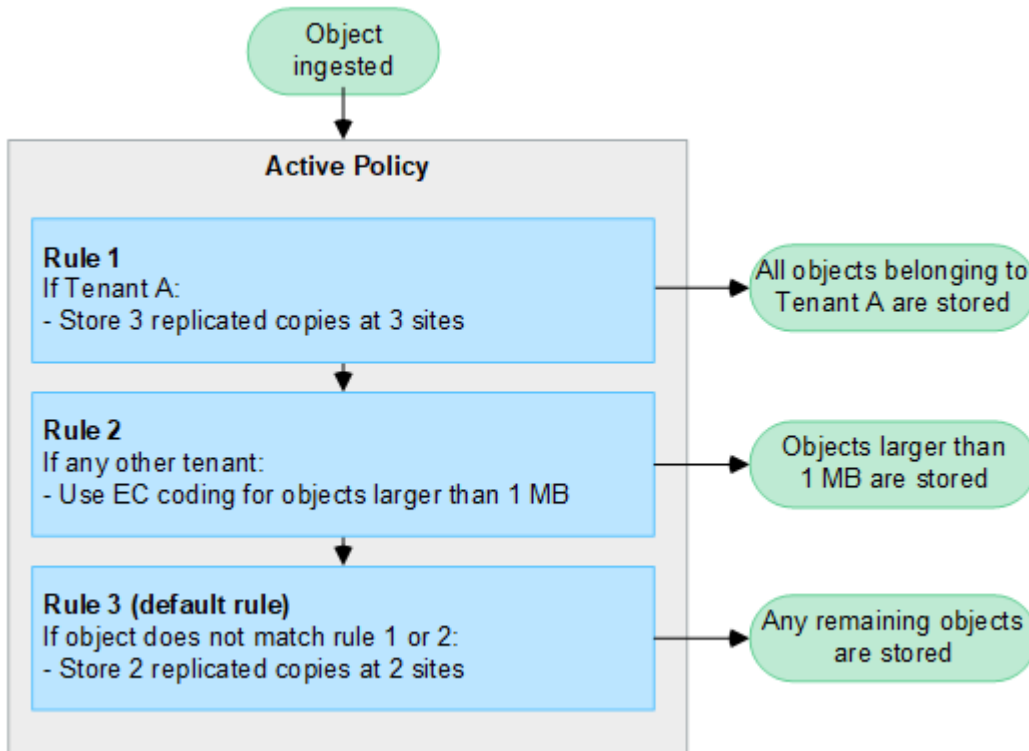
- **Regla 2: Codificación de borrado para objetos mayores a 1 MB**

- Coincide con todos los objetos de otros inquilinos, pero solo si son mayores a 1 MB. Estos objetos más grandes se almacenan utilizando codificación de borrado 6+3 en tres sitios.
- No coincide con objetos de 1 MB o más pequeños, por lo que estos objetos se evalúan según la Regla

3.

- **Regla 3: 2 copias, 2 centros de datos** (predeterminado)

- Es la última regla predeterminada de la política. No utiliza filtros.
- Realice dos copias replicadas de todos los objetos que no coincidan con la Regla 1 o la Regla 2 (objetos que no pertenecen al Inquilino A y que tienen 1 MB o menos).



¿Qué son las políticas activas e inactivas?

Cada sistema StorageGRID debe tener al menos una política ILM activa. Si desea tener más de una política ILM activa, cree etiquetas de política ILM y asigne una política a cada etiqueta. Luego, los inquilinos aplican etiquetas a los depósitos S3. La política predeterminada se aplica a todos los objetos en depósitos que no tienen una etiqueta de política asignada.

Cuando crea por primera vez una política ILM, selecciona una o más reglas ILM y las organiza en un orden específico. Después de haber simulado la política para confirmar su comportamiento, actívela.

Cuando activa una política ILM, StorageGRID utiliza esa política para administrar todos los objetos, incluidos los objetos existentes y los objetos recientemente ingeridos. Los objetos existentes podrían trasladarse a nuevas ubicaciones cuando se implementen las reglas ILM en la nueva política.

Si activa más de una política ILM a la vez y los inquilinos aplican etiquetas de política a los depósitos S3, los objetos en cada depósito se administran de acuerdo con la política asignada a la etiqueta.

Un sistema StorageGRID rastrea el historial de políticas que se han activado o desactivado.

Consideraciones para la creación de una política ILM

- Utilice únicamente la política proporcionada por el sistema (política Baseline 2 copias) en los sistemas de prueba. Para StorageGRID 11.6 y versiones anteriores, la regla Hacer 2 copias en esta política utiliza el grupo de almacenamiento Todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el

mismo sitio.



El grupo de almacenamiento Todos los nodos de almacenamiento se crea automáticamente durante la instalación de StorageGRID 11.6 y versiones anteriores. Si actualiza a una versión posterior de StorageGRID, el grupo de todos los nodos de almacenamiento seguirá existiendo. Si instala StorageGRID 11.7 o posterior como una instalación nueva, no se crea el grupo Todos los nodos de almacenamiento.

- Al diseñar una nueva política, tenga en cuenta todos los diferentes tipos de objetos que podrían incorporarse a su red. Asegúrese de que la política incluya reglas para hacer coincidir y colocar estos objetos según sea necesario.
- Mantenga la política de ILM lo más simple posible. Esto evita situaciones potencialmente peligrosas en las que los datos de los objetos no están protegidos como se espera cuando se realizan cambios en el sistema StorageGRID a lo largo del tiempo.
- Asegúrese de que las reglas de la política estén en el orden correcto. Cuando se activa la política, los objetos nuevos y existentes se evalúan mediante las reglas en el orden enumerado, comenzando desde arriba. Por ejemplo, si la primera regla de una política coincide con un objeto, ese objeto no será evaluado por ninguna otra regla.
- La última regla en cada política ILM es la regla ILM predeterminada, que no puede usar ningún filtro. Si un objeto no ha sido emparejado con otra regla, la regla predeterminada controla dónde se coloca ese objeto y durante cuánto tiempo se conserva.
- Antes de activar una nueva política, revise cualquier cambio que la política esté realizando en la ubicación de los objetos existentes. Cambiar la ubicación de un objeto existente puede generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.

Crear políticas ILM

Cree una o más políticas ILM para satisfacer sus requisitos de calidad de servicio.

Tener una política ILM activa le permite aplicar las mismas reglas ILM a todos los inquilinos y grupos.

Tener múltiples políticas ILM activas le permite aplicar las reglas ILM adecuadas a inquilinos y grupos específicos para cumplir con múltiples requisitos de calidad de servicio.

Crear una política ILM

Acerca de esta tarea

Antes de crear su propia política, verifique que la [política ILM predeterminada](#) no cumple con sus requisitos de almacenamiento.



Utilice únicamente las políticas proporcionadas por el sistema, 2 copias de la política (para redes de un sitio) o 1 copia por sitio (para redes de varios sitios), en los sistemas de prueba. Para StorageGRID 11.6 y versiones anteriores, la regla predeterminada en esta política utiliza el grupo de almacenamiento Todos los nodos de almacenamiento, que contiene todos los sitios. Si su sistema StorageGRID tiene más de un sitio, es posible que se coloquen dos copias de un objeto en el mismo sitio.



Si el ["Se ha habilitado la configuración global de bloqueo de objetos S3"](#), debe asegurarse de que la política ILM cumpla con los requisitos de los depósitos que tienen habilitado el bloqueo de objetos S3. En esta sección, siga las instrucciones que mencionan tener habilitado el bloqueo de objetos S3.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["permisos de acceso necesarios"](#) .
- Tienes ["creó reglas ILM"](#) dependiendo de si el bloqueo de objetos S3 está habilitado.

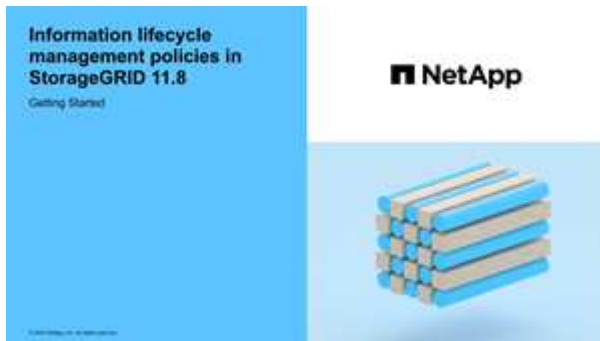
Bloqueo de objetos S3 no habilitado

- Tienes ["creó las reglas de ILM"](#) desea agregar a la política. Según sea necesario, puede guardar una política, crear reglas adicionales y luego editar la política para agregar las nuevas reglas.
- Tienes ["creó una regla ILM predeterminada"](#) que no contiene ningún filtro.

Bloqueo de objetos S3 habilitado

- El ["La configuración global de bloqueo de objetos S3 ya está habilitada"](#) para el sistema StorageGRID .
- Tienes ["creó las reglas ILM compatibles y no compatibles"](#) desea agregar a la política. Según sea necesario, puede guardar una política, crear reglas adicionales y luego editar la política para agregar las nuevas reglas.
- Tienes ["creó una regla ILM predeterminada"](#) para la política que se cumple.

- Opcionalmente has visto el vídeo: ["Vídeo: Resumen de las políticas de ILM"](#)



Consulte también ["Utilice las políticas de ILM"](#) .

Pasos

1. Seleccione **ILM > Políticas**.

Si la configuración global de Bloqueo de objetos S3 está habilitada, la página de políticas de ILM indica qué reglas de ILM son compatibles.

2. Determine cómo desea crear la política ILM.

Crear nueva política

- a. Seleccione **Crear política**.

Clonar política existente

- a. Seleccione la casilla de verificación de la política con la que desea comenzar y luego seleccione **Clonar**.

Editar la política existente

- a. Si una política está inactiva, puedes editarla. Seleccione la casilla de verificación de la política inactiva con la que desea comenzar y luego seleccione **Editar**.

3. En el campo **Nombre de la política**, ingrese un nombre único para la política.
4. Opcionalmente, en el campo **Motivo del cambio**, ingrese el motivo por el cual está creando una nueva política.
5. Para agregar reglas a la política, seleccione **Seleccionar reglas**. Seleccione un nombre de regla para ver la configuración de esa regla.

Si está clonando una política:

- Se seleccionan las reglas utilizadas por la política que estás clonando.
- Si la política que está clonando utilizó reglas sin filtros que no eran la regla predeterminada, se le solicitará que elimine todas esas reglas excepto una.
- Si la regla predeterminada utilizó un filtro, se le solicitará que seleccione una nueva regla predeterminada.
- Si la regla predeterminada no fue la última regla, puede mover la regla al final de la nueva política.

Bloqueo de objetos S3 no habilitado

- a. Seleccione una regla predeterminada para la política. Para crear una nueva regla predeterminada, seleccione **Página de reglas ILM**.

La regla predeterminada se aplica a cualquier objeto que no coincida con otra regla de la política. La regla predeterminada no puede usar ningún filtro y siempre se evalúa en último lugar.



No utilice la regla Hacer 2 copias como regla predeterminada para una política. La regla Hacer 2 copias utiliza un único grupo 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.

Bloqueo de objetos S3 habilitado

- a. Seleccione una regla predeterminada para la política. Para crear una nueva regla predeterminada, seleccione **Página de reglas ILM**.

La lista de reglas contiene solo las reglas que cumplen los requisitos y no utilizan ningún filtro.



No utilice la regla Hacer 2 copias como regla predeterminada para una política. La regla Hacer 2 copias utiliza un único grupo de almacenamiento, Todos los nodos de almacenamiento, que contiene todos los sitios. Si utiliza esta regla, es posible que se coloquen varias copias de un objeto en el mismo sitio.

- b. Si necesita una regla "predeterminada" diferente para los objetos en depósitos S3 no compatibles, seleccione **Incluir una regla sin filtros para depósitos S3 no compatibles** y seleccione una regla no compatible que no use un filtro.

Por ejemplo, es posible que desee utilizar un grupo de almacenamiento en la nube para almacenar objetos en depósitos que no tengan habilitado el bloqueo de objetos S3.



Solo puede seleccionar una regla no compatible que no utilice un filtro.

Consulte también ["Ejemplo 7: Política ILM compatible con el bloqueo de objetos S3"](#) .

6. Cuando haya terminado de seleccionar la regla predeterminada, seleccione **Continuar**.
7. Para el paso Otras reglas, seleccione cualquier otra regla que desee agregar a la política. Estas reglas utilizan al menos un filtro (cuenta de inquilino, nombre del depósito, filtro avanzado o tiempo de referencia no actual). Luego seleccione **Seleccionar**.

La ventana Crear una política ahora enumera las reglas que seleccionó. La regla predeterminada está al final, con las demás reglas encima.

Si el bloqueo de objetos S3 está habilitado y también seleccionó una regla "predeterminada" no compatible, esa regla se agrega como la segunda a la última regla en la política.



Aparece una advertencia si alguna regla no retiene los objetos para siempre. Cuando activa esta política, debe confirmar que desea que StorageGRID elimine objetos cuando transcurran las instrucciones de ubicación de la regla predeterminada (a menos que un ciclo de vida de depósito conserve los objetos durante un período de tiempo más prolongado).

8. Arrastre las filas de las reglas no predeterminadas para determinar el orden en que se evaluarán estas reglas.

No puedes mover la regla predeterminada. Si el bloqueo de objetos S3 está habilitado, tampoco podrá mover la regla "predeterminada" no compatible si se seleccionó una.



Debes confirmar que las reglas de ILM estén en el orden correcto. Cuando se activa la política, los objetos nuevos y existentes se evalúan mediante las reglas en el orden enumerado, comenzando desde arriba.

9. Según sea necesario, seleccione **Seleccionar reglas** para agregar o eliminar reglas.
10. Cuando haya terminado, seleccione **Guardar**.
11. Repita estos pasos para crear políticas ILM adicionales.
12. [Simular una política ILM](#) . Siempre debe simular una política antes de activarla para asegurarse de que funcione como se espera.

Simular una política

Simule una política en objetos de prueba antes de activarla y aplicarla a sus datos de producción.

Antes de empezar

- Conoces la clave de objeto/depósito S3 para cada objeto que deseas probar.

Pasos

1. Usando un cliente S3 o el "[Consola S3](#)" , ingerir los objetos necesarios para probar cada regla.
2. En la página de políticas de ILM, seleccione la casilla de verificación de la política y luego seleccione **Simular**.
3. En el campo **Objeto**, ingrese el S3 bucket/object-key para un objeto de prueba. Por ejemplo, bucket-01/filename.png .
4. Si el control de versiones S3 está habilitado, ingrese opcionalmente un ID de versión para el objeto en el campo **ID de versión**.
5. Seleccione **Simular**.
6. En la sección Resultados de simulación, confirme que cada objeto coincidió con la regla correcta.
7. Para determinar qué grupo de almacenamiento o perfil de codificación de borrado está en vigor, seleccione el nombre de la regla coincidente para ir a la página de detalles de la regla.



Revise cualquier cambio en la ubicación de los objetos replicados y codificados por borrado existentes. Cambiar la ubicación de un objeto existente puede generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.

Resultados

Cualquier modificación a las reglas de la política se reflejará en los resultados de la simulación y mostrará el nuevo partido y el partido anterior. La ventana de política Simular conserva los objetos que probó hasta que

seleccione **Borrar todo** o el ícono de eliminar  para cada objeto en la lista de resultados de simulación.

Información relacionada

["Ejemplo de simulaciones de políticas de ILM"](#)

Activar una política

Cuando se activa una única política ILM nueva, los objetos existentes y los objetos recientemente ingeridos son administrados por esa política. Cuando se activan varias políticas, las etiquetas de política ILM asignadas a los depósitos determinan los objetos que se deben administrar.

Antes de activar una nueva política:

1. Simule la política para confirmar que se comporta como espera.
2. Revise cualquier cambio en la ubicación de los objetos replicados y codificados por borrado existentes.
Cambiar la ubicación de un objeto existente puede generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.



Los errores en una política ILM pueden provocar una pérdida de datos irrecuperable.

Acerca de esta tarea

Cuando se activa una política ILM, el sistema distribuye la nueva política a todos los nodos. Sin embargo, es posible que la nueva política activa no entre en vigor hasta que todos los nodos de la red estén disponibles para recibirla. En algunos casos, el sistema espera para implementar una nueva política activa para garantizar que los objetos de la cuadrícula no se eliminen accidentalmente. Específicamente:

- Si realiza cambios de política que **aumentan la redundancia o durabilidad de los datos**, esos 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, esa política se implementará de inmediato porque aumenta la redundancia de datos.
- Si realiza cambios de política que **podrían disminuir la redundancia o durabilidad de los datos**, dichos cambios no se implementarán hasta que todos los nodos de la red estén disponibles. Por ejemplo, si activa una nueva política que utiliza una regla de dos copias en lugar de una regla de tres copias, la nueva política aparecerá en la pestaña Política activa, pero no tendrá efecto hasta que todos los nodos estén en línea y disponibles.

Pasos

Siga los pasos para activar una o varias políticas:

Activar una política

Siga estos pasos si solo tendrá una política activa. Si ya tiene una o más políticas activas y está activando políticas adicionales, siga los pasos para activar varias políticas.

1. Cuando esté listo para activar una política, seleccione **ILM > Políticas**.

Alternativamente, puede activar una sola política desde la página **ILM > Etiquetas de política**.

2. En la pestaña Políticas, seleccione la casilla de verificación de la política que desea activar y luego seleccione **Activar**.
3. Siga el paso apropiado:
 - Si un mensaje de advertencia le solicita que confirme que desea activar la política, seleccione **Aceptar**.
 - Si aparece un mensaje de advertencia que contiene detalles sobre la política:
 - i. Revise los detalles para asegurarse de que la política administre los datos como se espera.
 - ii. Si la regla predeterminada almacena objetos durante una cantidad limitada de días, revise el diagrama de retención y luego escriba esa cantidad de días en el cuadro de texto.
 - iii. Si la regla predeterminada almacena objetos para siempre, pero una o más reglas tienen una retención limitada, escriba **sí** en el cuadro de texto.
 - iv. Seleccione **Activar política**.

Activar múltiples políticas

Para activar varias políticas, debe crear etiquetas y asignar una política a cada etiqueta.



Cuando se utilizan varias etiquetas, si los inquilinos reasignan con frecuencia etiquetas de políticas a los depósitos, el rendimiento de la red podría verse afectado. Si tiene inquilinos que no son de confianza, considere usar solo la etiqueta Predeterminada.

1. Seleccione **ILM > Etiquetas de política**.
2. Seleccione **Crear**.
3. En el cuadro de diálogo Crear etiqueta de política, escriba un nombre de etiqueta y, opcionalmente, una descripción para la etiqueta.



Los nombres y descripciones de las etiquetas son visibles para los inquilinos. Elija valores que ayuden a los inquilinos a tomar una decisión informada al momento de seleccionar etiquetas de políticas para asignar a sus grupos. Por ejemplo, si la política asignada eliminará objetos después de un período de tiempo, podría comunicarlo en la descripción. No incluya información confidencial en estos campos.

4. Seleccione **Crear etiqueta**.
5. En la tabla de etiquetas de políticas de ILM, utilice el menú desplegable para seleccionar una política para asignar a la etiqueta.
6. Si aparecen advertencias en la columna Limitaciones de la política, seleccione **Ver detalles de la política** para revisar la política.
7. Asegúrese de que cada política gestione los datos como se espera.
8. Seleccione **Activar políticas asignadas**. O seleccione **Borrar cambios** para eliminar la asignación

de política.

9. En el cuadro de diálogo Activar políticas con nuevas etiquetas, revise las descripciones de cómo cada etiqueta, política y regla administrará los objetos. Realice los cambios necesarios para garantizar que las políticas administren los objetos como se espera.
10. Cuando esté seguro de que desea activar las políticas, escriba **sí** en el cuadro de texto y luego seleccione **Activar políticas**.

Información relacionada

["Ejemplo 6: Cambiar una política de ILM"](#)

Ejemplo de simulaciones de políticas de ILM

Los ejemplos de simulaciones de políticas ILM proporcionan pautas para estructurar y modificar simulaciones para su entorno.

Ejemplo 1: Verificar reglas al simular una política ILM

Este ejemplo describe cómo verificar reglas al simular una política.

En este ejemplo, se simula la **política ILM de ejemplo** contra los objetos ingeridos en dos buckets. La política incluye tres reglas, como sigue:

- La primera regla, **Dos copias, dos años para el contenedor a**, se aplica únicamente a los objetos del contenedor a.
- La segunda regla, **Objetos EC > 1 MB**, se aplica a todos los buckets, pero filtra los objetos mayores de 1 MB.
- La tercera regla, **Dos copias, dos centros de datos**, es la regla predeterminada. No incluye ningún filtro y no utiliza el tiempo de referencia no actual.

Después de simular la política, confirme que cada objeto coincida con la regla correcta.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
<button>Clear all</button> 				
Object 	Version ID 	Rule matched  	Previous match  	Actions
bucket-a/bucket-a object.pdf	—	Two copies, two years for bucket-a	—	
bucket-b/test object greater than 1 MB.pdf	—	EC objects > 1 MB	—	
bucket-b/test object less than 1 MB.pdf	—	Two copies, two data centers	—	

En este ejemplo:

- bucket-a/bucket-a object.pdf coincidió correctamente con la primera regla, que filtra los objetos en `bucket-a`.

- `bucket-b/test object greater than 1 MB.pdf` está en `bucket-b`, por lo que no coincidía con la primera regla. En cambio, la segunda regla coincidió correctamente, ya que filtra objetos de más de 1 MB.
- `bucket-b/test object less than 1 MB.pdf` no coincidió con los filtros de las dos primeras reglas, por lo que se colocará por la regla predeterminada, que no incluye filtros.

Ejemplo 2: Reordenar reglas al simular una política ILM

Este ejemplo muestra cómo se pueden reordenar las reglas para cambiar los resultados al simular una política.

En este ejemplo, se está simulando la política **Demo**. Esta política, que tiene como objetivo encontrar objetos que tengan metadatos de usuario `series=x-men`, incluye tres reglas, como sigue:

- La primera regla, **PNGs**, filtra los nombres de clave que terminan en `.png`.
- La segunda regla, **X-men**, se aplica solo a los objetos del inquilino A y filtra 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 política, seleccione **Simular**.
2. En el campo **Objeto**, ingrese la clave de objeto/depósito S3 para un objeto de prueba y seleccione **Simular**.

Aparecen los resultados de la simulación, que muestran que `Havok.png` El objeto coincidió con la regla **PNGs**.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	PNGs	—	X

Sin embargo, `Havok.png` Estaba destinado a probar la regla de los **X-men**.

3. Para resolver el problema, reordene las reglas.
 - a. Seleccione **Finalizar** para cerrar la ventana Simular política ILM.
 - b. Seleccione **Editar** para editar la política.
 - c. Arrastre la regla **X-men** a la parte superior de la lista.
 - d. Seleccione **Guardar**.
4. Seleccione **Simular**.

Los objetos que probó anteriormente se vuelven a evaluar en función de la política actualizada y se muestran los nuevos resultados de la simulación. En el ejemplo, la columna Regla coincidente muestra que `Havok.png` El objeto ahora coincide con la regla de metadatos de X-Men, como se esperaba. La

columna Coincidencia anterior muestra que la regla PNG coincidió con el objeto en la simulación anterior.

Simulation results

Use this table to confirm the results of applying this policy to the selected objects.

Clear all

Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	X-men	PNGs	

Ejemplo 3: Corregir una regla al simular una política ILM

Este ejemplo muestra cómo simular una política, corregir una regla en la política y continuar la simulación.

En este ejemplo, se está simulando la política **Demo**. Esta política tiene como objetivo encontrar objetos que tengan `series=x-men` metadatos del usuario. Sin embargo, se produjeron resultados inesperados al simular esta política contra la `Beast.jpg` objeto. En lugar de coincidir con la regla de metadatos de X-Men, el objeto coincidió con la regla predeterminada: Dos copias, dos centros de datos.

Simulation results

Use this table to confirm the results of applying this policy to the selected objects.

Clear all

Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	Two copies two data centers	—	

Cuando un objeto de prueba no coincide con la regla esperada en la política, debe examinar cada regla en la política y corregir cualquier error.

Pasos

1. Seleccione **Finalizar** para cerrar el cuadro de diálogo Simular política. En la página de detalles de la política, seleccione **Diagrama de retención**. Luego, seleccione **Expandir todo** o **Ver detalles** para cada regla según sea necesario.
2. Revise la cuenta de inquilino de la regla, el tiempo de referencia y los criterios de filtrado.

A modo de ejemplo, supongamos que los metadatos para la regla de X-men se ingresaron como "x-men01" en lugar de "x-men".
3. Para resolver el error, corrija la regla de la siguiente manera:
 - Si la regla es parte de la política, puede clonar la regla o eliminarla de la política y luego editarla.
 - Si la regla es parte de la política activa, debe clonar la regla. No se puede editar ni eliminar una regla de la política activa.
4. Realice la simulación nuevamente.

En este ejemplo, la regla corregida de los X-Men ahora coincide con la `Beast.jpg` objeto basado en el `series=x-men` metadatos del usuario, como se esperaba.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
photos/Beast.jpg	—	X-men	—	X

Administrar etiquetas de políticas de ILM

Puede ver los detalles de la etiqueta de política de ILM, editar una etiqueta o eliminar una etiqueta.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["permisos de acceso necesarios"](#).

Ver detalles de la etiqueta de política de ILM

Para ver los detalles de una etiqueta:

1. Seleccione **ILM > Etiquetas de política**.
2. Seleccione el nombre de la política de la tabla. Aparece la página de detalles de la etiqueta.
3. En la página de detalles, vea el historial anterior de políticas asignadas.
4. Ver una política seleccionándola.

Editar la etiqueta de política de ILM



Los nombres y descripciones de las etiquetas son visibles para los inquilinos. Elija valores que ayuden a los inquilinos a tomar una decisión informada al momento de seleccionar etiquetas de políticas para asignar a sus grupos. Por ejemplo, si la política asignada eliminará objetos después de un período de tiempo, podría comunicarlo en la descripción. No incluya información confidencial en estos campos.

Para editar la descripción de una etiqueta existente:

1. Seleccione **ILM > Etiquetas de política**.
2. Seleccione la casilla de verificación de la etiqueta y luego seleccione **Editar**.

Alternativamente, seleccione el nombre de la etiqueta. Aparecerá la página de detalles de la etiqueta y podrás seleccionar **Editar** en esa página.

3. Cambie la descripción de la etiqueta según sea necesario
4. Seleccione **Guardar**.

Eliminar la etiqueta de política de ILM

Cuando se elimina una etiqueta de política, a todos los depósitos que tengan asignada esa etiqueta se les

aplicará la política predeterminada.

Para eliminar una etiqueta:

1. Seleccione **ILM > Etiquetas de política**.
2. Seleccione la casilla de verificación de la etiqueta y luego seleccione **Eliminar**. Aparece un cuadro de diálogo de confirmación.

Alternativamente, seleccione el nombre de la etiqueta. Aparecerá la página de detalles de la etiqueta y podrás seleccionar **Eliminar** en esa página.

3. Seleccione **Sí** para eliminar la etiqueta.

Verificar una política de ILM con la búsqueda de metadatos de objetos

Después de haber activado una política ILM, ingiera objetos de prueba representativos en el sistema StorageGRID y luego realice una búsqueda de metadatos de objetos para confirmar que se estén realizando copias según lo previsto y se estén colocando en las ubicaciones correctas.

Antes de empezar

Tiene un identificador de objeto, que puede ser uno de los siguientes: * **UUID**: el identificador único universal del objeto. * **CBID**: El identificador único del objeto dentro de StorageGRID. Puede obtener el CBID de un objeto desde el registro de auditoría. Introduzca el CBD en mayúsculas. ***Clave de objeto y depósito S3**: cuando se ingiere un objeto a través de la interfaz S3, la aplicación cliente utiliza una combinación de clave de objeto y depósito para almacenar e identificar el objeto. Si el bucket S3 tiene versiones y desea buscar una versión específica de un objeto S3 usando la clave del bucket y del objeto, tendrá el **ID de versión**.

Pasos

1. Ingerir el objeto.
2. Seleccione **ILM > Búsqueda de metadatos de objetos**.
3. Escriba el identificador del objeto en el campo **Identificador**. Puede ingresar un UUID, CBID o una clave de objeto/depósito S3.
4. Opcionalmente, ingrese un ID de versión para el objeto (sólo S3).
5. Seleccione **Buscar**.

Aparecen los resultados de la búsqueda de metadatos del objeto. En esta página se enumeran los siguientes tipos de información:

- Metadatos del sistema, como ID de objeto (UUID), tipo de resultado (objeto, marcador de eliminación, depósito S3) y tamaño lógico del objeto. Consulte la captura de pantalla de ejemplo a continuación para obtener más detalles.
- Cualquier par clave-valor de metadatos de usuario personalizados asociados con el objeto.
- Para los objetos S3, cualquier par clave-valor de etiqueta de objeto asociado con el objeto.
- Para copias de objetos replicados, la ubicación de almacenamiento actual de cada copia.
- Para las copias de objetos con código de borrado, la ubicación de almacenamiento actual de cada fragmento.
- Para las copias de objetos en un grupo de almacenamiento en la nube, la ubicación del objeto, incluido el nombre del depósito externo y el identificador único del objeto.

- Para objetos segmentados y objetos multiparte, una lista de segmentos de objetos que incluye identificadores de segmento y tamaños de datos. Para los objetos con más de 100 segmentos, solo se muestran los primeros 100 segmentos.
 - Todos los metadatos del objeto en el formato de almacenamiento interno sin procesar. Estos metadatos sin procesar incluyen metadatos internos del sistema que no se garantiza que persistan de una versión a otra.
6. Confirme que el objeto esté almacenado en la ubicación o ubicaciones correctas y que sea el tipo de copia correcto.

Si la opción Auditoría está habilitada, también puede supervisar el registro de auditoría para el mensaje Reglas de objeto ORLM cumplidas. El mensaje de auditoría de ORLM puede brindarle más información sobre el estado del proceso de evaluación de ILM, pero no puede brindarle información sobre la exactitud de la ubicación de los datos del objeto ni sobre la integridad de la política de ILM. Debes evaluar esto tú mismo. Para obtener más información, consulte ["Revisar los registros de auditoría"](#).

El siguiente ejemplo muestra los resultados de la búsqueda de metadatos de un objeto de prueba S3 que se almacena como dos copias replicadas.



La siguiente captura de pantalla es un ejemplo. Los resultados variarán según la versión de StorageGRID .

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAIIS": "2",

```

Información relacionada

["Utilice la API REST de S3"](#)

Trabajar con políticas y reglas de ILM

A medida que cambian sus requisitos de almacenamiento, es posible que necesite implementar políticas adicionales o modificar las reglas de ILM asociadas con una política. Puede ver las métricas de ILM para determinar el rendimiento del sistema.

Antes de empezar

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

Ver las políticas de ILM

Para ver las políticas ILM activas e inactivas y el historial de activación de políticas:

1. Seleccione **ILM > Políticas**.
2. Seleccione **Políticas** para ver una lista de políticas activas e inactivas. La tabla enumera el nombre de cada política, las etiquetas a las que está asignada la política y si la política está activa o inactiva.
3. Seleccione **Historial de activación** para ver una lista de las fechas de inicio y finalización de la activación de las políticas.
4. Seleccione un nombre de política para ver los detalles de la política.



Si visualiza los detalles de una política cuyo estado es Editado o Eliminado, aparece un mensaje que explica que está visualizando la versión de la política que estuvo activa durante el período de tiempo especificado y que desde entonces ha sido editada o eliminada.

Editar una política de ILM

Sólo puedes editar una política inactiva. Si desea editar una política activa, desactívela o cree un clon y edítelo.

Para editar una política:

1. Seleccione **ILM > Políticas**.
2. Seleccione la casilla de verificación de la política que desea editar y luego seleccione **Editar**.
3. Edite la política siguiendo las instrucciones en "[Crear políticas ILM](#)".
4. Simule la política antes de reactivarla.



Una política ILM que se haya configurado incorrectamente puede provocar una pérdida irreparable de datos. Antes de activar una política ILM, revise cuidadosamente la política ILM y sus reglas ILM y luego simule la política ILM. Confirme siempre que la política ILM funcionará según lo previsto.

Clonar una política de ILM

Para clonar una política ILM:

1. Seleccione **ILM > Políticas**.
2. Seleccione la casilla de verificación de la política que desea clonar y luego seleccione **Clonar**.
3. Cree una nueva política a partir de la política que ha clonado siguiendo las instrucciones en "[Crear políticas ILM](#)".



Una política ILM que se haya configurado incorrectamente puede provocar una pérdida irreparable de datos. Antes de activar una política ILM, revise cuidadosamente la política ILM y sus reglas ILM y luego simule la política ILM. Confirme siempre que la política ILM funcionará según lo previsto.

Eliminar una política de ILM

Solo puedes eliminar una política ILM si está inactiva. Para eliminar una política:

1. Seleccione **ILM > Políticas**.

2. Seleccione la casilla de verificación de la política inactiva que desea eliminar.
3. Seleccione **Eliminar**.

Ver detalles de las reglas de ILM

Para ver los detalles de una regla ILM, incluido el diagrama de retención y las instrucciones de ubicación de la regla:

1. Seleccione **ILM > Reglas**.
2. Seleccione el nombre de la regla cuyos detalles desea ver. Ejemplo:

2 copies 2 data centers

Compliant: No
Ingest behavior: Strict
Reference time: Noncurrent time

[Clone](#) [Edit](#) [Remove](#)

[Rule detail](#) [Used in policies](#)

Time period and placements

[Retention diagram](#) [Placement instructions](#)

Sort placements by [Time period](#) [Storage pool](#)

● Replicated copy ● Erasure-coded (EC) copy

Rule analysis:

- Objects processed by this rule will not be deleted by ILM.

Reference time: **Noncurrent time** Ingest behavior: **Strict**

Day 0

Day 0 - forever

2 replicated copies - Data Center 1

EC 2+1 - Data Center 1

Duration Forever

Además, puede utilizar la página de detalles para clonar, editar o eliminar una regla. No puedes editar ni eliminar una regla si se utiliza en alguna política.

Clonar una regla ILM

Puede clonar una regla existente si desea crear una nueva regla que utilice algunas de las configuraciones de la regla existente. Si necesita editar una regla que se utiliza en alguna política, debe clonar la regla y realizar cambios en el clon. Después de realizar cambios en el clon, puede eliminar la regla original de la política y reemplazarla con la versión modificada según sea necesario.



No se puede clonar una regla ILM si se creó utilizando StorageGRID versión 10.2 o anterior.

Pasos

1. Seleccione **ILM > Reglas**.
2. Seleccione la casilla de verificación de la regla que desea clonar y luego seleccione **Clonar**.

Alternativamente, seleccione el nombre de la regla y luego seleccione **Clonar** en la página de detalles de la regla.

3. Actualice la regla clonada siguiendo los pasos para [editar una regla ILM](#) y ["Uso de filtros avanzados en las reglas de ILM"](#).

Al clonar una regla ILM, debe ingresar un nuevo nombre.

Editar una regla de ILM

Es posible que necesite editar una regla ILM para cambiar un filtro o una instrucción de ubicación.

No puedes editar una regla si se utiliza en alguna política de ILM. En cambio, puedes [clonar la regla](#) y realizar los cambios necesarios en la copia clonada.



Una política ILM que se haya configurado incorrectamente puede provocar una pérdida irreparable de datos. Antes de activar una política ILM, revise cuidadosamente la política ILM y sus reglas ILM y luego simule la política ILM. Confirme siempre que la política ILM funcionará según lo previsto.

Pasos

1. Seleccione **ILM > Reglas**.
2. Confirme que la regla que desea editar no se utiliza en ninguna política de ILM.
3. Si la regla que desea editar no está en uso, seleccione la casilla de verificación de la regla y seleccione **Acciones > Editar**. Alternativamente, seleccione el nombre de la regla y luego seleccione **Editar** en la página de detalles de la regla.
4. Complete los pasos del asistente Editar regla de ILM. Según sea necesario, siga los pasos para ["creando una regla ILM"](#) y ["Uso de filtros avanzados en las reglas de ILM"](#).

Al editar una regla ILM, no puedes cambiar su nombre.

Eliminar una regla ILM

Para mantener manejable la lista de reglas ILM actuales, elimine cualquier regla ILM que probablemente no utilice.

Pasos

Para eliminar una regla ILM que se utiliza actualmente en una política activa:

1. Clonar la política.
2. Eliminar la regla ILM del clon de política.
3. Guarde, simule y active la nueva política para asegurarse de que los objetos estén protegidos como se espera.
4. Vaya a los pasos para eliminar una regla ILM que se utiliza actualmente en una política inactiva.

Para eliminar una regla ILM que se utiliza actualmente en una política inactiva:

1. Seleccione la política inactiva.
2. Eliminar la regla ILM de la política o [eliminar la política](#).
3. Vaya a los pasos para eliminar una regla ILM que no se utiliza actualmente.

Para eliminar una regla ILM que no se utiliza actualmente:

1. Seleccione **ILM > Reglas**.
2. Confirme que la regla que desea eliminar no se utiliza en ninguna política.
3. Si la regla que desea eliminar no está en uso, selecciónela y seleccione **Acciones > Eliminar**. Puede seleccionar varias reglas y eliminarlas todas al mismo tiempo.
4. Seleccione **Sí** para confirmar que desea eliminar la regla ILM.

Ver métricas de ILM

Puede ver métricas de ILM, como la cantidad de objetos en la cola y la tasa de evaluación. Puede supervisar estas métricas para determinar el rendimiento del sistema. Una cola o tasa de evaluación grande podría indicar que el sistema no puede mantener el ritmo de la tasa de ingesta, que la carga de las aplicaciones cliente es excesiva o que existe alguna condición anormal.

Pasos

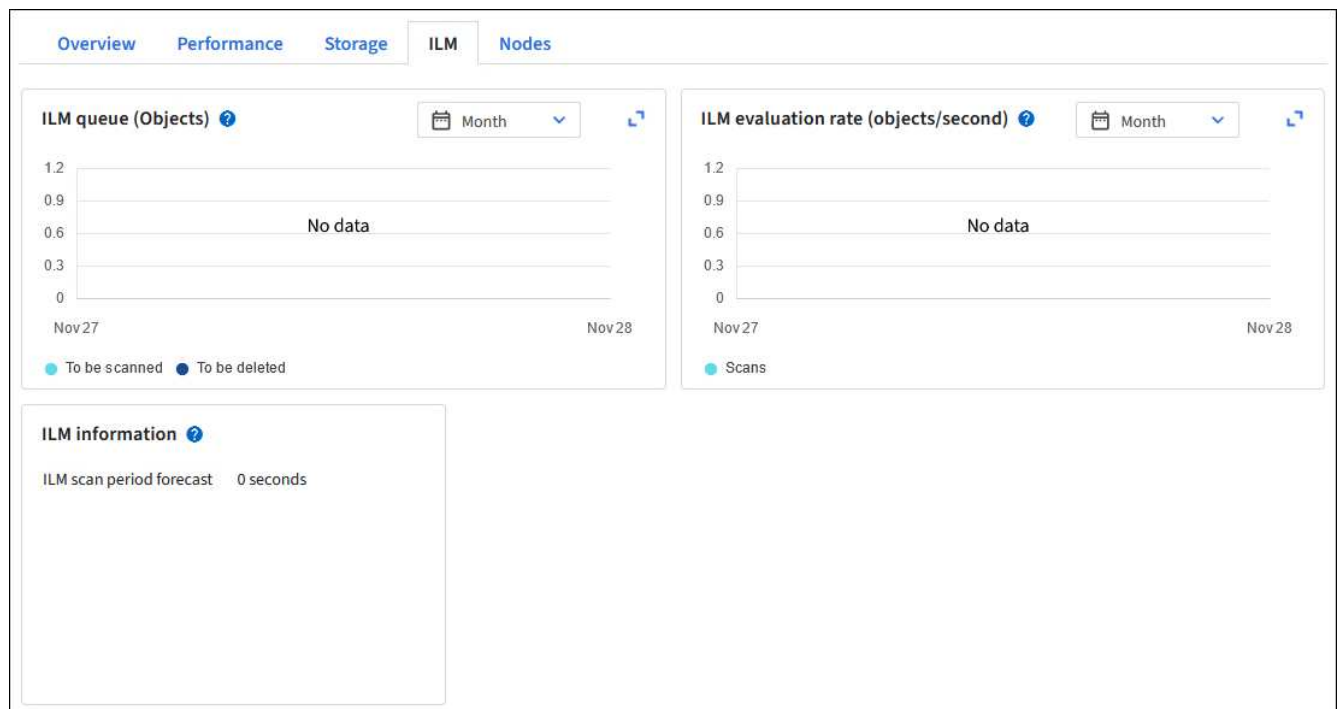
1. Seleccione **Panel de control > ILM**.



Debido a que el panel se puede personalizar, es posible que la pestaña ILM no esté disponible.

2. Supervise las métricas en la pestaña ILM.

Puedes seleccionar el signo de interrogación (?) para ver una descripción de los elementos en la pestaña ILM.



Usar bloqueo de objetos S3

Administrar objetos con S3 Object Lock

Como administrador de la red, puede habilitar el bloqueo de objetos S3 para su sistema StorageGRID e implementar una política ILM compatible para ayudar a garantizar que los objetos en depósitos S3 específicos no se eliminen ni se sobrescriban durante un período de tiempo específico.

¿Qué es el bloqueo de objetos S3?

La función StorageGRID S3 Object Lock es una solución de protección de objetos que es equivalente a S3 Object Lock en Amazon Simple Storage Service (Amazon S3).

Cuando la configuración global de Bloqueo de objetos S3 está habilitada para un sistema StorageGRID, una cuenta de inquilino S3 puede crear depósitos con o sin el Bloqueo de objetos S3 habilitado. Si un bucket tiene habilitado el bloqueo de objetos S3, se requiere el control de versiones del bucket y se habilita automáticamente.

Un depósito sin bloqueo de objetos S3 solo puede tener objetos sin configuraciones de retención especificadas. Ningún objeto ingerido tendrá configuraciones de retención.

Un depósito con bloqueo de objetos S3 puede tener objetos con y sin configuraciones de retención especificadas por las aplicaciones cliente S3. Algunos objetos ingeridos tendrán configuraciones de retención.

Un depósito con bloqueo de objetos S3 y retención predeterminada configurada puede tener objetos cargados con configuraciones de retención especificadas y objetos nuevos sin configuraciones de retención. Los nuevos objetos utilizan la configuración predeterminada, porque la configuración de retención no se ha configurado a nivel de objeto.

De hecho, todos los objetos recién ingeridos tienen configuraciones de retención cuando se configura la retención predeterminada. Los objetos existentes sin configuraciones de retención de objetos no se verán afectados.

Modos de retención

La función de bloqueo de objetos de StorageGRID S3 admite dos modos de retención para aplicar diferentes niveles de protección a los objetos. Estos modos son equivalentes a los modos de retención de Amazon S3.

- En modo de cumplimiento:
 - El objeto no se puede eliminar hasta que se alcance su fecha de conservación.
 - La fecha de conservación del objeto se puede aumentar, pero no se puede disminuir.
 - La fecha de retención del objeto no se puede eliminar hasta que se alcance esa fecha.
- En modo de gobernanza:
 - Los usuarios con permiso especial pueden usar un encabezado de omisión en las solicitudes para modificar ciertas configuraciones de retención.
 - Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su fecha de conservación.
 - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de conservación de un objeto.

Configuración de retención para versiones de objetos

Si se crea un depósito con el bloqueo de objetos S3 habilitado, los usuarios pueden usar la aplicación cliente S3 para especificar opcionalmente las siguientes configuraciones de retención para cada objeto que se agregue al depósito:

- **Modo de retención:** Cumplimiento o gobernanza.
- **Conservar hasta fecha:** si la fecha de conservación de una versión de un objeto está en el futuro, el objeto se puede recuperar, pero no se puede eliminar.
- **Retención legal:** al aplicar una retención legal a una versión de un objeto, se bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesites colocar una retención legal en un objeto que esté relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, sino que permanece vigente hasta que se elimina explícitamente. Las retenciones legales son independientes de la fecha de conservación.



Si un objeto está bajo retención legal, nadie puede eliminarlo, independientemente de su modo de retención.

Para obtener detalles sobre la configuración de los objetos, consulte ["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#).

Configuración de retención predeterminada para depósitos

Si se crea un depósito con el bloqueo de objetos S3 habilitado, los usuarios pueden especificar opcionalmente las siguientes configuraciones predeterminadas para el depósito:

- **Modo de retención predeterminado:** Cumplimiento o gobernanza.
- **Período de retención predeterminado:** durante cuánto tiempo se deben conservar las nuevas versiones de objetos agregadas a este depósito, a partir del día en que se agregan.

La configuración de depósito predeterminada se aplica únicamente a los objetos nuevos que no tienen su propia configuración de retención. Los objetos de bucket existentes no se ven afectados cuando agrega o cambia estas configuraciones predeterminadas.

Ver ["Crear un bucket S3"](#) y ["Actualizar la retención predeterminada de bloqueo de objetos S3"](#).

Comparación del bloqueo de objetos S3 con la conformidad heredada

El bloqueo de objetos S3 reemplaza la función de Cumplimiento que estaba disponible en versiones anteriores de StorageGRID. Debido a que la función de bloqueo de objetos S3 se ajusta a los requisitos de Amazon S3, deja obsoleta la función de cumplimiento patentada de StorageGRID, que ahora se denomina "cumplimiento heredado".



La configuración de Cumplimiento global está obsoleta. Si habilitó esta configuración utilizando una versión anterior de StorageGRID, la configuración de Bloqueo de objetos S3 se habilita automáticamente. Puede seguir usando StorageGRID para administrar las configuraciones de los depósitos compatibles existentes; sin embargo, no puede crear depósitos compatibles nuevos. Para más detalles, consulte ["Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5"](#).

Si utilizó la función de Cumplimiento heredada en una versión anterior de StorageGRID, consulte la siguiente tabla para saber cómo se compara con la función de Bloqueo de objetos S3 en StorageGRID.

	Bloqueo de objetos S3	Cumplimiento (legado)
¿Cómo se habilita la función a nivel global?	Desde el Administrador de cuadrícula, seleccione CONFIGURACIÓN > Sistema > Bloqueo de objetos S3 .	Ya no se admite.
¿Cómo se habilita la función para un bucket?	Los usuarios deben habilitar el bloqueo de objetos S3 al crear un nuevo depósito mediante el Administrador de inquilinos, la API de administración de inquilinos o la API REST de S3.	Ya no se admite.
¿Se admite el control de versiones del bucket?	Sí. El control de versiones del depósito es necesario y se habilita automáticamente cuando S3 Object Lock está habilitado para el depósito.	No.
¿Cómo se establece la retención de objetos?	Los usuarios pueden establecer una fecha de retención para cada versión del objeto o pueden establecer un período de retención predeterminado para cada depósito.	Los usuarios deben establecer un período de retención para todo el depósito. El período de retención se aplica a todos los objetos del depósito.
¿Se puede modificar el periodo de conservación?	• En el modo de cumplimiento, la fecha de retención para una versión de objeto se puede aumentar, pero nunca disminuir. • En el modo de gobernanza, los usuarios con permisos especiales pueden disminuir o incluso eliminar la configuración de retención de un objeto.	El período de retención de un depósito se puede aumentar, pero nunca disminuir.
¿Dónde se controla la retención legal?	Los usuarios pueden colocar una retención legal o levantar una retención legal para cualquier versión de objeto en el depósito.	Se coloca una retención legal en el cubo y afecta a todos los objetos que se encuentran en el cubo.

	Bloqueo de objetos S3	Cumplimiento (legado)
¿Cuándo se pueden eliminar objetos?	- En el modo de cumplimiento, se puede eliminar una versión de un objeto una vez alcanzada la fecha de retención, siempre que el objeto no esté bajo retención legal. - En el modo de gobernanza, los usuarios con permisos especiales pueden eliminar un objeto antes de que se alcance su fecha de retención, siempre que el objeto no esté bajo retención legal.	Se puede eliminar un objeto una vez que expire el período de retención, siempre que el depósito no esté bajo retención legal. Los objetos se pueden eliminar de forma automática o manual.
¿Se admite la configuración del ciclo de vida del bucket?	Sí	No

Tareas de bloqueo de objetos S3

Como administrador de la red, debe coordinarse estrechamente con los usuarios inquilinos para garantizar que los objetos estén protegidos de una manera que satisfaga sus requisitos de retención.



La aplicación de la configuración de los inquilinos en toda la red podría demorar 15 minutos o más según la conectividad de la red, el estado del nodo y las operaciones de Cassandra.

Las siguientes listas para administradores de red y usuarios inquilinos contienen las tareas de alto nivel para usar la función de bloqueo de objetos S3.

Administrador de red

- Habilite la configuración global de bloqueo de objetos S3 para todo el sistema StorageGRID .
- Asegúrese de que las políticas de gestión del ciclo de vida de la información (ILM) sean *compatibles*; es decir, que cumplan con los requisitos "[Requisitos de los buckets con bloqueo de objetos S3 habilitado](#)".
- Según sea necesario, permita que un inquilino utilice Cumplimiento como modo de retención. De lo contrario, solo se permite el modo Gobernanza.
- Según sea necesario, establezca un período máximo de retención para un inquilino.

Usuario inquilino

- Revise las consideraciones para depósitos y objetos con bloqueo de objetos S3.
- Según sea necesario, comuníquese con el administrador de la red para habilitar la configuración global de bloqueo de objetos S3 y establecer permisos.
- Cree depósitos con el bloqueo de objetos S3 habilitado.
- De manera opcional, configure los ajustes de retención predeterminados para un depósito:

- Modo de retención predeterminado: Gobernanza o Cumplimiento, si lo permite el administrador de la red.
- Período de retención predeterminado: debe ser menor o igual al período de retención máximo establecido por el administrador de la red.
- Utilice la aplicación cliente S3 para agregar objetos y, opcionalmente, configurar la retención específica de objetos:
 - Modo de retención. Gobernanza o Cumplimiento, si lo permite el administrador de la red.
 - Conservar hasta la fecha: debe ser menor o igual a lo permitido por el período máximo de retención establecido por el administrador de la red.

Requisitos para el bloqueo de objetos S3

Debe revisar los requisitos para habilitar la configuración global de Bloqueo de objetos S3, los requisitos para crear reglas y políticas ILM compatibles y las restricciones que StorageGRID impone a los depósitos y objetos que usan Bloqueo de objetos S3.

Requisitos para utilizar la configuración global de bloqueo de objetos S3

- Debe habilitar la configuración global de Bloqueo de objetos S3 mediante el Administrador de cuadrícula o la API de administración de cuadrícula antes de que cualquier inquilino de S3 pueda crear un depósito con el Bloqueo de objetos S3 habilitado.
- Al habilitar la configuración global de Bloqueo de objetos S3, se permite que todas las cuentas de inquilinos de S3 creen depósitos con el Bloqueo de objetos S3 habilitado.
- Después de habilitar la configuración global de Bloqueo de objetos S3, no podrá deshabilitarla.
- No se puede habilitar el bloqueo de objetos S3 global a menos que la regla predeterminada en todas las políticas ILM activas sea *compatible* (es decir, la regla predeterminada debe cumplir con los requisitos de los depósitos con el bloqueo de objetos S3 habilitado).
- Cuando la configuración global de Bloqueo de objetos S3 está habilitada, no puede crear una nueva política ILM ni activar una política ILM existente a menos que la regla predeterminada en la política sea compatible. Una vez habilitada la configuración global de bloqueo de objetos S3, las páginas de reglas ILM y políticas ILM indican qué reglas ILM son compatibles.

Requisitos para el cumplimiento de las normas ILM

Si desea habilitar la configuración global de bloqueo de objetos S3, debe asegurarse de que la regla predeterminada en todas las políticas ILM activas sea compatible. Una regla compatible satisface los requisitos de ambos depósitos con S3 Object Lock habilitado y de cualquier depósito existente que tenga habilitada la conformidad heredada:

- Debe crear al menos dos copias del objeto replicado o una copia con código de borrado.
- Estas copias deben existir en los nodos de almacenamiento durante toda la duración de cada línea en las instrucciones de ubicación.
- Las copias de objetos no se pueden guardar en un grupo de almacenamiento en la nube.
- Al menos una línea de las instrucciones de ubicación debe comenzar en el día 0, utilizando **Hora de ingesta** como tiempo de referencia.
- Al menos una línea de las instrucciones de colocación debe ser "para siempre".

Requisitos para las políticas de ILM

Cuando la configuración global de Bloqueo de objetos S3 está habilitada, las políticas ILM activas e inactivas pueden incluir reglas compatibles y no compatibles.

- La regla predeterminada en una política ILM activa o inactiva debe ser compatible.
- Las reglas no conformes solo se aplican a los objetos en depósitos que no tienen habilitado el Bloqueo de objetos S3 o que no tienen habilitada la función de Cumplimiento heredada.
- Las reglas compatibles se pueden aplicar a objetos en cualquier bucket; no es necesario habilitar S3 Object Lock ni la conformidad heredada para el bucket.

"Ejemplo de una política ILM compatible con el bloqueo de objetos S3"

Requisitos para los buckets con el bloqueo de objetos S3 habilitado

- Si la configuración global de Bloqueo de objetos S3 está habilitada para el sistema StorageGRID , puede usar el Administrador de inquilinos, la API de administración de inquilinos o la API REST de S3 para crear depósitos con el Bloqueo de objetos S3 habilitado.
- Si planea utilizar S3 Object Lock, debe habilitar S3 Object Lock cuando cree el depósito. No se puede habilitar el bloqueo de objetos S3 para un depósito existente.
- Cuando S3 Object Lock está habilitado para un bucket, StorageGRID habilita automáticamente el control de versiones para ese bucket. No puedes deshabilitar el bloqueo de objetos S3 ni suspender el control de versiones del depósito.
- De manera opcional, puede especificar un modo de retención predeterminado y un período de retención para cada depósito mediante el Administrador de inquilinos, la API de administración de inquilinos o la API REST de S3. La configuración de retención predeterminada del depósito se aplica únicamente a los objetos nuevos agregados al depósito que no tienen su propia configuración de retención. Puede anular estas configuraciones predeterminadas especificando un modo de retención y una fecha de retención para cada versión del objeto cuando se carga.
- La configuración del ciclo de vida del bucket es compatible con los buckets que tienen el bloqueo de objetos S3 habilitado.
- La replicación de CloudMirror no es compatible con depósitos con el bloqueo de objetos S3 habilitado.

Requisitos para objetos en depósitos con bloqueo de objetos S3 habilitado

- Para proteger una versión de objeto, puede especificar la configuración de retención predeterminada para el depósito o puede especificar la configuración de retención para cada versión de objeto. Las configuraciones de retención a nivel de objeto se pueden especificar mediante la aplicación cliente S3 o la API REST S3.
- Las configuraciones de retención se aplican a versiones de objetos individuales. Una versión de objeto puede tener una configuración de conservación hasta la fecha y una configuración de conservación legal, una pero no la otra, o ninguna. Al especificar una configuración de retención hasta la fecha o de retención legal para un objeto, se protege únicamente la versión especificada en la solicitud. Puede crear nuevas versiones del objeto, mientras la versión anterior del objeto permanece bloqueada.

Ciclo de vida de objetos en buckets con S3 Object Lock habilitado

Cada objeto que se guarda en un bucket con el bloqueo de objetos S3 habilitado pasa por estas etapas:

1. Ingesta de objeto

Cuando se agrega una versión de objeto a un depósito que tiene habilitado el Bloqueo de objetos S3, las

configuraciones de retención se aplican de la siguiente manera:

- Si se especifican configuraciones de retención para el objeto, se aplican las configuraciones a nivel de objeto. Se ignoran todas las configuraciones de depósito predeterminadas.
- Si no se especifican configuraciones de retención para el objeto, se aplican las configuraciones de depósito predeterminadas, si existen.
- Si no se especifican configuraciones de retención para el objeto o el depósito, el objeto no estará protegido por el bloqueo de objetos S3.

Si se aplican configuraciones de retención, tanto el objeto como cualquier metadato definido por el usuario de S3 estarán protegidos.

2. Retención y eliminación de objetos

StorageGRID almacena varias copias de cada objeto protegido durante el período de retención especificado. La cantidad exacta y el tipo de copias de objetos y las ubicaciones de almacenamiento están determinados por las reglas compatibles con las políticas ILM activas. Si un objeto protegido se puede eliminar antes de que se alcance su fecha de retención depende de su modo de retención.

- Si un objeto está bajo retención legal, nadie puede eliminarlo, independientemente de su modo de retención.

Información relacionada

- ["Crear un bucket S3"](#)
- ["Actualizar la retención predeterminada de bloqueo de objetos S3"](#)
- ["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#)
- ["Ejemplo 7: Política ILM compatible con el bloqueo de objetos S3"](#)

Habilitar el bloqueo de objetos S3 globalmente

Si una cuenta de inquilino S3 necesita cumplir con requisitos reglamentarios al guardar datos de objetos, debe habilitar S3 Object Lock para todo su sistema StorageGRID . Al habilitar la configuración global de Bloqueo de objetos S3, cualquier usuario inquilino de S3 puede crear y administrar depósitos y objetos con Bloqueo de objetos S3.

Antes de empezar

- Tú tienes el ["Permiso de acceso root"](#) .
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Ha revisado el flujo de trabajo de bloqueo de objetos S3 y comprende las consideraciones.
- Ha confirmado que la regla predeterminada en la política ILM activa es compatible. Ver ["Crear una regla ILM predeterminada"](#) Para más detalles.

Acerca de esta tarea

Un administrador de red debe habilitar la configuración global de Bloqueo de objetos S3 para permitir que los usuarios inquilinos creen nuevos depósitos que tengan habilitado el Bloqueo de objetos S3. Una vez habilitada esta configuración, no se podrá deshabilitar.

Revise la configuración de cumplimiento de los inquilinos existentes después de habilitar la configuración global de Bloqueo de objetos S3. Cuando habilita esta configuración, las configuraciones de bloqueo de objetos S3 por inquilino dependen de la versión de StorageGRID en el momento en que se creó el inquilino.



La configuración de Cumplimiento global está obsoleta. Si habilitó esta configuración utilizando una versión anterior de StorageGRID, la configuración de Bloqueo de objetos S3 se habilita automáticamente. Puede seguir usando StorageGRID para administrar las configuraciones de los depósitos compatibles existentes; sin embargo, no puede crear depósitos compatibles nuevos. Para más detalles, consulte ["Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5"](#) .

Pasos

1. Seleccione **CONFIGURACIÓN > Sistema > Bloqueo de objetos S3**.

Aparece la página Configuración de bloqueo de objetos S3.

2. Seleccione **Habilitar bloqueo de objetos S3**.

3. Seleccione **Aplicar**.

Aparece un cuadro de diálogo de confirmación que le recuerda que no puede deshabilitar S3 Object Lock una vez habilitado.

4. Si está seguro de que desea habilitar permanentemente S3 Object Lock para todo el sistema, seleccione **Aceptar**.

Al seleccionar **Aceptar**:

- Si la regla predeterminada en la política ILM activa es compatible, el bloqueo de objetos S3 ahora está habilitado para toda la cuadrícula y no se puede deshabilitar.
- Si la regla predeterminada no se cumple, aparece un error. Debe crear y activar una nueva política ILM que incluya una regla compatible como regla predeterminada. Seleccione **Aceptar**. Luego, crea una nueva política, simulénala y actívala. Ver ["Crear una política ILM"](#) para obtener instrucciones.

Resolver errores de coherencia al actualizar el bloqueo de objetos S3 o la configuración de cumplimiento heredada

Si un sitio de un centro de datos o varios nodos de almacenamiento en un sitio dejan de estar disponibles, es posible que deba ayudar a los usuarios inquilinos de S3 a aplicar cambios en el bloqueo de objetos de S3 o en la configuración de cumplimiento heredada.

Los usuarios inquilinos que tienen depósitos con S3 Object Lock (o cumplimiento heredado) habilitado pueden cambiar ciertas configuraciones. Por ejemplo, un usuario inquilino que utiliza S3 Object Lock podría necesitar colocar una versión de objeto bajo retención legal.

Cuando un usuario inquilino actualiza la configuración de un depósito S3 o una versión de objeto, StorageGRID intenta actualizar inmediatamente los metadatos del depósito o del objeto en toda la red. Si el sistema no puede actualizar los metadatos porque un sitio del centro de datos o varios nodos de almacenamiento no están disponibles, devuelve un error:

```
503: Service Unavailable
```

```
Unable to update compliance settings because the settings can't be  
consistently applied on enough storage services. Contact your grid  
administrator for assistance.
```

Para resolver este error, siga estos pasos:

1. Intente que todos los nodos o sitios de almacenamiento vuelvan a estar disponibles lo antes posible.
2. Si no puede poner a disposición suficientes nodos de almacenamiento en cada sitio, comuníquese con el soporte técnico, que puede ayudarlo a recuperar nodos y garantizar que los cambios se apliquen de manera uniforme en toda la red.
3. Una vez que se haya resuelto el problema subyacente, recuérdelo al usuario inquilino que vuelva a intentar realizar los cambios de configuración.

Información relacionada

- ["Utilice una cuenta de inquilino"](#)
- ["Utilice la API REST de S3"](#)
- ["Recuperar y mantener"](#)

Ejemplo de reglas y políticas de ILM

Ejemplo 1: Reglas y políticas de ILM para el almacenamiento de objetos

Puede utilizar las siguientes reglas y políticas de ejemplo como punto de partida al definir una política ILM para cumplir con sus requisitos de retención y protección de objetos.



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlere la para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

Regla 1 de ILM para el ejemplo 1: Copiar datos de objetos a dos sitios

Esta regla ILM de ejemplo copia datos de objetos en grupos de almacenamiento en dos sitios.

Definición de regla	Valor de ejemplo
Piscinas de almacenamiento en un solo sitio	Dos grupos de almacenamiento, cada uno con sitios diferentes, denominados Sitio 1 y Sitio 2.
Nombre de la regla	Dos copias, dos sitios
Tiempo de referencia	Tiempo de ingesta
Colocaciones	Desde el día 0 hasta siempre, conserve una copia replicada en el Sitio 1 y una copia replicada en el Sitio 2.

La sección de análisis de reglas del diagrama de retención establece:

- La protección contra pérdida de sitios de StorageGRID se aplicará mientras dure esta regla.
- Los objetos procesados por esta regla no serán eliminados por ILM.

Reference time ⓘ

Ingest time

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1

From Day 0

store forever

×

Store objects by replicating

1

copies at Site 1

×

✎

×

and store objects by replicating

1

copies at Site 2

×

✎

×

[Add other type or location](#)

Add another time period

Retention diagram

● Replicated copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Day 0 - forever

1 replicated copy - Site 1

1 replicated copy - Site 2

Duration

Forever

Regla 2 de ILM para el ejemplo 1: Perfil de codificación de borrado con coincidencia de depósito

Esta regla ILM de ejemplo utiliza un perfil de codificación de borrado y un depósito S3 para determinar dónde y durante cuánto tiempo se almacena el objeto.

Definición de regla	Valor de ejemplo
Pool de almacenamiento con múltiples sitios	- Un grupo de almacenamiento en tres sitios (sitios 1, 2 y 3) - Utilice el esquema de codificación de borrado 6+3
Nombre de la regla	Registros financieros del depósito S3
Tiempo de referencia	Tiempo de ingesta
Colocaciones	Para los objetos en el bucket S3 llamado finance-records, cree una copia con código de borrado en el grupo especificado por el perfil de codificación de borrado. Conserve esta copia para siempre.

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1

From Day 0

store forever

Store objects by

erasure coding

using 6+3 EC scheme at Sites 1, 2, 3

Add other type or location

Add another time period

Retention diagram

Erasure-coded (EC) copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Day 0 - forever

EC 6+3 - Sites 1, 2, 3

Duration Forever

Política de ILM, por ejemplo 1

En la práctica, la mayoría de las políticas ILM son simples, aunque el sistema StorageGRID le permite diseñar políticas ILM sofisticadas y complejas.

Una política ILM típica para una red de múltiples sitios podría incluir reglas ILM como las siguientes:

- En la ingesta, almacene todos los objetos que pertenecen al bucket S3 denominado `finance-records` en un grupo de almacenamiento que contiene tres sitios. Utilice la codificación de borrado 6+3.
- Si un objeto no coincide con la primera regla ILM, utilice la regla ILM predeterminada de la política, Dos copias, dos centros de datos, para almacenar una copia de ese objeto en el Sitio 1 y una copia en el Sitio 2.

Información relacionada

- ["Utilice las políticas de ILM"](#)
- ["Crear políticas ILM"](#)

Ejemplo 2: Reglas y políticas de ILM para el filtrado del tamaño de objetos EC

Puede utilizar las siguientes reglas y políticas de ejemplo como puntos de partida para definir una política ILM que filtre por tamaño de objeto para cumplir con los requisitos de EC recomendados.



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlere la para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

Regla 1 de ILM para el ejemplo 2: utilizar EC para objetos mayores a 1 MB

Este ejemplo de código de borrado de reglas ILM codifica objetos que tienen más de 1 MB.



La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Solo objetos EC > 1 MB
Tiempo de referencia	Tiempo de ingesta
Filtro avanzado para el tamaño del objeto	Tamaño de objeto mayor a 1 MB
Colocaciones	Cree una copia con código de borrado 2+1 utilizando tres sitios

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ×

Object size ▼

greater than ▼

1 ↕

MB ▼ ×

Regla 2 de ILM para el ejemplo 2: Dos copias replicadas

Esta regla ILM de ejemplo crea dos copias replicadas y no filtra por tamaño de objeto. Esta regla es la regla predeterminada para la política. Dado que la primera regla filtra todos los objetos mayores a 1 MB, esta regla solo se aplica a objetos de 1 MB o menos.

Definición de regla	Valor de ejemplo
Nombre de la regla	Dos copias replicadas
Tiempo de referencia	Tiempo de ingesta
Filtro avanzado para el tamaño del objeto	Ninguno
Colocaciones	Desde el día 0 hasta siempre, conserve una copia replicada en el Sitio 1 y una copia replicada en el Sitio 2.

Política de ILM para el ejemplo 2: utilizar EC para objetos mayores a 1 MB

Este ejemplo de política ILM incluye dos reglas ILM:

- La primera regla borra todos los objetos que tengan un tamaño superior a 1 MB.
- La segunda regla ILM (predeterminada) crea dos copias replicadas. Debido a que la regla 1 filtró los objetos de más de 1 MB, la regla 2 solo se aplica a objetos de 1 MB o menos.

Ejemplo 3: Reglas y políticas de ILM para una mejor protección de los archivos de imagen

Puede utilizar las siguientes reglas y políticas de ejemplo para garantizar que las imágenes de más de 1 MB tengan un código de borrado y que se hagan dos copias de imágenes más pequeñas.



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlere la para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

Regla 1 de ILM para el ejemplo 3: utilizar EC para archivos de imagen de más de 1 MB

Esta regla ILM de ejemplo utiliza filtrado avanzado para borrar el código de todos los archivos de imagen de más de 1 MB.



La codificación de borrado es más adecuada para objetos de más de 1 MB. No utilice codificación de borrado para objetos más pequeños que 200 KB para evitar la sobrecarga de administrar fragmentos muy pequeños codificados por borrado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Archivos de imagen EC > 1 MB
Tiempo de referencia	Tiempo de ingesta
Filtro avanzado para el tamaño del objeto	Tamaño de objeto mayor a 1 MB
Filtros avanzados para clave	• Termina en .jpg • Termina en .png
Colocaciones	Cree una copia con código de borrado 2+1 utilizando tres sitios

Filter group 1

Objects with all of following metadata will be evaluated by this rule:

Object size

greater than

1

MB

X

and

Key

ends with

.jpg

X

or

Filter group 2

Objects with all of following metadata will be evaluated by this rule:

Object size

greater than

1

MB

X

and

Key

ends with

.png

X

Debido a que esta regla está configurada como la primera regla en la política, la instrucción de ubicación de codificación de borrado solo se aplica a archivos .jpg y .png que tengan más de 1 MB.

Regla 2 de ILM para el ejemplo 3: Crear 2 copias replicadas para todos los archivos de imagen restantes

Esta regla ILM de ejemplo utiliza filtrado avanzado para especificar que se repliquen archivos de imagen más pequeños. Dado que la primera regla de la política ya ha coincidido con archivos de imagen de más de 1 MB, esta regla se aplica a archivos de imagen de 1 MB o menos.

Definición de regla	Valor de ejemplo
Nombre de la regla	2 copias para archivos de imagen
Tiempo de referencia	Tiempo de ingesta
Filtros avanzados para clave	• Termina en .jpg • Termina en .png
Colocaciones	Cree 2 copias replicadas en dos grupos de almacenamiento

Política de ILM, por ejemplo 3: Mejor protección para los archivos de imagen

Este ejemplo de política ILM incluye tres reglas:

- La primera regla borra todos los archivos de imagen mayores a 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 imagen).

Ejemplo 4: Reglas y políticas de ILM para objetos versionados de S3

Si tiene un bucket S3 con control de versiones habilitado, puede administrar las versiones de objetos no actuales incluyendo reglas en su política ILM que utilicen "Hora no actual" como hora de referencia.



Si especifica un tiempo de retención limitado para los objetos, dichos objetos se eliminarán de forma permanente una vez alcanzado el período de tiempo. Asegúrese de comprender cuánto tiempo se conservarán los objetos.

Como muestra este ejemplo, puede controlar la cantidad de almacenamiento utilizada por objetos versionados mediante el uso de diferentes instrucciones de ubicación para versiones de objetos no actuales.



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlere la para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.



Para realizar una simulación de política ILM en una versión no actual de un objeto, debe conocer el UUID o CBID de la versión del objeto. Para encontrar el UUID y el CBID, utilice ["búsqueda de metadatos de objetos"](#) mientras el objeto todavía esté actual.

Información relacionada

"Cómo se eliminan los objetos"

Regla 1 de ILM, por ejemplo 4: Guardar tres copias durante 10 años

Esta regla ILM de ejemplo almacena una copia de cada objeto en tres sitios durante 10 años.

Esta regla se aplica a todos los objetos, independientemente de si tienen versiones o no.

Definición de regla	Valor de ejemplo
Pools de almacenamiento	Tres grupos de almacenamiento, cada uno de ellos compuesto por diferentes centros de datos, denominados Sitio 1, Sitio 2 y Sitio 3.
Nombre de la regla	Tres copias, diez años
Tiempo de referencia	Tiempo de ingesta
Colocaciones	El día 0, conserve tres copias replicadas durante 10 años (3652 días), una en el Sitio 1, una en el Sitio 2 y una en el Sitio 3. Al cabo de 10 años, elimine todas las copias del objeto.

Regla 2 de ILM, por ejemplo 4: Guardar dos copias de versiones no actuales durante 2 años

Esta regla ILM de ejemplo almacena dos copias de las versiones no actuales de un objeto versionado S3 durante 2 años.

Dado que la regla 1 de ILM se aplica a todas las versiones del objeto, debe crear otra regla para filtrar las versiones no actuales.

Para crear una regla que use "Hora no actual" como hora de referencia, seleccione **Sí** para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en depósitos S3 con control de versiones habilitado)?" en el Paso 1 (Ingresar detalles) del asistente Crear una regla de ILM. Cuando selecciona **Sí**, se selecciona automáticamente *Hora no actual* como hora de referencia y no puede seleccionar una hora de referencia diferente.

1

Enter details

2

Define placements

3

Select ingest behavior

Rule name

Older Object Versions: Two Copies Two Years

Description (optional)

Older versions only

Basic filters (optional)

Specify which tenant accounts and buckets this rule applies to.

Tenant accounts ?

Select tenant accounts

Bucket name ?

matches all

Apply this rule to older object versions only (in S3 buckets with versioning enabled)? ?

☐ No☒ Yes

En este ejemplo, solo se almacenan dos copias de las versiones no actuales, y esas copias se almacenarán durante dos años.

Definición de regla	Valor de ejemplo
Pools de almacenamiento	Dos grupos de almacenamiento, cada uno en diferentes centros de datos, Sitio 1 y Sitio 2.
Nombre de la regla	Versiones no actuales: dos copias dos años
Tiempo de referencia	Tiempo no actual Se selecciona automáticamente cuando selecciona Sí para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores (en depósitos S3 con control de versiones habilitado)?" en el asistente Crear una regla de ILM.
Colocaciones	El día 0 en relación con el tiempo no actual (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 no actuales del objeto durante 2 años (730 días), una en el Sitio 1 y otra en el Sitio 2. Al cabo de 2 años, elimine las versiones no actuales.

Política de ILM para el ejemplo 4: objetos versionados S3

Si desea administrar versiones anteriores de un objeto de forma diferente a la versión actual, las reglas que utilizan "Hora no actual" como hora de referencia deben aparecer en la política ILM antes que las reglas que se aplican a la versión actual del objeto.

Una política ILM para objetos versionados S3 podría incluir reglas ILM como las siguientes:

- Conserve cualquier versión anterior (no actual) de cada objeto durante 2 años, a partir del día en que la versión dejó de estar actual.



Las reglas de "Hora no actual" deben aparecer en la política antes de las reglas que se aplican a la versión actual del objeto. De lo contrario, las versiones de objetos no actuales nunca coincidirán con la regla "Tiempo no actual".

- Al momento de la ingesta, cree tres copias replicadas y almacene una copia en cada uno de los tres sitios. Conserve copias de la versión actual del objeto durante 10 años.

Al simular la política de ejemplo, esperaría que los objetos de prueba se evaluarán de la siguiente manera:

- Cualquier versión de objeto no actual se corresponderá con la primera regla. Si una versión no actual de un objeto tiene más de 2 años, ILM la elimina de forma permanente (todas las copias de la versión no actual se eliminan de la red).
- 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 de eliminación como la versión actual del objeto y hace que la versión anterior del objeto sea "no actual". La próxima vez que se realiza una evaluación ILM, esta versión no actual coincide con la primera regla. Como resultado, la copia en el Sitio 3 se elimina y las dos copias en el Sitio 1 y el Sitio 2 se almacenan durante 2 años más.

Ejemplo 5: Reglas y políticas de ILM para el comportamiento de ingesta estricto

Puede utilizar un filtro de ubicación y el comportamiento de ingesta estricta en 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 cuestiones regulatorias. Otros objetos, incluidos todos los objetos de otras cuentas de inquilinos, se pueden almacenar 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. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlrela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

Información relacionada

- ["Opciones de ingesta"](#)
- ["Crear regla de ILM: Seleccionar comportamiento de ingesta"](#)

Regla 1 de ILM, por ejemplo 5: Ingesta estricta para garantizar el centro de datos de París

Esta regla ILM de ejemplo utiliza el comportamiento de ingesta estricta para garantizar que los objetos guardados por un inquilino con sede en París en depósitos S3 con la región configurada en eu-west-3 (París) nunca se almacenen en el centro de datos de EE. UU.

Esta regla se aplica a los objetos que pertenecen al inquilino de París y que tienen la región de depósito S3

establecida en eu-west-3 (París).

Definición de regla	Valor de ejemplo
Cuenta de inquilino	inquilino de París
Filtro avanzado	La restricción de ubicación es igual a eu-west-3
Pools de almacenamiento	Sitio 1 (París)
Nombre de la regla	Ingesta estricta para garantizar el centro de datos de París
Tiempo de referencia	Tiempo de ingesta
Colocaciones	El día 0, conserve dos copias replicadas para siempre en el Sitio 1 (París)
Comportamiento de ingesta	Estricto. Utilice siempre las ubicaciones de esta regla al ingerir. La ingesta falla si no es posible almacenar dos copias del objeto en el centro de datos de París.

Strict ingest to guarantee Paris data center

Compliant: Yes

Used in active policy: No

Used in proposed policy: No

Ingest behavior: Strict

Reference time: Ingest time

Clone

Edit

Remove

Filters

This rule applies if:

- Tenant is Paris tenant

And it only applies if objects have this metadata:

- Location constraint is eu-west-3

Time period and placements

Retention diagram

Placement instructions

Sort placements by

Time period

Storage pool

● Replicated copy

Rule analysis:

- StorageGRID site-loss protection will not apply from Day 0 - Forever.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Ingest behavior: Strict

Day 0

Day 0 - forever

2 replicated copies - Site 1

Duration

Forever

733

Regla 2 de ILM, por ejemplo 5: Ingesta equilibrada para otros objetos

Esta regla ILM de ejemplo utiliza el comportamiento de ingesta equilibrada para proporcionar una eficiencia ILM óptima para cualquier objeto que no coincida con la primera regla. Se almacenarán dos copias de todos los objetos que coincidan con esta regla: una en el centro de datos de EE. UU. y otra en el centro de datos de París. Si la regla no puede cumplirse inmediatamente, se almacenan copias provisionales en cualquier ubicación disponible.

Esta regla se aplica a los objetos que pertenecen a cualquier inquilino y a cualquier región.

Definición de regla	Valor de ejemplo
Cuenta de inquilino	Ignorar
Filtro avanzado	<i>No especificado</i>
Pools de almacenamiento	Sitio 1 (París) y Sitio 2 (EE. UU.)
Nombre de la regla	2 copias 2 centros de datos
Tiempo de referencia	Tiempo de ingesta
Colocaciones	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 ubicación de la regla, si es posible. De lo contrario, se realizan copias provisionales en cualquier lugar disponible.

Política ILM para el ejemplo 5: Combinación de comportamientos de ingesta

La política ILM de ejemplo incluye dos reglas que tienen diferentes comportamientos de ingesta.

Una política ILM que utiliza dos comportamientos de ingesta diferentes podría incluir reglas ILM como las siguientes:

- Almacene los objetos que pertenecen al inquilino de París y que tienen la región de depósito S3 configurada en eu-west-3 (París) solo en el centro de datos de París. Error en la ingesta si el centro de datos de París no está disponible.
- Almacene todos los demás objetos (incluidos aquellos que pertenecen al inquilino de París pero que tienen una región de depósito diferente) tanto en el centro de datos de EE. UU. como en el centro de datos de París. Haga copias provisionales en cualquier ubicación disponible si no se puede cumplir con las instrucciones de ubicación.

Al simular la política de ejemplo, espera que los objetos de prueba se evalúen de la siguiente manera:

- Todos los objetos que pertenecen al inquilino de París y que tienen la región de bucket S3 establecida en eu-west-3 coinciden con la primera regla y se almacenan en el centro de datos de París. Debido a que la primera regla utiliza ingesta estricta, estos objetos nunca se almacenan en el centro de datos de EE. UU. Si los nodos de almacenamiento en el centro de datos de París no están disponibles, la ingesta falla.

- Todos los demás objetos coinciden con la segunda regla, incluidos los objetos que pertenecen al inquilino de París y que no tienen la región de depósito S3 establecida en eu-west-3. Se guarda una copia de cada objeto en cada centro de datos. Sin embargo, debido a que la segunda regla utiliza ingesta equilibrada, si un centro de datos no está disponible, se guardan dos copias provisionales en cualquier ubicación disponible.

Ejemplo 6: Cambiar una política de ILM

Si necesita cambiar su protección de datos o agrega nuevos sitios, puede crear y activar una nueva política ILM.

Antes de cambiar una política, debe comprender cómo los cambios en las ubicaciones de ILM pueden afectar temporalmente el rendimiento general de un sistema StorageGRID .

En este ejemplo, se ha agregado un nuevo sitio StorageGRID en una expansión y se debe implementar una nueva política ILM activa para almacenar datos en el nuevo sitio. Para implementar una nueva política activa, primero ["crear una política"](#) . Después, debes ["simular"](#) y luego ["activar"](#) La nueva política.



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlrela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

Cómo afecta el cambio de una política de ILM al rendimiento

Cuando activa una nueva política ILM, el rendimiento de su sistema StorageGRID podría verse afectado temporalmente, especialmente si las instrucciones de ubicación de la nueva política requieren que muchos objetos existentes se muevan a nuevas ubicaciones.

Cuando activa una nueva política ILM, StorageGRID la utiliza para administrar todos los objetos, incluidos los objetos existentes y los objetos recientemente ingeridos. Antes de activar una nueva política ILM, revise cualquier cambio en la ubicación de los objetos replicados y codificados por borrado existentes. Cambiar la ubicación de un objeto existente podría generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.

Para garantizar que una nueva política de ILM no afecte la ubicación de los objetos replicados y codificados por borrado existentes, puede ["crear una regla ILM con un filtro de tiempo de ingesta"](#) . Por ejemplo, **La hora de ingesta es el o después de <fecha y hora>**, de modo que la nueva regla se aplica solo a los objetos ingeridos en o después de la fecha y hora especificadas.

Los tipos de cambios de política de ILM que pueden afectar temporalmente el rendimiento de StorageGRID incluyen los siguientes:

- Aplicar un perfil de codificación de borrado diferente a objetos con codificación de borrado existentes.



StorageGRID considera que cada perfil de codificación de borrado es único y no reutiliza fragmentos de codificación de borrado cuando se utiliza un nuevo perfil.

- Cambiar el tipo de copias necesarias para los objetos existentes; por ejemplo, convertir un gran porcentaje de objetos replicados en objetos con código de borrado.
- Mover copias de objetos existentes a una ubicación completamente diferente; por ejemplo, mover una gran cantidad de objetos hacia o desde un grupo de almacenamiento en la nube o hacia o desde un sitio remoto.

Política ILM activa, por ejemplo 6: Protección de datos en dos sitios

En este ejemplo, la política ILM activa se diseñó inicialmente para un sistema StorageGRID de dos sitios y utiliza dos reglas ILM.

Active policy

Policy history

Policy name:

Data Protection for Two Sites (2 rules)

Reason for change :

Data protection for two sites (using 2 rules)

Start date:

2022-10-11 10:37:11 MDT

Simulate

Policy rules

Retention diagram

Rule order ?	Rule name	Filters ?
1	One-Site Erasure Coding for Tenant A	Tenant is Tenant A
Default	Two-Site Replication for Other Tenants	—

En esta política ILM, los objetos que pertenecen al inquilino A están protegidos mediante codificación de borrado 2+1 en un solo sitio, mientras que los objetos que pertenecen a todos los demás inquilinos están protegidos en dos sitios mediante replicación de 2 copias.

Regla 1: Codificación de borrado de un sitio para el inquilino A

Definición de regla	Valor de ejemplo
Nombre de la regla	Codificación de borrado de un sitio para el inquilino A
Cuenta de inquilino	Inquilino A
Pool de almacenamiento	Sitio 1
Colocaciones	Codificación de borrado 2+1 en el Sitio 1 desde el día 0 hasta la eternidad

Regla 2: Replicación en dos sitios para otros inquilinos

Definición de regla	Valor de ejemplo
Nombre de la regla	Replicación de dos sitios para otros inquilinos
Cuenta de inquilino	Ignorar
Pools de almacenamiento	Sitio 1 y Sitio 2

Definición de regla	Valor de ejemplo
Colocaciones	Dos copias replicadas desde el día 0 hasta siempre: una copia en el Sitio 1 y una copia en el Sitio 2.

Política de ILM, ejemplo 6: Protección de datos en tres sitios

En este ejemplo, la política ILM se reemplaza por una nueva política para un sistema StorageGRID de tres sitios.

Después de realizar una expansión para agregar el nuevo sitio, el administrador de la red creó dos nuevos grupos de almacenamiento: un grupo de almacenamiento para el Sitio 3 y un grupo de almacenamiento que contiene los tres sitios (no el mismo que el grupo de almacenamiento predeterminado Todos los nodos de almacenamiento). Luego, el administrador creó dos nuevas reglas ILM y una nueva política ILM, diseñada para proteger los datos en los tres sitios.

Cuando se activa esta nueva política ILM, los objetos que pertenecen al Inquilino A estarán protegidos mediante codificación de borrado 2+1 en tres sitios, mientras que los objetos que pertenecen a otros inquilinos (y objetos más pequeños que pertenecen al Inquilino A) estarán protegidos en tres sitios mediante replicación de 3 copias.

Regla 1: Codificación de borrado de tres sitios para el inquilino A

Definición de regla	Valor de ejemplo
Nombre de la regla	Codificación de borrado de tres sitios para el inquilino A
Cuenta de inquilino	Inquilino A
Pool de almacenamiento	Los 3 sitios (incluye el Sitio 1, el Sitio 2 y el Sitio 3)
Colocaciones	Codificación de borrado 2+1 en los 3 sitios desde el día 0 hasta siempre

Regla 2: Replicación en tres sitios para otros inquilinos

Definición de regla	Valor de ejemplo
Nombre de la regla	Réplica de tres sitios para otros inquilinos
Cuenta de inquilino	Ignorar
Pools de almacenamiento	Sitio 1, Sitio 2 y Sitio 3
Colocaciones	Tres copias replicadas desde el día 0 hasta siempre: una copia en el Sitio 1, una copia en el Sitio 2 y una copia en el Sitio 3.

Activación de la política ILM por ejemplo 6

Cuando se activa una nueva política ILM, es posible que los objetos existentes se muevan a nuevas

ubicaciones o que se creen nuevas copias de objetos existentes, según las instrucciones de ubicación de cualquier regla nueva o actualizada.



Los errores en una política ILM pueden provocar una pérdida de datos irrecuperable. Revise cuidadosamente y simule la política antes de activarla para confirmar que funcionará según lo previsto.



Cuando activa una nueva política ILM, StorageGRID la utiliza para administrar todos los objetos, incluidos los objetos existentes y los objetos recientemente ingeridos. Antes de activar una nueva política ILM, revise cualquier cambio en la ubicación de los objetos replicados y codificados por borrado existentes. Cambiar la ubicación de un objeto existente podría generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.

¿Qué sucede cuando cambian las instrucciones de codificación de borrado?

En la política ILM actualmente activa para este ejemplo, los objetos que pertenecen al inquilino A están protegidos mediante codificación de borrado 2+1 en el sitio 1. En la nueva política ILM, los objetos que pertenecen al inquilino A estarán protegidos mediante codificación de borrado 2+1 en los sitios 1, 2 y 3.

Cuando se activa la nueva política ILM, se producen las siguientes operaciones ILM:

- Los nuevos objetos ingeridos por el inquilino A se dividen en dos fragmentos de datos y se agrega un fragmento de paridad. Luego, cada uno de los tres fragmentos se almacena en un sitio diferente.
- Los objetos existentes que pertenecen al inquilino A se vuelven a evaluar durante el proceso de escaneo ILM en curso. Debido a que las instrucciones de colocación de ILM utilizan un nuevo perfil de codificación de borrado, se crean fragmentos codificados de borrado completamente nuevos y se distribuyen a los tres sitios.



Los fragmentos 2+1 existentes en el Sitio 1 no se reutilizan. StorageGRID considera que cada perfil de codificación de borrado es único y no reutiliza fragmentos de codificación de borrado cuando se utiliza un nuevo perfil.

¿Qué sucede cuando cambian las instrucciones de replicación?

En la política ILM actualmente activa para este ejemplo, los objetos que pertenecen a otros inquilinos están protegidos mediante dos copias replicadas en grupos de almacenamiento en los sitios 1 y 2. En la nueva política de ILM, los objetos que pertenecen a otros inquilinos estarán protegidos mediante tres copias replicadas en grupos de almacenamiento en los sitios 1, 2 y 3.

Cuando se activa la nueva política ILM, se producen las siguientes operaciones ILM:

- Cuando cualquier inquilino que no sea el inquilino A ingiere un nuevo objeto, StorageGRID crea tres copias y guarda una copia en cada sitio.
- Los objetos existentes que pertenecen a estos otros inquilinos se vuelven a evaluar durante el proceso de escaneo ILM en curso. Dado que las copias de objetos existentes en el Sitio 1 y el Sitio 2 continúan satisfaciendo los requisitos de replicación de la nueva regla ILM, StorageGRID solo necesita crear una nueva copia del objeto para el Sitio 3.

Impacto en el rendimiento de la activación de esta política

Cuando se activa la política ILM en este ejemplo, el rendimiento general de este sistema StorageGRID se verá afectado temporalmente. Se requerirán niveles de recursos de red superiores a los normales para crear

nuevos fragmentos con código de borrado para los objetos existentes del Inquilino A y nuevas copias replicadas en el Sitio 3 para los objetos existentes de otros inquilinos.

Como resultado del cambio de política de ILM, las solicitudes de lectura y escritura del cliente podrían experimentar temporalmente latencias más altas de lo normal. Las latencias volverán a los niveles normales después de que las instrucciones de ubicación se implementen completamente en toda la red.

Para evitar problemas de recursos al activar una nueva política ILM, puede usar el filtro avanzado Tiempo de ingesta en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establezca el tiempo de ingesta para que sea mayor o igual al tiempo aproximado en que entrará en vigencia la nueva política para garantizar que los objetos existentes no se muevan innecesariamente.



Comuníquese con el soporte técnico si necesita reducir o aumentar la velocidad a la que se procesan los objetos después de un cambio de política de ILM.

Ejemplo 7: Política ILM compatible con el bloqueo de objetos S3

Puede usar el depósito S3, las reglas ILM y la política ILM en este ejemplo como punto de partida al definir una política ILM para cumplir con los requisitos de protección y retención de objetos para objetos en depósitos con el bloqueo de objetos S3 habilitado.



Si utilizó la función de Cumplimiento heredada en versiones anteriores de StorageGRID , también puede usar este ejemplo para ayudar a administrar cualquier depósito existente que tenga habilitada la función de Cumplimiento heredada.



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlere la para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas.

Información relacionada

- ["Administrar objetos con S3 Object Lock"](#)
- ["Crear una política ILM"](#)

Ejemplo de bloqueo de objetos y cubos para S3

En este ejemplo, una cuenta de inquilino S3 llamada Bank of ABC utilizó el Administrador de inquilinos para crear un depósito con el Bloqueo de objetos S3 habilitado para almacenar registros bancarios críticos.

Definición de cubo	Valor de ejemplo
Nombre de la cuenta del inquilino	Banco de ABC
Nombre del depósito	registros bancarios
Región del cubo	us-east-1 (predeterminado)

Cada objeto y versión de objeto que se agrega al depósito de registros bancarios utilizará los siguientes valores para `retain-until-date` y `legal hold` ajustes.

Configuración para cada objeto	Valor de ejemplo
<code>retain-until-date</code>	"2030-12-30T23:59:59Z" (30 de diciembre de 2030) Cada versión del objeto tiene su propia <code>retain-until-date</code> configuración. Este ajuste se puede aumentar, pero no disminuir.
<code>legal hold</code>	"OFF" (Sin efecto) Se puede colocar o levantar una retención legal sobre cualquier versión de un 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 <code>retain-until-date</code> Se ha alcanzado.

Ejemplo de regla 1 de ILM para bloqueo de objetos S3: Perfil de codificación de borrado con coincidencia de depósito

Esta regla ILM de ejemplo se aplica únicamente a la cuenta de inquilino S3 denominada Banco ABC. Coincide con cualquier objeto del `bank-records` y luego utiliza codificación de borrado para almacenar el objeto en nodos de almacenamiento en tres sitios de centros de datos utilizando un perfil de codificación de borrado 6+3. Esta regla satisface los requisitos de los depósitos con el bloqueo de objetos S3 habilitado: se conserva una copia en los nodos de almacenamiento desde el día 0 hasta siempre, utilizando el tiempo de ingesta como tiempo de referencia.

Definición de regla	Valor de ejemplo
Nombre de la regla	Norma de cumplimiento: Objetos CE en el contenedor de registros bancarios - Banco ABC
Cuenta de inquilino	Banco de ABC
Nombre del depósito	<code>bank-records</code>
Filtro avanzado	Tamaño del objeto (MB) mayor a 1 Nota: Este filtro garantiza que la codificación de borrado no se utilice para objetos de 1 MB o menos.

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Colocaciones	Desde el día 0 tienda para siempre
Perfil de codificación de borrado	• Cree una copia con código de borrado en los nodos de almacenamiento en tres sitios de centros de datos • Utiliza el esquema de codificación de borrado 6+3

Regla 2 de ILM para el ejemplo de bloqueo de objetos S3: regla no conforme

Esta regla ILM de ejemplo almacena inicialmente dos copias de objetos replicados en los nodos de almacenamiento. Después de un año, almacena una copia en un grupo de almacenamiento en la nube para siempre. Debido a que esta regla utiliza un grupo de almacenamiento en la nube, no es compatible y no se aplicará a los objetos en depósitos con el bloqueo de objetos S3 habilitado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Regla no conforme: utilizar el grupo de almacenamiento en la nube
Cuentas de inquilinos	No especificado
Nombre del depósito	No se especifica, pero solo se aplicará a los depósitos que no tengan habilitado el bloqueo de objetos S3 (o la función de cumplimiento heredada).
Filtro avanzado	No especificado

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Colocaciones	• El día 0, mantenga dos copias replicadas en los nodos de almacenamiento del centro de datos 1 y del centro de datos 2 durante 365 días • Después de 1 año, conserve una copia replicada en un grupo de almacenamiento en la nube para siempre

Regla 3 de ILM para el ejemplo de bloqueo de objetos S3: regla predeterminada

Esta regla ILM de ejemplo copia datos de objetos en grupos de almacenamiento en dos centros de datos. Esta regla de cumplimiento está diseñada para ser la regla predeterminada en la política ILM. No incluye ningún filtro, no utiliza el tiempo de referencia no actual y satisface los requisitos de los buckets con S3 Object Lock habilitado: se mantienen dos copias de objetos en los nodos de almacenamiento desde el día 0 hasta siempre, utilizando la ingesta como tiempo de referencia.

Definición de regla	Valor de ejemplo
Nombre de la regla	Regla de cumplimiento predeterminada: Dos copias, dos centros de datos
Cuenta de inquilino	No especificado
Nombre del depósito	No especificado
Filtro avanzado	No especificado

Definición de regla	Valor de ejemplo
Tiempo de referencia	Tiempo de ingesta
Colocaciones	Desde el día 0 y para siempre, conserve dos copias replicadas: una en los nodos de almacenamiento del centro de datos 1 y otra en los nodos de almacenamiento del centro de datos 2.

Ejemplo de política ILM compatible con bloqueo de objetos S3

Para crear una política ILM que proteja eficazmente todos los objetos de su sistema, incluidos aquellos en depósitos con el bloqueo de objetos S3 habilitado, debe seleccionar reglas ILM que satisfagan los requisitos de almacenamiento de todos los objetos. Luego debes simular y activar la política.

Agregar reglas a la política

En este ejemplo, la política ILM incluye tres reglas ILM, en el siguiente orden:

1. Una regla compatible que utiliza codificación de borrado para proteger objetos de más de 1 MB en un depósito específico con S3 Object Lock habilitado. Los objetos se almacenan en nodos de almacenamiento desde el día 0 hasta siempre.
2. Una regla no conforme que crea dos copias de objetos replicados en nodos de almacenamiento durante un año y luego mueve una copia de objeto a un grupo de almacenamiento en la nube para siempre. Esta regla no se aplica a los depósitos con el bloqueo de objetos S3 habilitado porque utiliza un grupo de almacenamiento en la nube.
3. La regla compatible predeterminada que crea dos copias de objetos replicados en los nodos de almacenamiento desde el día 0 hasta siempre.

Simular la política

Después de haber agregado reglas a su política, elegido una regla compatible predeterminada y organizado las otras reglas, debe simular la política probando objetos del depósito con S3 Object Lock habilitado y de otros depósitos. Por ejemplo, al simular la política de ejemplo, esperaría que los objetos de prueba se evaluarán de la siguiente manera:

- La primera regla solo coincidirá con objetos de prueba que tengan más de 1 MB en el depósito de registros bancarios para el inquilino del Banco de ABC.
- La segunda regla hará coincidir todos los objetos en todos los depósitos no compatibles para todas las demás cuentas de inquilino.
- La regla predeterminada coincidirá con estos objetos:
 - Objetos de 1 MB o menos en el depósito de registros bancarios para el inquilino del Banco ABC.
 - Objetos en cualquier otro depósito 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 como se esperaba, puede activarla.

Ejemplo 8: Prioridades para el ciclo de vida del depósito S3 y la política de ILM

Según la configuración de su ciclo de vida, los objetos siguen las configuraciones de retención del ciclo de vida del bucket S3 o de una política ILM.

Ejemplo de cómo el ciclo de vida del bucket tiene prioridad sobre la política de ILM

Política de ILM

- Regla basada en una referencia temporal no actual: el día 0, conservar X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminada): el día 0, conservar X copias durante 50 días

Ciclo de vida del bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},  
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Resultado

- Se ingiere un objeto llamado "docs/text". Coincide con el filtro del ciclo de vida del depósito del prefijo "docs/".
 - Después de 100 días, se crea un marcador de eliminación y "docs/text" deja de estar actualizado.
 - Después de 5 días, un total de 105 días desde la ingesta, se elimina "docs/text".
 - Después de 95 días, un total de 200 días desde la ingesta y 100 días desde que se creó el marcador de eliminación, se elimina el marcador de eliminación vencido.
- Se ingiere un objeto llamado "video/película". No coincide con el filtro y utiliza la política de retención ILM.
 - Después de 50 días, se crea un marcador de eliminación y el archivo "video/película" deja de estar vigente.
 - Después de 20 días, un total de 70 días desde la ingesta, se elimina "video/película".
 - Después de 30 días, un total de 100 días desde la ingesta y 50 días desde que se creó el marcador de eliminación, se elimina el marcador de eliminación vencido.

Ejemplo de ciclo de vida de un bucket que implícitamente se mantiene para siempre

Política de ILM

- Regla basada en una referencia temporal no actual: el día 0, conservar X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminada): el día 0, conservar X copias durante 50 días

Ciclo de vida del bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":  
true}
```

Resultado

- Se ingiere un objeto llamado "docs/text". Coincide con el filtro del ciclo de vida del depósito del prefijo "docs/".

El `Expiration` La acción se aplica solo a los marcadores de eliminación vencidos, lo que implica mantener todo lo demás para siempre (comenzando con "docs/").

Los marcadores de eliminación que comienzan con "docs/" se eliminan cuando caducan.

- Se ingiere un objeto llamado "video/película". No coincide con el filtro y utiliza la política de retención ILM.
 - Después de 50 días, se crea un marcador de eliminación y el archivo "video/película" deja de estar vigente.
 - Después de 20 días, un total de 70 días desde la ingesta, se elimina "video/película".
 - Después de 30 días, un total de 100 días desde la ingesta y 50 días desde que se creó el marcador de eliminación, se elimina el marcador de eliminación vencido.

Ejemplo de uso del ciclo de vida del bucket para duplicar ILM y limpiar marcadores de eliminación vencidos

Política de ILM

- Regla basada en una referencia temporal no actual: el día 0, conservar X copias durante 20 días
- Regla basada en la referencia de tiempo de ingesta (predeterminada): el día 0, conservar X copias para siempre

Ciclo de vida del bucket

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},  
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Resultado

- La política ILM se duplica en el ciclo de vida del depósito.
 - La regla permanente de la política ILM está diseñada para eliminar objetos manualmente y limpiar versiones no actuales después de 20 días. En consecuencia, la regla de tiempo de ingesta mantendrá los marcadores de eliminación vencidos para siempre.
 - El ciclo de vida del depósito duplica el comportamiento de la política ILM al agregar "ExpiredObjectDeleteMarker": true, que elimina los marcadores de eliminación una vez que han expirado
- Se ingiere un objeto. Sin filtro significa que el ciclo de vida del depósito se aplica a todos los objetos y anula las configuraciones de retención de ILM.
 - Cuando un inquilino emite una solicitud de eliminación de un objeto, se crea un marcador de eliminación y el objeto deja de ser actual.
 - Después de 20 días, el objeto no actual se elimina y el marcador de eliminación caduca.
 - Poco después, se elimina el marcador de eliminación caducado.

Endurecimiento del sistema

Consideraciones generales para el fortalecimiento del sistema

El fortalecimiento del sistema es el proceso de eliminar tantos riesgos de seguridad como sea posible de un sistema StorageGRID .

A medida que instala y configura StorageGRID, utilice estas pautas para ayudarlo a cumplir con los objetivos de seguridad prescritos en materia de confidencialidad, integridad y disponibilidad.

Ya debería estar utilizando las mejores prácticas estándar de la industria para el fortalecimiento del sistema. Por ejemplo, utiliza contraseñas seguras para StorageGRID, usa HTTPS en lugar de HTTP y habilita la

autenticación basada en certificados cuando esté disponible.

StorageGRID sigue las ["Política de gestión de vulnerabilidades de NetApp"](#) . Las vulnerabilidades reportadas se verifican y abordan de acuerdo con el proceso de respuesta a incidentes de seguridad del producto.

Al fortalecer un sistema StorageGRID , tenga en cuenta lo siguiente:

- ¿*Cuál de las tres redes StorageGRID * ha implementado? Todos los sistemas StorageGRID deben usar la red Grid, pero también es posible que utilice 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 en su sistema StorageGRID . Los nodos StorageGRID se pueden implementar en máquinas virtuales VMware, dentro de 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 fortalecimiento.
- **Qué tan confiables son las cuentas de los inquilinos.** Si usted es un proveedor de servicios con cuentas de inquilinos que no son de confianza, tendrá preocupaciones de seguridad diferentes que si solo utiliza inquilinos internos y de confianza.
- **Qué requisitos y convenciones de seguridad** sigue su organización. Es posible que deba cumplir con requisitos corporativos o regulatorios específicos.

Pautas de refuerzo para las actualizaciones de software

Debe mantener su sistema StorageGRID y los servicios relacionados actualizados para defenderse de los ataques.

Actualizaciones del software StorageGRID

Siempre que sea posible, debe actualizar el software StorageGRID a la versión principal más reciente o a la versión principal anterior. Mantener StorageGRID actualizado ayuda a reducir la cantidad de tiempo que las vulnerabilidades conocidas están activas y reduce la superficie de ataque general. Además, las versiones más recientes de StorageGRID a menudo contienen funciones de refuerzo de seguridad que no están incluidas en versiones anteriores.

Consultar el ["Herramienta de matriz de interoperabilidad de NetApp"](#) (IMT) para determinar qué versión del software StorageGRID debería utilizar. Cuando se requiere una revisión, 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 revisiones más recientes de StorageGRID , vaya a ["Descargas de NetApp : StorageGRID"](#) .
- Para actualizar el software StorageGRID , consulte la ["instrucciones de actualización"](#) .
- Para aplicar una revisión, consulte la ["Procedimiento de revisión de StorageGRID"](#) .

Actualizaciones de servicios externos

Los servicios externos pueden tener vulnerabilidades que afecten a StorageGRID indirectamente. Debe asegurarse de que los servicios de los que depende StorageGRID se mantengan actualizados. Estos servicios incluyen LDAP, KMS (o servidor KMIP), DNS y NTP.

Para obtener una lista de las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp"](#) .

Actualizaciones de hipervisores

Si sus nodos StorageGRID se ejecutan en VMware u otro hipervisor, debe asegurarse de que el software y el firmware del hipervisor estén actualizados.

Para obtener una lista de las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp"](#) .

Actualizaciones a nodos Linux

Si sus nodos StorageGRID utilizan plataformas de host Linux, debe asegurarse de que las actualizaciones de seguridad y las actualizaciones del kernel se apliquen al sistema operativo host. Además, debe aplicar actualizaciones de firmware al hardware vulnerable cuando estas actualizaciones estén disponibles.

Para obtener una lista de las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp"](#) .

Pautas de fortalecimiento para redes StorageGRID

El sistema StorageGRID admite hasta tres interfaces de red por nodo de red, lo que le permite configurar la red para cada nodo de red individual para que coincida con sus requisitos de seguridad y acceso.

Para obtener información detallada sobre las redes StorageGRID , consulte la ["Tipos de red StorageGRID"](#) .

Directrices para la red Grid

Debe configurar una red Grid para todo el tráfico interno de StorageGRID . Todos los nodos de la red están en la red de red y deben poder comunicarse con todos los demás nodos.

Al configurar la red Grid, siga estas pautas:

- Asegúrese de que la red esté protegida contra clientes que no sean de confianza, como aquellos en Internet abierto.
- Cuando sea posible, utilice la red Grid 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 la red Grid 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 Grid para brindar protección adicional para el tráfico interno.
- Algunos procedimientos de mantenimiento requieren acceso a shell seguro (SSH) en el puerto 22 entre el nodo de administración principal y todos los demás nodos de la red. Utilice un firewall externo para restringir el acceso SSH a clientes confiables.

Pautas para la red de administración

La red de administración generalmente se utiliza 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 internamente.

Si está utilizando la red de administración, siga estas pautas:

- Bloquear todos los puertos de tráfico interno en la red de administración. Ver el ["lista de puertos internos"](#) .
- Si los clientes no confiables 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 normalmente se utiliza para inquilinos y para comunicarse con servicios externos, como el servicio de replicación CloudMirror u otro servicio de plataforma. Sin embargo, StorageGRID no exige este uso internamente.

Si está utilizando la red de cliente, siga estas pautas:

- Bloquear todos los puertos de tráfico interno en la red del cliente. Ver el ["lista de puertos internos"](#) .
- Acepte el tráfico de clientes entrante solo en puntos finales configurados explícitamente. Ver la información sobre ["gestión de controles de firewall"](#) .

Pautas de refuerzo para nodos StorageGRID

Los nodos StorageGRID se pueden implementar en máquinas virtuales VMware, dentro de 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 mejores prácticas de fortalecimiento.

Controlar el acceso remoto de IPMI a BMC

Puede habilitar o deshabilitar el acceso IPMI remoto para todos los dispositivos que contengan un BMC. La interfaz IPMI remota permite el acceso de hardware de bajo nivel a sus dispositivos StorageGRID por parte de cualquier persona con una cuenta y contraseña de BMC . Si no necesita acceso IPMI remoto al BMC, desactive esta opción.

- Para controlar el acceso remoto de IPMI al BMC en Grid Manager, vaya a **CONFIGURACIÓN > Seguridad > Configuración de seguridad > Dispositivos**:
 - Desmarque la casilla de verificación **Habilitar acceso IPMI remoto** para deshabilitar el acceso IPMI al BMC.
 - Seleccione la casilla de verificación **Habilitar acceso IPMI remoto** para habilitar el acceso IPMI al BMC.

Configuración del firewall

Como parte del proceso de fortalecimiento del sistema, debe revisar las configuraciones del firewall externo y modificarlas para que el tráfico se acepte solo desde las direcciones IP y en los puertos desde los que es estrictamente necesario.

StorageGRID incluye un firewall interno en cada nodo que mejora la seguridad de su red al permitirle controlar el acceso de la red al nodo. Debería ["Administrar los controles internos del firewall"](#) para evitar el acceso a la red en todos los puertos excepto aquellos necesarios para su implementación de red específica. Los cambios de configuración que realice en la página de control del Firewall se implementarán en cada nodo.

En concreto, puedes gestionar estas áreas:

- **Direcciones privilegiadas**: puede permitir que direcciones IP o subredes seleccionadas accedan a puertos que estén cerrados por la configuración en la pestaña Administrar acceso externo.

- **Administrar acceso externo:** puedes cerrar puertos que están abiertos por defecto, o reabrir puertos previamente cerrados.
- **Red de cliente no confiable:** puede especificar si un nodo confía en el tráfico entrante de la red de cliente, así como los puertos adicionales que desea que estén abiertos cuando se configura la red de cliente no confiable.

Si bien este firewall interno proporciona una capa adicional de protección contra algunas amenazas comunes, no elimina la necesidad de un firewall externo.

Para obtener una lista de todos los puertos internos y externos utilizados por StorageGRID, consulte ["Referencia del puerto de red"](#).

Deshabilitar servicios no utilizados

Para todos los nodos de StorageGRID, debe deshabilitar o bloquear el acceso a los servicios no utilizados. Por ejemplo, si no planea utilizar DHCP, utilice el Administrador de cuadrícula para cerrar el puerto 68. Seleccione **CONFIGURACIÓN > Control de firewall > Administrar acceso externo**. A continuación, cambie el interruptor de estado del puerto 68 de **Abierto** a **Cerrado**.

Virtualización, contenedores y hardware compartido

Para todos los nodos de StorageGRID, evite ejecutar StorageGRID en el mismo hardware físico que software no confiable. No asuma que las protecciones del hipervisor evitarán que el malware acceda a los datos protegidos por StorageGRID si tanto StorageGRID como el malware existen en el mismo hardware físico. Por ejemplo, los ataques Meltdown y Spectre explotan vulnerabilidades críticas en los procesadores modernos y permiten que los programas roben datos de la memoria de la misma computadora.

Proteger los nodos durante la instalación

No permita que usuarios no confiables accedan a los nodos de StorageGRID a través de la red cuando se estén instalando los nodos. Los nodos no son completamente seguros hasta que se unen a la red.

Pautas para los nodos de administración

Los nodos de administración brindan servicios de gestión como configuración del sistema, monitoreo y registro. Cuando inicia sesión en Grid Manager o Tenant Manager, se conecta a un nodo de administración.

Siga estas pautas para proteger los nodos de administración en su sistema StorageGRID :

- Proteja todos los nodos de administración de clientes que no sean de confianza, como aquellos en Internet abierto. Asegúrese de que ningún cliente no confiable pueda acceder a ningún nodo de administración en la red Grid, la red de administración o la red de clientes.
- Los grupos de StorageGRID controlan el acceso a las funciones de Grid Manager y Tenant Manager. Otorgue a cada grupo de usuarios los permisos mínimos requeridos para su rol y utilice el modo de acceso de solo lectura para evitar que los usuarios cambien la configuración.
- Al utilizar puntos finales del balanceador de carga StorageGRID, utilice nodos de puerta de enlace en lugar de nodos de administración para el tráfico de clientes que no sean de confianza.
- Si tiene inquilinos que no son de confianza, no les permita tener acceso directo al Administrador de inquilinos ni a la API de administración de inquilinos. En su lugar, haga que los inquilinos que no sean de confianza utilicen un portal de inquilinos o un sistema de gestión de inquilinos externo, que interactúe con la API de gestión de inquilinos.
- Opcionalmente, utilice un proxy de administración para tener más control sobre la comunicación de

AutoSupport desde los nodos de administración al soporte de NetApp . Vea los pasos para ["creando un proxy de administrador"](#) .

- Opcionalmente, utilice los puertos restringidos 8443 y 9443 para separar las comunicaciones entre Grid Manager y Tenant Manager. Bloquee el puerto compartido 443 y limite las solicitudes de inquilinos al puerto 9443 para obtener protección adicional.
- De manera opcional, utilice nodos de administración separados para administradores de red y usuarios inquilinos.

Para obtener más información, consulte las instrucciones para ["administración de StorageGRID"](#) .

Directrices para nodos de almacenamiento

Los nodos de almacenamiento administran y almacenan datos de objetos y metadatos. Siga estas pautas para proteger los nodos de almacenamiento en su sistema StorageGRID .

- No permita que clientes no confiables se conecten directamente a los nodos de almacenamiento. Utilice un punto final de balanceador de carga atendido por un nodo de puerta de enlace o un balanceador de carga de terceros.
- No habilite servicios salientes para inquilinos que no sean de confianza. Por ejemplo, al crear la cuenta para un inquilino que no es de confianza, no permita que el inquilino use su propia fuente de identidad y no permita el uso de los servicios de la plataforma. Vea los pasos para ["crear una cuenta de inquilino"](#) .
- Utilice un balanceador de carga de terceros para el tráfico de clientes que no sean de confianza. El equilibrio de carga de terceros ofrece más control y capas adicionales de protección contra ataques.
- De manera opcional, utilice un proxy de almacenamiento para tener más control sobre los grupos de almacenamiento en la nube y la comunicación de los servicios de la plataforma desde los nodos de almacenamiento a los servicios externos. Vea los pasos para ["creando un proxy de almacenamiento"](#) .
- Opcionalmente, conéctese a servicios externos utilizando la red del cliente. Luego, seleccione **CONFIGURACIÓN > Seguridad > Control de firewall > Redes de cliente no confiables** e indique que la red de cliente en el nodo de almacenamiento no es confiable. El nodo de almacenamiento ya no acepta tráfico entrante en la red del cliente, pero continúa permitiendo solicitudes salientes para los servicios de plataforma.

Directrices para los nodos de enlace

Los nodos de puerta de enlace proporcionan una interfaz de equilibrio de carga opcional que las aplicaciones cliente pueden usar para conectarse a StorageGRID. Siga estas pautas para proteger cualquier nodo de puerta de enlace en su sistema StorageGRID :

- Configurar y utilizar puntos finales del balanceador de carga. Ver ["Consideraciones para el equilibrio de carga"](#) .
- Utilice un equilibrador de carga de terceros entre el cliente y el nodo de puerta de enlace o los nodos de almacenamiento para el tráfico de clientes no confiables. El equilibrio de carga de terceros ofrece más control y capas adicionales de protección contra ataques. Si utiliza un balanceador de carga de terceros, el tráfico de red puede configurarse opcionalmente para pasar por un punto final del balanceador de carga interno o enviarse directamente a los nodos de almacenamiento.
- Si está utilizando puntos finales de balanceador de carga, opcionalmente puede hacer que los clientes se conecten a través de la red del cliente. Luego, seleccione **CONFIGURACIÓN > Seguridad > Control de firewall > Redes de clientes no confiables** e indique que la red de clientes en el nodo de puerta de enlace no es confiable. El nodo de puerta de enlace solo acepta tráfico entrante en los puertos configurados explícitamente como puntos finales del equilibrador de carga.

Directrices para los nodos de dispositivos de hardware

Los dispositivos de hardware StorageGRID están diseñados especialmente para su uso en un sistema StorageGRID. Algunos dispositivos pueden utilizarse como nodos de almacenamiento. Se pueden utilizar otros dispositivos como nodos de administración o nodos de puerta de enlace. Puede combinar nodos de dispositivos con nodos basados en software o implementar redes de dispositivos completamente diseñadas.

Siga estas pautas para proteger cualquier nodo de dispositivo de hardware en su sistema StorageGRID :

- Si el dispositivo utiliza SANtricity System Manager para la administración del controlador de almacenamiento, evite que los clientes no confiables accedan a SANtricity System Manager 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 de BMC permite el acceso al hardware de bajo nivel. Conecte el puerto de administración de BMC únicamente a una red de administración interna segura y confiable. Si no hay dicha red disponible, deje el puerto de administración de BMC desconectado o bloqueado, a menos que el soporte técnico solicite una conexión de BMC.
- Si el dispositivo admite la administración remota del hardware del controlador a través de Ethernet utilizando el estándar de Interfaz de administración de plataforma inteligente (IPMI), bloquee el tráfico no confiable en el puerto 623.



Puede habilitar o deshabilitar el acceso IPMI remoto para todos los dispositivos que contengan un BMC. La interfaz IPMI remota permite el acceso de hardware de bajo nivel a sus dispositivos StorageGRID por parte de cualquier persona con una cuenta y contraseña de BMC. Si no necesita acceso IPMI remoto al BMC, deshabilite esta opción utilizando uno de los siguientes métodos: + En Grid Manager, vaya a **CONFIGURACIÓN > Seguridad > Configuración de seguridad > Dispositivos** y desmarque la casilla de verificación **Habilitar acceso IPMI remoto**. + En la API de administración de Grid, use el punto final privado: PUT /private/bmc .

- Para los modelos de dispositivos que contienen unidades SED, FDE o FIPS NL-SAS que administra con SANtricity System Manager, "[Habilitar y configurar SANtricity Drive Security](#)".
- Para los modelos de dispositivos que contienen SSD NVMe SED o FIPS que administra mediante el instalador de dispositivos StorageGRID y el administrador de red, "[Habilitar y configurar el cifrado de unidad StorageGRID](#)".
- Para dispositivos sin unidades SED, FDE o FIPS, habilite y configure el cifrado del nodo de software StorageGRID "[utilizando un servidor de administración de claves \(KMS\)](#)".

Pautas de refuerzo para TLS y SSH

Debe reemplazar los certificados predeterminados creados durante la instalación y seleccionar la política de seguridad adecuada para las conexiones TLS y SSH.

Directrices de endurecimiento de los certificados

Debe reemplazar los certificados predeterminados creados durante la instalación con sus propios certificados personalizados.

Para muchas organizaciones, el certificado digital autofirmado para el acceso web de StorageGRID no cumple con sus políticas de seguridad de la información. En los sistemas de producción, debe instalar un certificado digital firmado por una CA para usarlo en la autenticación de StorageGRID.

En concreto, debe utilizar certificados de servidor personalizados en lugar de estos certificados predeterminados:

- **Certificado de interfaz de administración:** se utiliza para proteger el acceso al Administrador de Grid, al Administrador de inquilinos, a la API de administración de Grid y a la API de administración de inquilinos.
- **Certificado API S3:** se utiliza para proteger el acceso a los nodos de almacenamiento y los nodos de puerta de enlace, que las aplicaciones cliente S3 utilizan para cargar y descargar datos de objetos.

Ver ["Administrar certificados de seguridad"](#) para obtener más detalles e instrucciones.



StorageGRID administra los certificados utilizados para los puntos finales del equilibrador de carga por separado. Para configurar los certificados del balanceador de carga, consulte ["Configurar los puntos finales del balanceador de carga"](#).

Al utilizar certificados de servidor personalizados, siga estas pautas:

- Los certificados deben tener una *subjectAltName* que coincide con las entradas DNS para StorageGRID. Para obtener más detalles, consulte la sección 4.2.1.6, "Nombre alternativo del sujeto", en ["RFC 5280: Certificado PKIX y perfil CRL"](#).
- Siempre que sea posible, evite el uso de certificados comodín. Una excepción a esta directriz es el certificado para un punto final de estilo alojado virtual S3, que requiere el uso de un comodín si los nombres de los depósitos no se conocen de antemano.
- Cuando sea necesario utilizar comodines en los certificados, deberá tomar medidas adicionales para reducir los riesgos. Utilice un patrón comodín como `*.s3.example.com`, y no utilices el `s3.example.com` sufijo para otras aplicaciones. Este patrón también funciona con acceso S3 de estilo de ruta, como `dc1-s1.s3.example.com/mybucket`.
- Establezca tiempos de vencimiento de certificados cortos (por ejemplo, 2 meses) y utilice la API de administración de cuadrícula para automatizar la rotación de certificados. Esto es especialmente importante para los certificados comodín.

Además, los clientes deben utilizar una verificación estricta del nombre de host al comunicarse con StorageGRID.

Directrices de endurecimiento de las políticas TLS y SSH

Puede seleccionar una política de seguridad para determinar qué protocolos y cifrados se utilizan para establecer conexiones TLS seguras con aplicaciones cliente y conexiones SSH seguras con servicios internos de StorageGRID.

La política de seguridad controla cómo TLS y SSH cifran los datos en movimiento. Como práctica recomendada, debe deshabilitar las opciones de cifrado que no sean necesarias para la compatibilidad de la aplicación. Utilice la política moderna predeterminada, a menos que su sistema necesite cumplir con los Criterios comunes o necesite utilizar otros cifrados.

Ver ["Administrar la política TLS y SSH"](#) para obtener detalles e instrucciones.

Otras pautas de endurecimiento

Además de seguir las pautas de fortalecimiento para las redes y los nodos de StorageGRID, debe seguir las pautas de fortalecimiento para otras áreas del sistema StorageGRID.

Contraseña de instalación temporal

Para proteger el sistema StorageGRID durante la instalación, configure una contraseña en la página de contraseña del instalador temporal en la interfaz de usuario de instalación de StorageGRID o en la API de instalación. Cuando se configura, esta contraseña se aplica a todos los métodos para instalar StorageGRID, incluida la interfaz de usuario, la API de instalación y `configure-storagegrid.py` guion.

Para obtener más información, consulte:

- ["Instalar StorageGRID en Red Hat Enterprise Linux"](#)
- ["Instalar StorageGRID en Ubuntu o Debian"](#)
- ["Instalar StorageGRID en VMware"](#)
- ["Instalar el dispositivo StorageGRID"](#)

Registros y mensajes de auditoría

Proteja siempre los registros de StorageGRID y la salida de mensajes de auditoría de manera segura. Los registros y mensajes de auditoría de StorageGRID proporcionan información invaluable desde el punto de vista de soporte y disponibilidad del sistema. Además, la información y los detalles contenidos en los registros de StorageGRID y en los mensajes de auditoría resultantes generalmente son de naturaleza confidencial.

Configure StorageGRID para enviar eventos de seguridad a un servidor syslog externo. Si utiliza la exportación de syslog, seleccione TLS y RELP/TLS para los protocolos de transporte.

Ver el ["Referencia de archivos de registro"](#) para obtener más información sobre los registros de StorageGRID .
Ver ["Mensajes de auditoría"](#) para obtener más información sobre los mensajes de auditoría de StorageGRID .

AutoSupport de NetApp

La función AutoSupport de StorageGRID le permite monitorear de manera proactiva el estado de su sistema y enviar paquetes automáticamente al sitio de soporte de NetApp , al equipo de soporte interno de su organización o a un socio de soporte. De forma predeterminada, el envío de paquetes de AutoSupport a NetApp está habilitado cuando StorageGRID se configura por primera vez.

La función AutoSupport se puede desactivar. Sin embargo, NetApp recomienda habilitarlo porque AutoSupport ayuda a acelerar la identificación y resolución de problemas en caso de que surja un problema en su sistema StorageGRID .

AutoSupport admite HTTPS, HTTP y SMTP como protocolos de transporte. Debido a la naturaleza sensible de los paquetes de AutoSupport , NetApp recomienda enfáticamente utilizar HTTPS como protocolo de transporte predeterminado para enviar paquetes de AutoSupport a NetApp.

Intercambio de recursos entre orígenes (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un bucket S3 si desea que ese bucket y los objetos que contiene sean accesibles para las aplicaciones web en otros dominios. En general, no habilite CORS a menos que sea necesario. Si se requiere CORS, límitelo a orígenes confiables.

Vea los pasos para ["Configuración del uso compartido de recursos entre orígenes \(CORS\)"](#) .

Dispositivos de seguridad externos

Una solución de fortalecimiento completa 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 eficaz de establecer y mantener una postura de seguridad estricta. Estos dispositivos de seguridad externos incluyen firewalls, sistemas de prevención de intrusiones (IPS) y otros dispositivos de seguridad.

Se recomienda un balanceador de carga de terceros para el tráfico de clientes que no son confiables. El equilibrio de carga de terceros ofrece más control y capas adicionales de protección contra ataques.

Mitigación de ransomware

Ayude a proteger los datos de sus objetos de los ataques de ransomware siguiendo las recomendaciones en ["Defensa contra ransomware con StorageGRID"](#).

Configurar StorageGRID para FabricPool

Configurar StorageGRID para FabricPool

Si utiliza el software NetApp ONTAP, puede utilizar NetApp FabricPool para agrupar datos inactivos en un sistema de almacenamiento de objetos NetApp StorageGRID.

Utilice estas instrucciones para:

- Conozca las consideraciones y las mejores prácticas para configurar StorageGRID para una carga de trabajo de FabricPool.
- Aprenda a configurar un sistema de almacenamiento de objetos StorageGRID para su uso con FabricPool.
- Aprenda cómo proporcionar los valores necesarios a ONTAP al adjuntar StorageGRID como un nivel de nube de FabricPool.

Inicio rápido para configurar StorageGRID para FabricPool

1

Planifique su configuración

- Decida qué política de niveles de volumen de FabricPool utilizará para organizar en niveles los datos inactivos de ONTAP en StorageGRID.
- Planifique e instale un sistema StorageGRID para satisfacer sus necesidades de capacidad de almacenamiento y rendimiento.
- Familiarícese con el software del sistema StorageGRID, incluido el ["Administrador de red"](#) y el ["Administrador de inquilinos"](#).
- Revise las mejores prácticas de FabricPool para ["Grupos HA"](#), ["balanceo de carga"](#), ["ILM"](#), y ["más"](#).
- Revise estos recursos adicionales, que brindan detalles sobre el uso y la configuración de ONTAP y FabricPool:

["TR-4598: Mejores prácticas de FabricPool en ONTAP"](#)

["Documentación de ONTAP para FabricPool"](#)

2

Realizar tareas previas

Obtener el ["Información necesaria para adjuntar StorageGRID como un nivel de nube"](#), incluido:

- Direcciones IP
- Nombres de dominio
- Certificado SSL

Opcionalmente, configure ["federación de identidades"](#) y ["inicio de sesión único"](#) .

3

Configurar los ajustes de StorageGRID

Utilice StorageGRID para obtener los valores que ONTAP necesita para conectarse a la red.

Usando el ["Asistente de configuración de FabricPool"](#) Es la forma recomendada y más rápida de configurar todos los elementos, pero también puedes configurar cada entidad manualmente, si es necesario.

4

Configurar ONTAP y DNS

Utilice ONTAP para ["añadir un nivel de nube"](#) que utiliza los valores StorageGRID . Entonces, ["configurar entradas DNS"](#) para asociar direcciones IP a cualquier nombre de dominio que planea utilizar.

5

Monitorear y gestionar

Cuando su sistema esté en funcionamiento, realice tareas continuas en ONTAP y StorageGRID para administrar y monitorear la clasificación de datos de FabricPool a lo largo del tiempo.

¿Qué es FabricPool?

FabricPool es una solución de almacenamiento híbrido ONTAP que utiliza un agregado flash de alto rendimiento como nivel de rendimiento y un almacén de objetos como nivel de nube. El uso de agregados habilitados FabricPool le ayuda a reducir el costo de almacenamiento sin comprometer el rendimiento, la eficiencia ni la protección.

FabricPool asocia un nivel de nube (un almacén de objetos externo, como StorageGRID) con un nivel local (un agregado de almacenamiento ONTAP) para crear una colección compuesta de discos. Los volúmenes dentro de FabricPool pueden aprovechar la clasificación en niveles al mantener los datos activos (calientes) en un almacenamiento de alto rendimiento (el nivel local) y clasificar los datos inactivos (fríos) en el almacén de objetos externo (el nivel de nube).

No se requieren cambios arquitectónicos y puede continuar administrando sus datos y entorno de aplicaciones desde el sistema de almacenamiento central ONTAP .

¿Qué es StorageGRID?

NetApp StorageGRID es una arquitectura de almacenamiento que administra los datos como objetos, a diferencia de otras arquitecturas de almacenamiento como el almacenamiento de archivos o bloques. Los objetos se guardan dentro de un único contenedor (como un bucket) y no están anidados como archivos dentro de un directorio dentro de otros directorios. Aunque el almacenamiento de objetos generalmente ofrece un rendimiento menor que el almacenamiento de archivos o bloques, es significativamente más escalable. Los depósitos StorageGRID pueden contener petabytes de datos y miles de millones de objetos.

¿Por qué utilizar StorageGRID como un nivel de nube de FabricPool ?

FabricPool puede organizar datos de ONTAP en varios proveedores de almacenamiento de objetos, incluido StorageGRID. A diferencia de las nubes públicas, que pueden establecer una cantidad máxima de operaciones de entrada/salida admitidas por segundo (IOPS) a nivel de contenedor o bucket, el rendimiento de StorageGRID se escala con la cantidad de nodos en un sistema. El uso de StorageGRID como un nivel de nube de FabricPool le permite mantener sus datos fríos en su propia nube privada para obtener el máximo rendimiento y un control total sobre sus datos.

Además, no se requiere una licencia de FabricPool cuando se utiliza StorageGRID como nivel de nube.

Información necesaria para adjuntar StorageGRID como un nivel de nube

Antes de poder adjuntar StorageGRID como un nivel de nube para FabricPool, debe realizar pasos de configuración en StorageGRID y obtener ciertos valores para usar en ONTAP.

¿Qué valores necesito?

La siguiente tabla muestra los valores que debe configurar en StorageGRID y cómo ONTAP y el servidor DNS utilizan esos valores.

Valor	Donde se configura el valor	Dónde se utiliza el valor
Direcciones IP virtuales (VIP)	StorageGRID > Grupo de alta disponibilidad	Entrada DNS
Puerto	StorageGRID > Punto final del balanceador de carga	Administrador del sistema ONTAP > Agregar nivel de nube
Certificado SSL	StorageGRID > Punto final del balanceador de carga	Administrador del sistema ONTAP > Agregar nivel de nube
Nombre del servidor (FQDN)	StorageGRID > Punto final del balanceador de carga	Entrada DNS
ID de clave de acceso y clave de acceso secreta	StorageGRID > Inquilino y depósito	Administrador del sistema ONTAP > Agregar nivel de nube
Nombre del cubo/contenedor	StorageGRID > Inquilino y depósito	Administrador del sistema ONTAP > Agregar nivel de nube

¿Cómo obtengo estos valores?

Dependiendo de sus necesidades, puede realizar cualquiera de las siguientes acciones para obtener la información que necesita:

- Utilice el "[Asistente de configuración de FabricPool](#)". El asistente de configuración de FabricPool lo ayuda a configurar rápidamente los valores necesarios en StorageGRID y genera un archivo que puede usar para configurar ONTAP System Manager. El asistente lo guía a través de los pasos necesarios y lo ayuda a garantizar que su configuración se ajuste a las mejores prácticas de StorageGRID y FabricPool .

- Configure cada elemento manualmente. Luego, ingrese los valores en el Administrador del sistema ONTAP o en la CLI de ONTAP . Siga estos pasos:
 - a. ["Configurar un grupo de alta disponibilidad \(HA\) para FabricPool"](#) .
 - b. ["Crear un punto final de balanceador de carga para FabricPool"](#) .
 - c. ["Crear una cuenta de inquilino para FabricPool"](#) .
 - d. Sign in en la cuenta del inquilino y ["Crea el depósito y las claves de acceso para el usuario raíz"](#) .
 - e. Cree una regla ILM para los datos de FabricPool y agréguela a sus políticas ILM activas. Ver ["Configurar ILM para datos de FabricPool"](#) .
 - f. Opcionalmente, ["crear una política de clasificación de tráfico para FabricPool"](#) .

Utilice el asistente de configuración de FabricPool

Utilizar el asistente de configuración de FabricPool : Consideraciones y requisitos

Puede utilizar el asistente de configuración de FabricPool para configurar StorageGRID como el sistema de almacenamiento de objetos para un nivel de nube de FabricPool . Después de completar el asistente de configuración, puede ingresar los detalles necesarios en ONTAP System Manager.

Cuándo utilizar el asistente de configuración de FabricPool

El asistente de configuración de FabricPool lo guía a través de cada paso de la configuración de StorageGRID para su uso con FabricPool y configura automáticamente ciertas entidades para usted, como las políticas de clasificación de tráfico e ILM. Como parte de completar el asistente, descargará un archivo que puede usar para ingresar valores en ONTAP System Manager. Utilice el asistente para configurar su sistema más rápidamente y asegurarse de que sus configuraciones se ajusten a las mejores prácticas de StorageGRID y FabricPool .

Suponiendo que tiene permiso de acceso de root, puede completar el asistente de configuración de FabricPool cuando comience a usar StorageGRID Grid Manager, o puede acceder y completar el asistente en cualquier momento posterior. Dependiendo de sus requisitos, también puede configurar algunos o todos los elementos necesarios manualmente y luego usar el asistente para reunir los valores que ONTAP necesita en un solo archivo.



Utilice el asistente de configuración de FabricPool a menos que sepa que tiene requisitos especiales o que su implementación requerirá una personalización significativa.

Antes de utilizar el asistente

Confirme que ha completado estos pasos previos.

Revisar las mejores prácticas

- Tienes una comprensión general de la ["Información necesaria para adjuntar StorageGRID como un nivel de nube"](#) .
- Ha revisado las mejores prácticas de FabricPool para:
 - ["Grupos de alta disponibilidad \(HA\)"](#)
 - ["Equilibrio de carga"](#)

- ["Normas y políticas de ILM"](#)

Obtener direcciones IP y configurar interfaces VLAN

Si configura un grupo de alta disponibilidad, sabrá a qué nodos se conectará ONTAP y qué red StorageGRID se utilizará. También sabe qué valores ingresar para el CIDR de subred, la dirección IP de puerta de enlace y las direcciones IP virtuales (VIP).

Si planea utilizar una LAN virtual para segregar el tráfico de FabricPool , ya ha configurado la interfaz VLAN. Ver ["Configurar interfaces VLAN"](#) .

Configurar la federación de identidades y el SSO

Si planea utilizar la federación de identidad o el inicio de sesión único (SSO) para su sistema StorageGRID , debe habilitar estas funciones. También sabe qué grupo federado debe tener acceso raíz para la cuenta de inquilino que utilizará ONTAP . Ver ["Utilizar la federación de identidades"](#) y ["Configurar el inicio de sesión único"](#) .

Obtener y configurar nombres de dominio

- Sabe qué nombre de dominio completo (FQDN) utilizar para StorageGRID. Las entradas del servidor de nombres de dominio (DNS) asignarán este FQDN a las direcciones IP virtuales (VIP) del grupo de alta disponibilidad que cree mediante el asistente. Ver ["Configurar el servidor DNS"](#) .
- Si planea utilizar solicitudes alojadas virtuales de estilo S3, debe ["nombres de dominio de punto final S3 configurados"](#) . ONTAP utiliza URL de estilo de ruta de manera predeterminada, pero se recomienda utilizar solicitudes de estilo alojado virtualmente.

Revisar los requisitos del balanceador de carga y del certificado de seguridad

Si planea utilizar el balanceador de carga StorageGRID , ha revisado las instrucciones generales ["Consideraciones para el equilibrio de carga"](#) . Tienes los certificados que cargarás o los valores que necesitas para generar un certificado.

Si planea utilizar un punto final de balanceador de carga externo (de terceros), debe tener el nombre de dominio completo (FQDN), el puerto y el certificado para ese balanceador de carga.

Confirmar la configuración del grupo de almacenamiento de ILM

Si instaló inicialmente StorageGRID 11.6 o una versión anterior, habrá configurado el grupo de almacenamiento que utilizará. En general, debe crear un grupo de almacenamiento para cada sitio StorageGRID que utilizará para almacenar datos de ONTAP .



Este requisito previo no se aplica si instaló inicialmente StorageGRID 11.7 o 11.8. Cuando instala inicialmente cualquiera de estas versiones, se crean automáticamente grupos de almacenamiento para cada sitio.

Relación entre ONTAP y el nivel de nube StorageGRID

El asistente de FabricPool lo guía a través del proceso de creación de un único nivel de nube StorageGRID que incluye un inquilino StorageGRID , un conjunto de claves de acceso y un depósito StorageGRID . Puede conectar este nivel de nube de StorageGRID a uno o más niveles locales de ONTAP .

La mejor práctica general es conectar un único nivel de nube a varios niveles locales en un clúster. Sin embargo, dependiendo de sus requisitos, es posible que desee utilizar más de un depósito o incluso más de

un inquilino de StorageGRID para los niveles locales en un solo clúster. El uso de diferentes depósitos e inquilinos le permite aislar los datos y el acceso a los datos entre los niveles locales de ONTAP , pero es un poco más complejo de configurar y administrar.

NetApp no recomienda adjuntar un solo nivel de nube a niveles locales en múltiples clústeres.



Para conocer las mejores prácticas para usar StorageGRID con NetApp MetroCluster™ y FabricPool Mirror, consulte ["TR-4598: Mejores prácticas de FabricPool en ONTAP"](#) .

Opcional: utilice un depósito diferente para cada nivel local

Para usar más de un bucket para los niveles locales en un clúster de ONTAP , agregue más de un nivel de nube StorageGRID en ONTAP. Cada nivel de nube comparte el mismo grupo de alta disponibilidad, punto final del equilibrador de carga, inquilino y claves de acceso, pero utiliza un contenedor diferente (depósito StorageGRID). Siga estos pasos generales:

1. Desde StorageGRID Grid Manager, complete el asistente de configuración de FabricPool para el primer nivel de nube.
2. Desde ONTAP System Manager, agregue un nivel de nube y use el archivo que descargó de StorageGRID para proporcionar los valores requeridos.
3. Desde StorageGRID Tenant Manager, inicie sesión en el inquilino creado por el asistente y cree un segundo depósito.
4. Complete nuevamente el asistente de FabricPool . Seleccione el grupo HA existente, el punto final del balanceador de carga y el inquilino. Luego, seleccione el nuevo depósito que creó manualmente. Cree una nueva regla ILM para el nuevo depósito y active una política ILM para incluir esa regla.
5. Desde ONTAP, agregue un segundo nivel de nube pero proporcione el nuevo nombre del depósito.

Opcional: utilice un inquilino y un depósito diferentes para cada nivel local

Para usar más de un inquilino y diferentes conjuntos de claves de acceso para los niveles locales en un clúster de ONTAP , agregue más de un nivel de nube StorageGRID en ONTAP. Cada nivel de nube comparte el mismo grupo de alta disponibilidad y punto final del equilibrador de carga, pero utiliza un inquilino, claves de acceso y contenedor diferentes (depósito StorageGRID). Siga estos pasos generales:

1. Desde StorageGRID Grid Manager, complete el asistente de configuración de FabricPool para el primer nivel de nube.
2. Desde ONTAP System Manager, agregue un nivel de nube y use el archivo que descargó de StorageGRID para proporcionar los valores requeridos.
3. Complete nuevamente el asistente de FabricPool . Seleccione el grupo HA existente y el punto final del balanceador de carga. Cree un nuevo inquilino y un depósito. Cree una nueva regla ILM para el nuevo depósito y active una política ILM para incluir esa regla.
4. Desde ONTAP, agregue un segundo nivel de nube, pero proporcione la nueva clave de acceso, la clave secreta y el nombre del depósito.

Acceda y complete el asistente de configuración de FabricPool

Puede utilizar el asistente de configuración de FabricPool para configurar StorageGRID como el sistema de almacenamiento de objetos para un nivel de nube de FabricPool .

Antes de empezar

- Usted ha revisado el ["Consideraciones y requisitos"](#) para utilizar el asistente de configuración de FabricPool .



Si desea configurar StorageGRID para su uso con cualquier otra aplicación cliente S3, vaya a ["Utilice el asistente de configuración de S3"](#) .

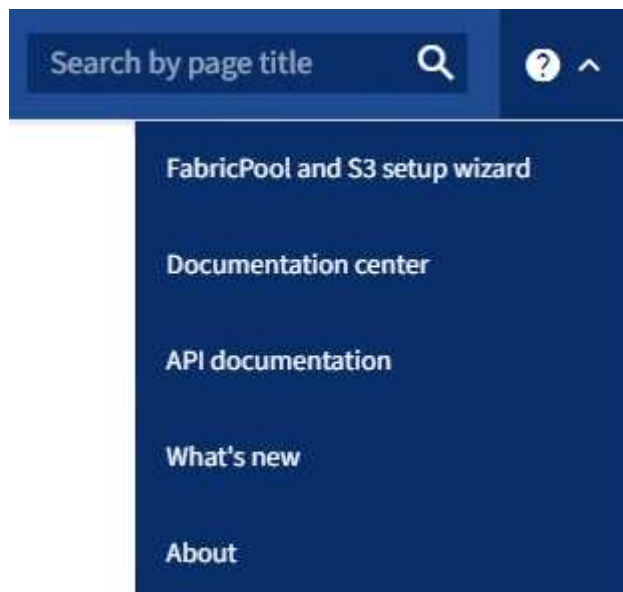
- Tú tienes el ["Permiso de acceso root"](#) .

Acceder al asistente

Puede completar el asistente de configuración de FabricPool cuando comience a utilizar StorageGRID Grid Manager, o puede acceder y completar el asistente en cualquier momento posterior.

Pasos

1. Sign in en Grid Manager usando un ["navegador web compatible"](#) .
2. Si aparece el banner **Asistente de configuración de FabricPool y S3** en el panel, seleccione el enlace en el banner. Si el banner ya no aparece, seleccione el ícono de ayuda en la barra de encabezado en el Administrador de cuadrícula y seleccione **Asistente de configuración de FabricPool y S3**.



3. En la sección FabricPool de la página del asistente de configuración de FabricPool y S3, seleccione **Configurar ahora**.

Aparece **Paso 1 de 9: Configurar el grupo HA**.

Paso 1 de 9: Configurar el grupo de alta disponibilidad

Un grupo de alta disponibilidad (HA) es una colección de nodos que contienen cada uno el servicio StorageGRID Load Balancer. Un grupo de alta disponibilidad puede contener nodos de puerta de enlace, nodos de administración o ambos.

Puede utilizar un grupo HA para ayudar a mantener disponibles las conexiones de datos de FabricPool . Un grupo de alta disponibilidad utiliza direcciones IP virtuales (VIP) para proporcionar acceso de alta disponibilidad al servicio Load Balancer. Si falla la interfaz activa en el grupo HA, una interfaz de respaldo puede administrar la carga de trabajo con poco impacto en las operaciones de FabricPool.

Para obtener más detalles sobre esta tarea, consulte ["Administrar grupos de alta disponibilidad"](#) y ["Mejores prácticas para grupos de alta disponibilidad"](#) .

Pasos

1. Si planea utilizar un balanceador de carga externo, no necesita crear un grupo de alta disponibilidad.
Seleccione **Omitir este paso** y vaya a [Paso 2 de 9: Configurar el punto final del balanceador de carga](#) .
2. Para utilizar el equilibrador de carga StorageGRID , cree un nuevo grupo de alta disponibilidad o utilice un grupo de alta disponibilidad existente.

Crear un grupo de alta disponibilidad

- Para crear un nuevo grupo de HA, seleccione **Crear grupo de HA**.
- Para el paso **Ingresar detalles**, complete los siguientes campos.

Campo	Descripción
Nombre del grupo HA	Un nombre para mostrar único para este grupo HA.
Descripción (opcional)	La descripción de este grupo HA.

- Para el paso **Agregar interfaces**, seleccione las interfaces de nodo que desea utilizar en este grupo de HA.

Utilice los encabezados de columna para ordenar las filas o ingrese un término de búsqueda para localizar interfaces más rápidamente.

Puede seleccionar uno o más nodos, pero solo puede seleccionar una interfaz para cada nodo.

- Para el paso **Priorizar interfaces**, determine la interfaz principal y cualquier interfaz de respaldo para este grupo de HA.

Arrastre filas para cambiar los valores en la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra una falla.

Si el grupo HA incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se mueven a la primera interfaz de respaldo en el orden de prioridad. Si esa interfaz falla, las direcciones VIP pasan a la siguiente interfaz de respaldo, y así sucesivamente. Cuando se resuelven las fallas, las direcciones VIP vuelven a la interfaz de mayor prioridad disponible.

- Para el paso **Ingresar direcciones IP**, complete los siguientes campos.

Campo	Descripción
CIDR de subred	La dirección de la subred VIP en notación CIDR: una dirección IPv4 seguida de una barra 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 .
Dirección IP de la puerta de enlace (opcional)	Opcional. Si las direcciones IP de ONTAP utilizadas para acceder a StorageGRID no están en la misma subred que las direcciones VIP de StorageGRID , ingrese la dirección IP de la puerta de enlace local VIP de StorageGRID . La dirección IP de la puerta de enlace local debe estar dentro de la subred VIP.

Campo	Descripción
Dirección IP virtual	Ingrese al menos una y no más de diez direcciones VIP para la interfaz activa en el grupo HA. Todas las direcciones VIP deben estar dentro de la subred VIP y todas estarán activas al mismo tiempo en la interfaz activa. Al menos una dirección debe ser IPv4. Opcionalmente, puede especificar direcciones IPv4 e IPv6 adicionales.

f. Seleccione **Crear grupo HA** y luego seleccione **Finalizar** para regresar al asistente de configuración de FabricPool .

g. Seleccione **Continuar** para ir al paso del balanceador de carga.

Utilizar el grupo HA existente

a. Para utilizar un grupo de HA existente, seleccione el nombre del grupo de HA en la lista desplegable **Seleccionar un grupo de HA**.

b. Seleccione **Continuar** para ir al paso del balanceador de carga.

Paso 2 de 9: Configurar el punto final del balanceador de carga

StorageGRID utiliza un equilibrador de carga para administrar la carga de trabajo de las aplicaciones cliente, como FabricPool. El equilibrio de carga maximiza la velocidad y la capacidad de conexión en múltiples nodos de almacenamiento.

Puede utilizar el servicio StorageGRID Load Balancer, que existe en todos los nodos de puerta de enlace y de administración, o puede conectarse a un balanceador de carga externo (de terceros). Se recomienda utilizar el balanceador de carga StorageGRID .

Para obtener más detalles sobre esta tarea, consulte la información general." [Consideraciones para el equilibrio de carga](#)" y el" [Mejores prácticas para el equilibrio de carga para FabricPool](#)" .

Pasos

1. Seleccione o cree un punto final de balanceador de carga StorageGRID o utilice un balanceador de carga externo.

Crear punto final

- Seleccione **Crear punto final**.
- Para el paso **Ingresar detalles del punto final**, complete los siguientes campos.

Campo	Descripción
Nombre	Un nombre descriptivo para el punto final.
Puerto	El puerto StorageGRID que desea utilizar para equilibrar la carga. Este campo tiene como valor predeterminado 10433 para el primer punto final que cree, pero puede ingresar cualquier puerto externo no utilizado. Si ingresa 80 o 443, el punto final se configura solo en los nodos de puerta de enlace, porque estos puertos están reservados en los nodos de administración. Nota: No se permiten los puertos utilizados por otros servicios de red. Ver el "Referencia del puerto de red".
Tipo de cliente	Debe ser S3 .
Protocolo de red	Seleccione HTTPS. Nota: Se admite la comunicación con StorageGRID sin cifrado TLS, pero no se recomienda.

- Para el paso **Seleccionar modo de enlace**, especifique el modo de enlace. El modo de enlace controla cómo se accede al punto final utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final utilizando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice la configuración Global (predeterminada) a menos que necesite restringir la accesibilidad de este punto final.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o FQDN correspondiente) de un grupo de HA para acceder a este punto final. Todos los puntos finales con este modo de enlace pueden usar el mismo número de puerto, siempre que los grupos de HA que seleccione para los puntos finales no se superpongan.
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.

Modo	Descripción
Tipo de nodo	Según el tipo de nodo que seleccione, los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este punto final.

d. Para el paso **Acceso de inquilino**, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (predeterminado)	Todas las cuentas de inquilinos pueden usar este punto final para acceder a sus depósitos. Permitir todos los inquilinos es casi siempre la opción adecuada para el punto final del balanceador de carga utilizado para FabricPool. Debe seleccionar esta opción si está utilizando el asistente de configuración de FabricPool para un nuevo sistema StorageGRID y aún no ha creado ninguna cuenta de inquilino.
Permitir inquilinos seleccionados	Solo las cuentas de inquilinos seleccionadas pueden usar este punto final para acceder a sus depósitos.
Bloquear inquilinos seleccionados	Las cuentas de inquilinos seleccionadas no pueden usar este punto final para acceder a sus depósitos. Todos los demás inquilinos pueden utilizar este punto final.

e. Para el paso **Adjuntar certificado**, seleccione una de las siguientes opciones:

Campo	Descripción
Subir certificado (recomendado)	Utilice esta opción para cargar un certificado de servidor firmado por una CA, una clave privada de certificado y un paquete de CA opcional.
Generar certificado	Utilice esta opción para generar un certificado autofirmado. Ver " Configurar los puntos finales del balanceador de carga " para obtener detalles de qué ingresar.
Utilice el certificado StorageGRID S3	Esta opción solo está disponible si ya ha cargado o generado una versión personalizada del certificado global de StorageGRID . Ver " Configurar certificados de API S3 " Para más detalles.

f. Seleccione **Finalizar** para regresar al asistente de configuración de FabricPool .

g. Seleccione **Continuar** para ir al paso de inquilino y depósito.



Los cambios en un certificado de punto final pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Utilice el punto final del balanceador de carga existente

- Seleccione el nombre de un punto final existente de la lista desplegable **Seleccionar un punto final del balanceador de carga**.
- Seleccione **Continuar** para ir al paso de inquilino y depósito.

Utilice un balanceador de carga externo

- Complete los siguientes campos para el balanceador de carga externo.

Campo	Descripción
Nombre de dominio completo (FQDN)	El nombre de dominio completo (FQDN) del balanceador de carga externo.
Puerto	El número de puerto que FabricPool utilizará para conectarse al balanceador de carga externo.
Certificado	Copie el certificado del servidor para el balanceador de carga externo y péguelo en este campo.

- Seleccione **Continuar** para ir al paso de inquilino y depósito.

Paso 3 de 9: Inquilino y cubo

Un inquilino es una entidad que puede utilizar aplicaciones S3 para almacenar y recuperar objetos en StorageGRID. Cada inquilino tiene sus propios usuarios, claves de acceso, depósitos, objetos y un conjunto específico de capacidades. Debe crear un inquilino de StorageGRID antes de poder crear el depósito que utilizará FabricPool .

Un bucket es un contenedor que se utiliza para almacenar objetos y metadatos de objetos de un inquilino. Aunque algunos inquilinos pueden tener muchos grupos, el asistente le permite crear o seleccionar solo un inquilino y un grupo a la vez. Más adelante podrá utilizar el Administrador de inquilinos para agregar cualquier grupo adicional que necesite.

Puede crear un nuevo inquilino y un depósito para uso de FabricPool , o puede seleccionar un inquilino y un depósito existentes. Si crea un nuevo inquilino, el sistema crea automáticamente el ID de clave de acceso y la clave de acceso secreta para el usuario raíz del inquilino.

Para obtener más detalles sobre esta tarea, consulte ["Crear una cuenta de inquilino para FabricPool"](#) y ["Cree un bucket S3 y obtenga una clave de acceso"](#) .

Pasos

Cree un nuevo inquilino y un depósito o seleccione un inquilino existente.

Nuevo inquilino y cubo

1. Para crear un nuevo inquilino y depósito, ingrese un **Nombre del inquilino**. Por ejemplo, `FabricPool tenant`.
2. Defina el acceso raíz para la cuenta de inquilino, en función de si su sistema StorageGRID utiliza ["federación de identidades"](#), ["inicio de sesión único \(SSO\)"](#), o ambos.

Opción	Haz esto
Si la federación de identidad no está habilitada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si la federación de identidad está habilitada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si tanto la federación de identidad como el inicio de sesión único (SSO) están habilitados	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

3. Para **Nombre del depósito**, ingrese el nombre del depósito que FabricPool utilizará para almacenar datos de ONTAP. Por ejemplo, `fabricpool-bucket`.



No puedes cambiar el nombre del depósito después de crearlo.

4. Seleccione la **Región** para este bucket.

Utilice la región predeterminada(`us-east-1`) a menos que espere utilizar ILM en el futuro para filtrar objetos según la región del depósito.

5. Seleccione **Crear y continuar** para crear el inquilino y el depósito y pasar al paso de descarga de datos.

Seleccionar inquilino y depósito

La cuenta de inquilino existente debe tener al menos un depósito que no tenga habilitada la función de control de versiones. No puede seleccionar una cuenta de inquilino existente si no existe ningún depósito para ese inquilino.

1. Seleccione el inquilino existente de la lista desplegable **Nombre del inquilino**.
2. Seleccione el depósito existente de la lista desplegable **Nombre del depósito**.

FabricPool no admite el control de versiones de objetos, por lo que los depósitos que tienen el control de versiones habilitado no se muestran.



No seleccione un depósito que tenga habilitado el bloqueo de objetos S3 para su uso con FabricPool.

3. Seleccione **Continuar** para ir al paso de descarga de datos.

Paso 4 de 9: Descargar la configuración de ONTAP

Durante este paso, descargará un archivo que puede usar para ingresar valores en ONTAP System Manager.

Pasos

1. Opcionalmente, seleccione el icono de copia () para copiar tanto el ID de la clave de acceso como la clave de acceso secreta al portapapeles.

Estos valores están incluidos en el archivo de descarga, pero es posible que desee guardarlos por separado.

2. Seleccione ***Descargar configuración de ONTAP *** para descargar un archivo de texto que contiene los valores que ha ingresado hasta ahora.

El `ONTAP_FabricPool_settings_bucketname.txt` El archivo incluye la información que necesita para configurar StorageGRID como el sistema de almacenamiento de objetos para un nivel de nube FabricPool, que incluye:

- Detalles de la conexión del balanceador de carga, incluido el nombre del servidor (FQDN), el puerto y el certificado
- Nombre del depósito
- ID de clave de acceso y clave de acceso secreta para el usuario raíz de la cuenta de inquilino

3. Guarde las claves copiadas y el archivo descargado en una ubicación segura.



No cierre esta página hasta que haya copiado ambas claves de acceso, descargado la configuración de ONTAP o ambas cosas. Las claves no estarán disponibles después de cerrar esta página. Asegúrese de guardar esta información en una ubicación segura porque puede usarse para obtener datos de su sistema StorageGRID.

4. Seleccione la casilla de verificación para confirmar que ha descargado o copiado el ID de la clave de acceso y la clave de acceso secreta.
5. Seleccione **Continuar** para ir al paso del grupo de almacenamiento ILM.

Paso 5 de 9: Seleccionar un grupo de almacenamiento

Un grupo de almacenamiento es un grupo de nodos de almacenamiento. Cuando selecciona un grupo de almacenamiento, determina qué nodos utilizará StorageGRID para almacenar los datos en niveles desde ONTAP.

Para obtener más detalles sobre este paso, consulte ["Crear un grupo de almacenamiento"](#).

Pasos

1. En la lista desplegable **Sitio**, seleccione el sitio StorageGRID que desea utilizar para los datos organizados en niveles desde ONTAP.
2. En la lista desplegable **Grupo de almacenamiento**, seleccione el grupo de almacenamiento para ese sitio.

El grupo de almacenamiento de un sitio incluye todos los nodos de almacenamiento de ese sitio.

3. Seleccione **Continuar** para ir al paso de la regla ILM.

Paso 6 de 9: Revisar la regla ILM para FabricPool

Las reglas de administración del ciclo de vida de la información (ILM) controlan la ubicación, la duración y el comportamiento de ingesta de todos los objetos en su sistema StorageGRID .

El asistente de configuración de FabricPool crea automáticamente la regla ILM recomendada para el uso de FabricPool . Esta regla se aplica únicamente al depósito que usted especificó. Utiliza codificación de borrado 2+1 en un solo sitio para almacenar los datos organizados en niveles desde ONTAP.

Para obtener más detalles sobre este paso, consulte ["Crear regla ILM"](#) y ["Mejores prácticas para usar ILM con datos de FabricPool"](#) .

Pasos

1. Revise los detalles de la regla.

Campo	Descripción
Nombre de la regla	Se genera automáticamente y no se puede cambiar.
Descripción	Se genera automáticamente y no se puede cambiar.
Filtrar	El nombre del cubo Esta regla solo se aplica a los objetos que se guardan en el depósito que usted especificó.
Tiempo de referencia	Tiempo de ingesta La instrucción de ubicación comienza cuando los objetos se guardan inicialmente en el depósito.
Instrucciones de colocación	Utilice la codificación de borrado 2+1

2. Ordene el diagrama de retención por **Período de tiempo** y **Grupo de almacenamiento** para confirmar la instrucción de ubicación.
 - El **Período de tiempo** de la regla es **Día 0 - para siempre**. **Día 0** significa que la regla se aplica cuando los datos se organizan en niveles desde ONTAP. **Para siempre** significa que StorageGRID ILM no eliminará datos que se hayan organizado en niveles desde ONTAP.
 - El **Grupo de almacenamiento** de la regla es el grupo de almacenamiento que usted seleccionó. **EC 2+1** significa que los datos se almacenarán utilizando codificación de borrado 2+1. Cada objeto se guardará como dos fragmentos de datos y un fragmento de paridad. Los tres fragmentos de cada objeto se guardarán en diferentes nodos de almacenamiento en un solo sitio.
3. Seleccione **Crear y continuar** para crear esta regla e ir al paso de política ILM.

Paso 7 de 9: Revisar y activar la política de ILM

Después de que el asistente de configuración de FabricPool crea la regla ILM para el uso de FabricPool , crea una política ILM. Debe simular y revisar cuidadosamente esta política antes de activarla.

Para obtener más detalles sobre este paso, consulte ["Crear una política ILM"](#) y ["Mejores prácticas para usar ILM con datos de FabricPool"](#).



Cuando activa una nueva política ILM, StorageGRID utiliza esa política para administrar la ubicación, la duración y la protección de datos de todos los objetos en la red, incluidos los objetos existentes y los objetos recientemente ingeridos. En algunos casos, la activación de una nueva política puede provocar que los objetos existentes se muevan a nuevas ubicaciones.



Para evitar la pérdida de datos, no utilice una regla ILM que caduque o elimine los datos del nivel de nube de FabricPool. Establezca el período de retención en **para siempre** para garantizar que StorageGRID ILM no elimine los objetos de FabricPool.

Pasos

1. Opcionalmente, actualice el **Nombre de la política** generado por el sistema. De forma predeterminada, el sistema agrega "+ FabricPool" al nombre de su política activa o inactiva, pero puede proporcionar su propio nombre.
2. Revise la lista de reglas en la política inactiva.
 - Si su cuadrícula no tiene una política ILM inactiva, el asistente crea una política inactiva clonando su política activa y agregando la nueva regla en la parte superior.
 - Si su red ya tiene una política ILM inactiva y esa política utiliza las mismas reglas y el mismo orden que la política ILM activa, el asistente agrega la nueva regla en la parte superior de la política inactiva.
 - Si su política inactiva contiene reglas diferentes o un orden diferente al de la política activa, el asistente crea una nueva política inactiva clonando su política activa y agregando la nueva regla en la parte superior.

3. Revise el orden de las reglas en la nueva política inactiva.

Debido a que la regla FabricPool es la primera regla, todos los objetos en el depósito FabricPool se colocan antes de que se evalúen las demás reglas de la política. Los objetos en cualquier otro grupo se colocan mediante reglas posteriores en la política.

4. Revise el diagrama de retención para aprender cómo se retendrán los diferentes objetos.
 - a. Seleccione **Expandir todo** para ver un diagrama de retención para cada regla en la política inactiva.
 - b. Seleccione **Período de tiempo y Grupo de almacenamiento** para revisar el diagrama de retención. Confirme que todas las reglas que se aplican al depósito o inquilino de FabricPool conservan los objetos **para siempre**.
5. Cuando haya revisado la política inactiva, seleccione **Activar y continuar** para activar la política y pasar al paso de clasificación de tráfico.



Los errores en una política ILM pueden provocar una pérdida de datos irreparable. Revise la política cuidadosamente antes de activar.

Paso 8 de 9: Crear una política de clasificación de tráfico

Como opción, el asistente de configuración de FabricPool puede crear una política de clasificación de tráfico que puede usar para monitorear la carga de trabajo de FabricPool. La política creada por el sistema utiliza una regla coincidente para identificar todo el tráfico de red relacionado con el depósito que usted creó. Esta política solo monitorea el tráfico; no limita el tráfico de FabricPool ni de ningún otro cliente.

Para obtener más detalles sobre este paso, consulte ["Crear una política de clasificación de tráfico para"](#)

Pasos

1. Revise la política.
2. Si desea crear esta política de clasificación de tráfico, seleccione **Crear y continuar**.

Tan pronto como FabricPool comience a organizar los datos en niveles en StorageGRID, podrá ir a la página Políticas de clasificación de tráfico para ver las métricas de tráfico de red para esta política. Más adelante, también puede agregar reglas para limitar otras cargas de trabajo y garantizar que la carga de trabajo de FabricPool tenga la mayor parte del ancho de banda.

3. De lo contrario, seleccione **Omitir este paso**.

Paso 9 de 9: Revisar el resumen

El resumen proporciona detalles sobre los elementos que configuró, incluido el nombre del balanceador de carga, el inquilino y el depósito, la política de clasificación de tráfico y la política ILM activa.

Pasos

1. Revise el resumen.
2. Seleccione **Finalizar**.

Próximos pasos

Después de completar el asistente de FabricPool , realice estos pasos adicionales.

Pasos

1. Ir a "[Configurar el Administrador del sistema ONTAP](#)" para ingresar los valores guardados y completar el lado ONTAP de la conexión. Debe agregar StorageGRID como un nivel de nube, adjuntar el nivel de nube a un nivel local para crear un FabricPool y establecer políticas de niveles de volumen.
2. Ir a "[Configurar el servidor DNS](#)" y asegúrese de que el DNS incluya un registro para asociar el nombre del servidor StorageGRID (nombre de dominio completo) a cada dirección IP de StorageGRID que utilizará.
3. Ir a "[Otras prácticas recomendadas para StorageGRID y FabricPool](#)" para conocer las mejores prácticas para los registros de auditoría de StorageGRID y otras opciones de configuración global.

Configurar StorageGRID manualmente

Cree un grupo de alta disponibilidad (HA) para FabricPool

Al configurar StorageGRID para su uso con FabricPool, puede crear opcionalmente uno o más grupos de alta disponibilidad (HA). Un grupo de alta disponibilidad es una colección de nodos que contienen cada uno el servicio StorageGRID Load Balancer. Un grupo de alta disponibilidad puede contener nodos de puerta de enlace, nodos de administración o ambos.

Puede utilizar un grupo HA para ayudar a mantener disponibles las conexiones de datos de FabricPool . Un grupo de alta disponibilidad utiliza direcciones IP virtuales (VIP) para proporcionar acceso de alta disponibilidad al servicio Load Balancer. Si la interfaz activa en el grupo HA falla, una interfaz de respaldo puede administrar la carga de trabajo con poco impacto en las operaciones de FabricPool .

Para obtener más detalles sobre esta tarea, consulte "[Administrar grupos de alta disponibilidad](#)" . Para utilizar

el asistente de configuración de FabricPool para completar esta tarea, vaya a ["Acceda y complete el asistente de configuración de FabricPool"](#) .

Antes de empezar

- Usted ha revisado el ["Mejores prácticas para grupos de alta disponibilidad"](#) .
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .
- Si planea utilizar una VLAN, habrá creado la interfaz VLAN. Ver ["Configurar interfaces VLAN"](#) .

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad**.
2. Seleccione **Crear**.
3. Para el paso **Ingresar detalles**, complete los siguientes campos.

Campo	Descripción
Nombre del grupo HA	Un nombre para mostrar único para este grupo HA.
Descripción (opcional)	La descripción de este grupo HA.

4. Para el paso **Agregar interfaces**, seleccione las interfaces de nodo que desea utilizar en este grupo de HA.

Utilice los encabezados de columna para ordenar las filas o ingrese un término de búsqueda para localizar interfaces más rápidamente.

Puede seleccionar uno o más nodos, pero solo puede seleccionar una interfaz para cada nodo.

5. Para el paso **Priorizar interfaces**, determine la interfaz principal y cualquier interfaz de respaldo para este grupo de HA.

Arrastre filas para cambiar los valores en la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra una falla.

Si el grupo HA incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se mueven a la primera interfaz de respaldo en el orden de prioridad. Si esa interfaz falla, las direcciones VIP pasan a la siguiente interfaz de respaldo, y así sucesivamente. Cuando se resuelven las fallas, las direcciones VIP vuelven a la interfaz de mayor prioridad disponible.

6. Para el paso **Ingresar direcciones IP**, complete los siguientes campos.

Campo	Descripción
CIDR de subred	La dirección de la subred VIP en notación CIDR: una dirección IPv4 seguida de una barra 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 .

Campo	Descripción
Dirección IP de la puerta de enlace (opcional)	Opcional. Si las direcciones IP de ONTAP utilizadas para acceder a StorageGRID no están en la misma subred que las direcciones VIP de StorageGRID, ingrese la dirección IP de la puerta de enlace local VIP de StorageGRID. La dirección IP de la puerta de enlace local debe estar dentro de la subred VIP.
Dirección IP virtual	Ingrese al menos una y no más de diez direcciones VIP para la interfaz activa en el grupo HA. Todas las direcciones VIP deben estar dentro de la subred VIP. Al menos una dirección debe ser IPv4. Opcionalmente, puede especificar direcciones IPv4 e IPv6 adicionales.

7. Seleccione **Crear grupo HA** y luego seleccione **Finalizar**.

Crear un punto final de balanceador de carga para FabricPool

StorageGRID utiliza un equilibrador de carga para administrar la carga de trabajo de las aplicaciones cliente, como FabricPool. El equilibrio de carga maximiza la velocidad y la capacidad de conexión en múltiples nodos de almacenamiento.

Al configurar StorageGRID para su uso con FabricPool, debe configurar un punto final del equilibrador de carga y cargar o generar un certificado de punto final del equilibrador de carga, que se utiliza para proteger la conexión entre ONTAP y StorageGRID.

Para utilizar el asistente de configuración de FabricPool para completar esta tarea, vaya a ["Acceda y complete el asistente de configuración de FabricPool"](#).

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).
- Has revisado la información general ["Consideraciones para el equilibrio de carga"](#) así como el ["Mejores prácticas para el equilibrio de carga para FabricPool"](#).

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Puntos finales del balanceador de carga**.
2. Seleccione **Crear**.
3. Para el paso **Ingresar detalles del punto final**, complete los siguientes campos.

Campo	Descripción
Nombre	Un nombre descriptivo para el punto final.

Campo	Descripción
Puerto	El puerto StorageGRID que desea utilizar para equilibrar la carga. Este campo tiene como valor predeterminado 10433 para el primer punto final que cree, pero puede ingresar cualquier puerto externo no utilizado. Si ingresa 80 o 443, el punto final se configura solo en los nodos de puerta de enlace. Estos puertos están reservados en los nodos de administración. Nota: No se permiten los puertos utilizados por otros servicios de red. Ver el "Referencia del puerto de red". Proporcionará este número a ONTAP cuando adjunte StorageGRID como un nivel de nube de FabricPool.
Tipo de cliente	Seleccione S3 .
Protocolo de red	Seleccione HTTPS. Nota: Se admite la comunicación con StorageGRID sin cifrado TLS, pero no se recomienda.

4. Para el paso **Seleccionar modo de enlace**, especifique el modo de enlace. El modo de enlace controla cómo se accede al punto final utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final utilizando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración, la dirección IP virtual (VIP) de cualquier grupo de alta disponibilidad en cualquier red o un FQDN correspondiente. Utilice la configuración Global (predeterminada) a menos que necesite restringir la accesibilidad de este punto final.
IP virtuales de grupos de alta disponibilidad	Los clientes deben usar una dirección IP virtual (o FQDN correspondiente) de un grupo de HA para acceder a este punto final. Todos los puntos finales con este modo de enlace pueden usar el mismo número de puerto, siempre que los grupos de HA que seleccione para los puntos finales no se superpongan.
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o FQDN correspondientes) de las interfaces de nodo seleccionadas para acceder a este punto final.
Tipo de nodo	Según el tipo de nodo que seleccione, los clientes deben usar la dirección IP (o FQDN correspondiente) de cualquier nodo de administración o la dirección IP (o FQDN correspondiente) de cualquier nodo de puerta de enlace para acceder a este punto final.

5. Para el paso **Acceso de inquilino**, seleccione una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (predeterminado)	Todas las cuentas de inquilinos pueden usar este punto final para acceder a sus depósitos. Permitir todos los inquilinos es casi siempre la opción adecuada para el punto final del balanceador de carga utilizado para FabricPool. Debe seleccionar esta opción si aún no ha creado ninguna cuenta de inquilino.
Permitir inquilinos seleccionados	Solo las cuentas de inquilinos seleccionadas pueden usar este punto final para acceder a sus depósitos.
Bloquear inquilinos seleccionados	Las cuentas de inquilinos seleccionadas no pueden usar este punto final para acceder a sus depósitos. Todos los demás inquilinos pueden utilizar este punto final.

6. Para el paso **Adjuntar certificado**, seleccione una de las siguientes opciones:

Campo	Descripción
Subir certificado (recomendado)	Utilice esta opción para cargar un certificado de servidor firmado por una CA, una clave privada de certificado y un paquete de CA opcional.
Generar certificado	Utilice esta opción para generar un certificado autofirmado. Ver" Configurar los puntos finales del balanceador de carga " para obtener detalles de qué ingresar.
Utilice el certificado StorageGRID S3	Esta opción solo está disponible si ya ha cargado o generado una versión personalizada del certificado global de StorageGRID . Ver" Configurar certificados de API S3 " Para más detalles.

7. Seleccione **Crear**.



Los cambios en un certificado de punto final pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Crear una cuenta de inquilino para FabricPool

Debe crear una cuenta de inquilino en Grid Manager para usar FabricPool .

Las cuentas de inquilino permiten que las aplicaciones cliente almacenen y recuperen objetos en StorageGRID. Cada cuenta de inquilino tiene su propio ID de cuenta, grupos y usuarios autorizados, depósitos y objetos.

Para obtener más detalles sobre esta tarea, consulte"[Crear una cuenta de inquilino](#)" . Para utilizar el asistente

de configuración de FabricPool para completar esta tarea, vaya a ["Acceda y complete el asistente de configuración de FabricPool"](#) .

Antes de empezar

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

Pasos

1. Seleccione **INQUILINOS**.
2. Seleccione **Crear**.
3. Para los pasos de Ingresar detalles, ingrese la siguiente información.

Campo	Descripción
Nombre	Un nombre para la cuenta del inquilino. Los nombres de los inquilinos no necesitan ser únicos. Cuando se crea la cuenta de inquilino, recibe un ID de cuenta numérico único.
Descripción (opcional)	Una descripción para ayudar a identificar al inquilino.
Tipo de cliente	Debe ser S3 para FabricPool.
Cuota de almacenamiento (opcional)	Deje este campo en blanco para FabricPool.

4. Para el paso Seleccionar permisos:

- a. No seleccione **Permitir servicios de plataforma**.

Los inquilinos de FabricPool normalmente no necesitan utilizar servicios de plataforma, como la replicación de CloudMirror.

- b. Opcionalmente, seleccione **Usar fuente de identidad propia**.

- c. No seleccione **Permitir selección S3**.

Los inquilinos de FabricPool normalmente no necesitan utilizar S3 Select.

- d. Opcionalmente, seleccione **Usar conexión de federación de red** para permitir que el inquilino utilice una ["conexión de federación de red"](#) para clonación de cuentas y replicación entre redes. Luego, seleccione la conexión de federación de red que desea utilizar.

5. Para el paso Definir acceso raíz, especifique qué usuario tendrá el permiso de acceso raíz inicial para la cuenta de inquilino, en función de si su sistema StorageGRID utiliza ["federación de identidades"](#) , ["inicio de sesión único \(SSO\)"](#) , o ambos.

Opción	Haz esto
Si la federación de identidad no está habilitada	Especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.

Opción	Haz esto
Si la federación de identidad está habilitada	a. Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. b. Opcionalmente, especifique la contraseña que se utilizará al iniciar sesión en el inquilino como usuario raíz local.
Si tanto la federación de identidad como el inicio de sesión único (SSO) están habilitados	Seleccione un grupo federado existente para tener permiso de acceso raíz para el inquilino. Ningún usuario local puede iniciar sesión.

6. Seleccione **Crear inquilino**.

Cree un depósito S3 y obtenga claves de acceso

Antes de usar StorageGRID con una carga de trabajo de FabricPool, debe crear un depósito S3 para sus datos de FabricPool. También debe obtener una clave de acceso y una clave de acceso secreta para la cuenta de inquilino que utilizará para FabricPool.

Para obtener más detalles sobre esta tarea, consulte ["Crear un depósito S3"](#) y ["Crea tus propias claves de acceso S3"](#). Para utilizar el asistente de configuración de FabricPool para completar esta tarea, vaya a ["Acceda y complete el asistente de configuración de FabricPool"](#).

Antes de empezar

- Ha creado una cuenta de inquilino para uso de FabricPool.
- Tiene acceso root a la cuenta del inquilino.

Pasos

1. Sign in en el Administrador de inquilinos.

Puede realizar cualquiera de las siguientes acciones:

- Desde la página Cuentas de inquilino en el Administrador de cuadrícula, seleccione el enlace * Sign in* para el inquilino e ingrese sus credenciales.
- Ingrese la URL de la cuenta de inquilino en un navegador web e ingrese sus credenciales.

2. Cree un depósito S3 para los datos de FabricPool.

Debe crear un depósito único para cada clúster de ONTAP que planea utilizar.

- Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.
- Seleccione **Crear depósito**.
- Ingrese el nombre del depósito StorageGRID que desea utilizar con FabricPool. Por ejemplo, `fabricpool-bucket`.



No puedes cambiar el nombre del depósito después de crearlo.

d. Seleccione la región para este bucket.

De forma predeterminada, todos los depósitos se crean en el `us-east-1` región.

- e. Seleccione **Continuar**.
- f. Seleccione **Crear depósito**.



No seleccione **Habilitar control de versiones de objetos** para el depósito FabricPool . De manera similar, no edite un bucket FabricPool para usar **Disponible** o una consistencia no predeterminada. La consistencia recomendada para los buckets de FabricPool es **Lectura después de una nueva escritura**, que es la consistencia predeterminada para un nuevo bucket.

3. Crea 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 la clave de acceso y la clave de acceso secreta.

Ingresa estos valores en ONTAP cuando configures StorageGRID como un nivel de nube de FabricPool .



Si genera una nueva clave de acceso y una clave de acceso secreta en StorageGRID en el futuro, ingrese las nuevas claves en ONTAP antes de eliminar los valores antiguos de StorageGRID. De lo contrario, ONTAP podría perder temporalmente su acceso a StorageGRID.

Configurar ILM para datos de FabricPool

Puede utilizar esta sencilla política de ejemplo como punto de partida para sus propias reglas y políticas de ILM.

Este ejemplo supone que está diseñando las reglas ILM y una política ILM para un sistema StorageGRID que tiene cuatro nodos de almacenamiento en un solo centro de datos en Denver, Colorado. Los datos de FabricPool en este ejemplo utilizan un depósito llamado `fabricpool-bucket` .



Las siguientes reglas y políticas de ILM son solo ejemplos. Hay muchas formas de configurar las reglas ILM. Antes de activar una nueva política, simúlrela para confirmar que funcionará como está previsto para proteger el contenido contra pérdidas. Para obtener más información, consulte ["Administrar objetos con ILM"](#) .



Para evitar la pérdida de datos, no utilice una regla ILM que caduque o elimine los datos del nivel de nube de FabricPool . Establezca el período de retención en **para siempre** para garantizar que StorageGRID ILM no elimine los objetos de FabricPool .

Antes de empezar

- Usted ha revisado el ["Mejores prácticas para usar ILM con datos de FabricPool"](#) .
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso ILM o root"](#) .

- Si actualizó a StorageGRID 11.9 desde una versión anterior de StorageGRID , habrá configurado el grupo de almacenamiento que utilizará. En general, debe crear un grupo de almacenamiento para cada sitio StorageGRID que utilizará para almacenar datos.



Este requisito previo no se aplica si instaló inicialmente StorageGRID 11.7 o 11.8. Cuando instala inicialmente cualquiera de estas versiones, se crean automáticamente grupos de almacenamiento para cada sitio.

Pasos

1. Cree una regla ILM que se aplique únicamente a los datos en `fabricpool-bucket`. Esta regla de ejemplo crea copias con código de borrado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Codificación de borrado 2 + 1 para datos de FabricPool
Nombre del depósito	<code>fabricpool-bucket</code> También puede filtrar por cuenta de inquilino de FabricPool .
Filtros avanzados	Tamaño del objeto mayor a 0,2 MB. Nota: FabricPool solo escribe objetos de 4 MB, pero debe agregar un filtro de tamaño de objeto porque esta regla usa codificación de borrado.
Tiempo de referencia	Tiempo de ingesta
Periodo de tiempo y ubicaciones	Desde el día 0 tienda para siempre Almacene objetos mediante codificación de borrado utilizando el esquema EC 2+1 en Denver y conserve esos objetos en StorageGRID para siempre. Para evitar la pérdida de datos, no utilice una regla ILM que caduque o elimine los datos del nivel de nube de FabricPool .
Comportamiento de ingesta	Equilibrado

2. Cree una regla ILM predeterminada que creará dos copias replicadas de cualquier objeto que no coincida con la primera regla. No seleccione un filtro básico (cuenta de inquilino o nombre de depósito) ni ningún filtro avanzado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Dos copias replicadas

Definición de regla	Valor de ejemplo
Nombre del depósito	<i>ninguno</i>
Filtros avanzados	<i>ninguno</i>
Tiempo de referencia	Tiempo de ingesta
Periodo de tiempo y ubicaciones	Desde el día 0 tienda para siempre Almacene objetos replicando 2 copias en Denver.
Comportamiento de ingesta	Equilibrado

3. Cree una política ILM y seleccione las dos reglas. Debido a que la regla de replicación no utiliza ningún filtro, puede ser la regla predeterminada (última) para la política.
4. Ingerir objetos de prueba en la red.
5. Simular la política con los objetos de prueba para verificar el comportamiento.
6. Activar la política.

Cuando se activa esta política, StorageGRID coloca los datos de los objetos de la siguiente manera:

- Los datos organizados en niveles desde FabricPool en `fabricpool-bucket` se codificarán mediante borrado utilizando 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 depósitos. Se crearán dos copias y se colocarán en dos nodos de almacenamiento diferentes.
- Las copias se mantendrán en StorageGRID para siempre. StorageGRID ILM no eliminará estos objetos.

Crear una política de clasificación de tráfico para FabricPool

Opcionalmente, puede diseñar una política de clasificación de tráfico de StorageGRID para optimizar la calidad del servicio para la carga de trabajo de FabricPool .

Para obtener más detalles sobre esta tarea, consulte ["Administrar políticas de clasificación de tráfico"](#) . Para utilizar el asistente de configuración de FabricPool para completar esta tarea, vaya a ["Acceda y complete el asistente de configuración de FabricPool"](#) .

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .

Acerca de esta tarea

Las mejores prácticas para crear una política de clasificación de tráfico para FabricPool dependen de la carga de trabajo, de la siguiente manera:

- Si planea agrupar los datos de la carga de trabajo principal de FabricPool en StorageGRID, debe asegurarse de que la carga de trabajo de FabricPool tenga la mayor parte del ancho de banda. Puede

crear una política de clasificación de tráfico para limitar todas las demás 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 , debe crear una política de clasificación de tráfico. Puede limitar el tráfico de red para los demás depósitos, inquilinos, subredes IP o puntos finales del balanceador de carga.

- Por lo general, no debe imponer límites de calidad de servicio en ninguna carga de trabajo de FabricPool ; solo debe limitar las demás cargas de trabajo.
- Los límites impuestos a otras cargas de trabajo deben tener en cuenta el comportamiento de esas cargas de trabajo. Los límites impuestos también variarán en función del tamaño y las capacidades de su red y de la cantidad de utilización esperada.

Pasos

1. Seleccione **CONFIGURACIÓN > Red > Clasificación de tráfico**.
2. Seleccione **Crear**.
3. Ingrese un nombre y una descripción (opcional) para la política y seleccione **Continuar**.
4. Para el paso Agregar reglas coincidentes, agregue al menos una regla.
 - a. Seleccione **Agregar regla**
 - b. Para Tipo, seleccione **Punto final del balanceador de carga** y seleccione el punto final del balanceador de carga que creó para FabricPool.

También puede seleccionar la cuenta de inquilino o el depósito de FabricPool .
 - c. Si desea que esta política de tráfico limite el tráfico hacia los demás puntos finales, seleccione **Coincidencia inversa**.
5. Opcionalmente, agregue uno o más límites para controlar el tráfico de red que coincide con la regla.



StorageGRID recopila métricas incluso si no agrega ningún límite, para que pueda comprender las tendencias de tráfico.

- a. Seleccione **Agregar un límite**.
 - b. Seleccione el tipo de tráfico que desea limitar y el límite a aplicar.
6. Seleccione **Continuar**.
 7. Lea y revise la política de clasificación de tráfico. Utilice el botón **Anterior** para volver atrás y realizar los cambios necesarios. Cuando esté satisfecho con la política, seleccione **Guardar y continuar**.

Después de terminar

["Ver métricas de tráfico de red"](#) para verificar que las políticas estén haciendo cumplir los límites de tráfico esperados.

Configurar el Administrador del sistema ONTAP

Una vez que haya obtenido la información de StorageGRID requerida, puede ir a ONTAP para agregar StorageGRID como un nivel de nube.

Antes de empezar

- Si completó el asistente de configuración de FabricPool , tendrá la `ONTAP_FabricPool_settings_bucketname.txt` archivo que descargaste.
- Si configuró StorageGRID manualmente, tiene el nombre de dominio completo (FQDN) que está usando para StorageGRID o la dirección IP virtual (VIP) para el grupo HA de StorageGRID , el número de puerto para el punto final del balanceador de carga, el certificado del balanceador de carga, la ID de clave de acceso y la clave secreta para el usuario raíz de la cuenta del inquilino y el nombre del depósito que ONTAP usará en ese inquilino.

Administrador del sistema Access ONTAP

Estas instrucciones describen cómo utilizar ONTAP System Manager para agregar StorageGRID como un nivel de nube. Puede completar la misma configuración utilizando la CLI de ONTAP . Para obtener instrucciones, vaya a ["Documentación de ONTAP para FabricPool"](#) .

Pasos

1. Acceda al Administrador del sistema para el clúster ONTAP que desea conectar a StorageGRID.
2. Sign in como administrador del clúster.
3. Vaya a **ALMACENAMIENTO > Niveles > Agregar nivel de nube**.
4. Seleccione * StorageGRID* de la lista de proveedores de almacenamiento de objetos.

Introduzca los valores de StorageGRID

Ver ["Documentación de ONTAP para FabricPool"](#) Para más información.

Pasos

1. Complete el formulario Agregar nivel de nube, utilizando el `ONTAP_FabricPool_settings_bucketname.txt` archivo o los valores obtenidos manualmente.

Campo	Descripción
Nombre	Ingrese un nombre único para este nivel de nube. Puede aceptar el valor predeterminado.
Estilo de URL	Si usted "nombres de dominio de punto final S3 configurados" , seleccione URL de estilo alojado virtual. Path-Style URL es el valor predeterminado para ONTAP, pero se recomienda usar solicitudes de estilo alojado virtual para StorageGRID. Debe utilizar URL de estilo de ruta si proporciona una dirección IP en lugar de un nombre de dominio para el campo Nombre del servidor (FQDN).

Campo	Descripción
Nombre del servidor (FQDN)	Ingrese el nombre de dominio completo (FQDN) que está utilizando para StorageGRID o la dirección IP virtual (VIP) para el grupo HA de StorageGRID . Por ejemplo, <code>s3.storagegrid.company.com</code> . Tenga en cuenta lo siguiente: • La dirección IP o el nombre de dominio que especifique aquí debe coincidir con el certificado que cargó o generó para el punto final del balanceador de carga de StorageGRID . • Si proporciona un nombre de dominio, el registro DNS debe asignarse a cada dirección IP que utilizará para conectarse a StorageGRID. Ver "Configurar el servidor DNS" .
SSL	Habilitado (predeterminado).
Certificado de almacén de objetos	Pegue el certificado PEM que está utilizando para el punto final del balanceador de carga StorageGRID , incluido: <pre>-----BEGIN CERTIFICATE----- y -----END CERTIFICATE----- .</pre> Nota: Si una CA intermedia emitió el certificado StorageGRID , debe proporcionar el certificado de CA intermedia. Si el certificado StorageGRID fue emitido directamente por la CA raíz, debe proporcionar el certificado de la CA raíz.
Puerto	Ingrese el puerto utilizado por el punto final del balanceador de carga de StorageGRID . ONTAP utilizará este puerto cuando se conecte a StorageGRID. Por ejemplo, 10433.
Clave de acceso y clave secreta	Ingrese el ID de la clave de acceso y la clave de acceso secreta para el usuario raíz de la cuenta de inquilino de StorageGRID . Sugerencia: Si genera una nueva clave de acceso y una clave de acceso secreta en StorageGRID en el futuro, ingrese las nuevas claves en ONTAP antes de eliminar los valores antiguos de StorageGRID. De lo contrario, ONTAP podría perder temporalmente su acceso a StorageGRID.
Nombre del contenedor	Ingrese el nombre del depósito StorageGRID que creó para usar con este nivel de ONTAP .

2. Complete la configuración final de FabricPool en ONTAP.
 - a. Adjunte uno o más agregados al nivel de nube.
 - b. Opcionalmente, cree una política de niveles de volumen.

Configurar el servidor DNS

Después de configurar grupos de alta disponibilidad, puntos finales del equilibrador de carga y nombres de dominio de puntos finales S3, debe asegurarse de que el DNS

incluya las entradas necesarias para StorageGRID. Debe incluir una entrada DNS para cada nombre en el certificado de seguridad y para cada dirección IP que pueda utilizar.

Ver ["Consideraciones para el equilibrio de carga"](#) .

Entradas DNS para el nombre del servidor StorageGRID

Agregue entradas DNS para asociar el nombre del servidor StorageGRID (nombre de dominio completo) a cada dirección IP de StorageGRID que utilizará. Las direcciones IP que ingrese en el DNS dependen de si está utilizando un grupo HA de nodos de equilibrio de carga:

- Si ha configurado un grupo de HA, ONTAP se conectará a las direcciones IP virtuales de ese grupo de HA.
- Si no está utilizando un grupo HA, ONTAP puede conectarse al servicio StorageGRID Load Balancer usando la dirección IP de cualquier nodo de puerta de enlace o nodo de administración.
- Si el nombre del servidor se resuelve en más de una dirección IP, ONTAP establece conexiones de cliente con todas las direcciones IP (hasta un máximo de 16 direcciones IP). Las direcciones IP se seleccionan mediante un método rotatorio cuando se establecen conexiones.

Entradas DNS para solicitudes de estilo alojado virtual

Si has definido ["Nombres de dominio de punto final S3"](#) y utilizará solicitudes de estilo alojado virtual, agregará entradas DNS para todos los nombres de dominio de punto final S3 requeridos, incluidos los nombres comodín.

Prácticas recomendadas de StorageGRID para FabricPool

Mejores prácticas para grupos de alta disponibilidad (HA)

Antes de adjuntar StorageGRID como un nivel de nube de FabricPool , obtenga información sobre los grupos de alta disponibilidad (HA) de StorageGRID y revise las mejores prácticas para usar grupos de HA con FabricPool.

¿Qué es un grupo HA?

Un grupo de alta disponibilidad (HA) es una colección de interfaces de varios nodos de puerta de enlace de StorageGRID , nodos de administración o ambos. Un grupo HA ayuda a mantener disponibles las conexiones de datos del cliente. Si la interfaz activa en el grupo HA falla, una interfaz de respaldo puede administrar la carga de trabajo con poco impacto en las operaciones de FabricPool .

Cada grupo HA 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 nodos de puerta de enlace o en nodos de administración y nodos de puerta de enlace proporciona acceso de alta disponibilidad al servicio de balanceador de carga compartido.

Para obtener más información sobre los grupos de alta disponibilidad, consulte ["Administrar grupos de alta disponibilidad \(HA\)"](#) .

Uso de grupos de HA

Las mejores prácticas para crear un grupo StorageGRID HA para FabricPool dependen de la carga de trabajo.

- Si planea utilizar FabricPool con datos de carga de trabajo principales, debe crear un grupo de alta disponibilidad que incluya al menos dos nodos de equilibrio de carga para evitar interrupciones en la

recuperación de datos.

- Si planea utilizar la política de niveles de volumen de solo instantáneas de FabricPool o niveles de rendimiento local no primarios (por ejemplo, ubicaciones de recuperación ante desastres o destinos de NetApp SnapMirror), puede configurar un grupo de alta disponibilidad con solo un nodo.

Estas instrucciones describen cómo configurar un grupo HA para HA de respaldo activo (un nodo es activo y el otro es de respaldo). Sin embargo, es posible que prefieras utilizar DNS Round Robin o Active-Active HA. Para conocer los beneficios de estas otras configuraciones de HA, consulte ["Opciones de configuración para grupos de alta disponibilidad"](#).

Mejores prácticas para el equilibrio de carga para FabricPool

Antes de adjuntar StorageGRID como un nivel de nube de FabricPool, revise las mejores prácticas para usar balanceadores de carga con FabricPool.

Para obtener información general sobre el balanceador de carga StorageGRID y el certificado del balanceador de carga, consulte ["Consideraciones para el equilibrio de carga"](#).

Prácticas recomendadas para el acceso de los inquilinos al punto final del balanceador de carga utilizado para FabricPool

Puede controlar qué inquilinos pueden usar un punto final de balanceador de carga específico para acceder a sus depósitos. Puede permitir a todos los inquilinos, permitir a algunos inquilinos o bloquear a algunos inquilinos. Al crear un punto final de equilibrio de carga para el uso de FabricPool, seleccione **Permitir todos los inquilinos**. ONTAP cifra los datos que se colocan en los depósitos StorageGRID, por lo que esta capa de seguridad adicional proporcionaría poca seguridad adicional.

Mejores prácticas para el certificado de seguridad

Cuando crea un punto final de balanceador de carga StorageGRID para uso de FabricPool, proporciona el certificado de seguridad que permitirá que ONTAP se autentique con StorageGRID.

En la mayoría de los casos, la conexión entre ONTAP y StorageGRID debe utilizar el cifrado de seguridad de la capa de transporte (TLS). Se admite el uso de FabricPool sin cifrado TLS, pero no se recomienda. Cuando seleccione el protocolo de red para el punto final del balanceador de carga StorageGRID, seleccione **HTTPS**. Luego proporcione el certificado de seguridad que permitirá que ONTAP se autentique con StorageGRID.

Para obtener más información sobre el certificado de servidor para un punto final de equilibrio de carga:

- ["Administrar certificados de seguridad"](#)
- ["Consideraciones para el equilibrio de carga"](#)
- ["Pautas de refuerzo para certificados de servidor"](#)

Agregar certificado a ONTAP

Cuando agrega StorageGRID como un nivel de nube de FabricPool, debe instalar el mismo certificado en el clúster de ONTAP, incluidos los certificados raíz y cualquier certificado de autoridad de certificación (CA) subordinada.

Administrar la expiración del certificado



Si el certificado utilizado para proteger la conexión entre ONTAP y StorageGRID caduca, FabricPool dejará de funcionar temporalmente y ONTAP perderá temporalmente el acceso a los datos almacenados en StorageGRID.

Para evitar problemas de vencimiento de certificados, siga estas prácticas recomendadas:

- Supervise atentamente cualquier alerta que advierta sobre fechas de vencimiento de certificados próximas, como las alertas **Vencimiento del certificado del punto final del equilibrador de carga** y **Vencimiento del certificado del servidor global para la API de S3**.
- Mantenga siempre sincronizadas las versiones StorageGRID y ONTAP del certificado. Si reemplaza o renueva el certificado utilizado para un punto final del balanceador de carga, debe reemplazar o renovar el certificado equivalente utilizado por ONTAP para el nivel de nube.
- Utilice un certificado CA firmado públicamente. Si utiliza un certificado firmado por una CA, puede utilizar la API de administración de Grid para automatizar la rotación de certificados. Esto le permite reemplazar certificados que están a punto de vencer sin interrupciones.
- Si ha generado un certificado StorageGRID autofirmado y ese certificado está a punto de caducar, debe reemplazarlo manualmente tanto en StorageGRID como en ONTAP antes de que caduque el certificado existente. Si un certificado autofirmado ya ha expirado, desactive la validación del certificado en ONTAP para evitar la pérdida de acceso.

Ver ["Base de conocimientos de NetApp : Cómo configurar un nuevo certificado de servidor autofirmado de StorageGRID en una implementación existente de ONTAP FabricPool"](#) para obtener instrucciones.

Mejores prácticas para usar ILM con datos de FabricPool

Si está utilizando FabricPool para organizar datos en niveles en StorageGRID, debe comprender los requisitos para usar la gestión del ciclo de vida de la información (ILM) de StorageGRID con datos de FabricPool .



FabricPool no tiene conocimiento de las reglas o políticas de StorageGRID ILM. Puede ocurrir pérdida de datos si la política ILM de StorageGRID está mal configurada. Para obtener información detallada, consulte ["Utilice reglas ILM para administrar objetos"](#) y ["Crear políticas ILM"](#) .

Pautas para usar ILM con FabricPool

Cuando utiliza el asistente de configuración de FabricPool , este crea automáticamente una nueva regla ILM para cada bucket S3 que cree y agrega esa regla a una política inactiva. Se le solicitará que active la política. La regla creada automáticamente sigue las mejores prácticas recomendadas: utiliza codificación de borrado 2+1 en un solo sitio.

Si está configurando StorageGRID manualmente en lugar de utilizar el asistente de configuración de FabricPool , revise estas pautas para asegurarse de que sus reglas y políticas de ILM sean adecuadas para los datos de FabricPool y los requisitos de su negocio. Es posible que necesite crear nuevas reglas y actualizar sus políticas ILM activas para cumplir con estas pautas.

- Puede utilizar cualquier combinación de reglas de replicación y codificación de borrado para proteger los datos de nivel de nube.

La mejor práctica recomendada es utilizar codificación de borrado 2+1 dentro de un sitio para lograr una protección de datos rentable. La codificación de borrado utiliza más CPU, pero ofrece significativamente

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 red. Para obtener más información, consulte ["Añadir capacidad de almacenamiento para objetos con código de borrado"](#) .

- Cada regla aplicada a los datos de FabricPool debe utilizar codificación de borrado o debe crear al menos dos copias replicadas.



Una regla ILM que crea solo una copia replicada por cada período de tiempo pone los datos en riesgo de pérdida permanente. Si solo existe una copia replicada de un objeto, ese objeto se pierde si un nodo de almacenamiento falla o tiene un error significativo. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como actualizaciones.

- Si es necesario ["eliminar datos de FabricPool de StorageGRID"](#) , use ONTAP para recuperar todos los datos del volumen FabricPool y promoverlo al nivel de rendimiento.



Para evitar la pérdida de datos, no utilice una regla ILM que caduque o elimine los datos del nivel de nube de FabricPool . Establezca el período de retención en cada regla ILM en **para siempre** para garantizar que StorageGRID ILM no elimine los objetos de FabricPool .

- No cree reglas que muevan los datos del nivel de nube de FabricPool fuera del depósito a otra ubicación. No se puede utilizar un grupo de almacenamiento en la nube para mover datos de FabricPool a otro almacén de objetos.



No se admite el uso de grupos de almacenamiento en la nube con FabricPool debido a la latencia adicional para recuperar un objeto del destino del grupo de almacenamiento en la nube.

- A partir de ONTAP 9.8, puede crear opcionalmente etiquetas de objetos para ayudar a clasificar y ordenar datos escalonados para una gestión más sencilla. Por ejemplo, puede establecer etiquetas solo en los volúmenes de FabricPool adjuntos a StorageGRID. Luego, cuando crea reglas ILM en StorageGRID, puede usar el filtro avanzado Etiqueta de objeto para seleccionar y colocar estos datos.

Otras prácticas recomendadas para StorageGRID y FabricPool

Al configurar un sistema StorageGRID para su uso con FabricPool, es posible que deba cambiar otras opciones de StorageGRID . Antes de cambiar una configuración global, considere cómo afectará el cambio a otras aplicaciones S3.

Destinos de mensajes y registros de auditoría

Las cargas de trabajo de FabricPool a menudo tienen una alta tasa de operaciones de lectura, lo que puede generar un gran volumen de mensajes de auditoría.

- Si no necesita un registro de las operaciones de lectura del cliente para FabricPool o cualquier otra aplicación S3, vaya opcionalmente a **CONFIGURACIÓN > Monitoreo > Servidor de auditoría y syslog**. Cambie la configuración **Lecturas de cliente a Error** para disminuir la cantidad de mensajes de auditoría registrados en el registro de auditoría. Ver ["Configurar mensajes de auditoría y destinos de registro"](#) Para más detalles.
- Si tiene una red grande, utiliza varios tipos de aplicaciones S3 o desea conservar todos los datos de auditoría, configure un servidor syslog externo y guarde la información de auditoría de forma remota. El

uso de un servidor externo minimiza el impacto en el rendimiento del registro de mensajes de auditoría sin reducir la integridad de los datos de auditoría. Ver "[Consideraciones para el servidor syslog externo](#)" Para más detalles.

Cifrado de objetos

Al configurar StorageGRID, puede habilitar opcionalmente la "[Opción global para el cifrado de objetos almacenados](#)". Si se requiere cifrado de datos para otros clientes de StorageGRID. Los datos que se almacenan en niveles desde FabricPool a StorageGRID ya están cifrados, por lo que no es necesario habilitar la configuración de StorageGRID. Las claves de cifrado del lado del cliente son propiedad de ONTAP.

Compresión de objetos

Al configurar StorageGRID, no habilite la "[Opción global para comprimir objetos almacenados](#)". Los datos almacenados en niveles desde FabricPool a StorageGRID ya están comprimidos. El uso de la opción StorageGRID no reducirá aún más el tamaño de un objeto.

Consistencia del cubo

Para los buckets de FabricPool, la consistencia recomendada es **Lectura después de una nueva escritura**, que es la consistencia predeterminada para un bucket nuevo. No edite los depósitos de FabricPool para usar **Disponible** o **Sitio fuerte**.

Nivelación de FabricPool

Si un nodo StorageGRID usa almacenamiento asignado desde un sistema NetApp ONTAP, confirme que el volumen no tenga habilitada una política de niveles de FabricPool. Por ejemplo, si un nodo StorageGRID se ejecuta en un host VMware, asegúrese de que el volumen que respalda el almacén de datos para el nodo StorageGRID no tenga una política de niveles de FabricPool habilitada. Deshabilitar la organización en niveles de FabricPool para los volúmenes utilizados con nodos StorageGRID simplifica la resolución de problemas y las operaciones de almacenamiento.



Nunca use FabricPool para agrupar datos relacionados con StorageGRID en StorageGRID mismo. La organización de los datos de StorageGRID en niveles en StorageGRID aumenta la resolución de problemas y la complejidad operativa.

Eliminar datos de FabricPool de StorageGRID

Si necesita eliminar los datos de FabricPool que actualmente están almacenados en StorageGRID, debe usar ONTAP para recuperar todos los datos del volumen de FabricPool y promoverlo al nivel de rendimiento.

Antes de empezar

- Has revisado las instrucciones y consideraciones en "[Promocionar datos al nivel de rendimiento](#)".
- Está utilizando ONTAP 9.8 o posterior.
- Estás usando un "[navegador web compatible](#)".
- Pertenece a un grupo de usuarios de StorageGRID para la cuenta de inquilino de FabricPool que tiene la "[Administrar todos los depósitos o permisos de acceso raíz](#)".

Acerca de esta tarea

Estas instrucciones explican cómo mover datos desde StorageGRID a FabricPool. Realice este procedimiento utilizando ONTAP y StorageGRID Tenant Manager.

Pasos

1. Desde ONTAP, emita el `volume modify` dominio.

Colocar `tiering-policy` a `none` Para detener la nueva clasificación y establecer `cloud-retrieval-policy` a `promote` para devolver todos los datos que anteriormente estaban almacenados en StorageGRID.

Ver ["Promocionar todos los datos de un volumen FabricPool al nivel de rendimiento"](#) .

2. Espere a que se complete la operación.

Puedes utilizar el `volume object-store` comando con el `tiering` opción a ["comprobar el estado de la promoción del nivel de rendimiento"](#) .

3. Una vez completada la operación de promoción, inicie sesión en StorageGRID Tenant Manager para la cuenta de inquilino de FabricPool .
4. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.
5. Confirme que el depósito FabricPool ahora esté vacío.
6. Si el cubo está vacío, ["eliminar el depósito"](#) .

Después de terminar

Cuando se elimina el bucket, la organización en niveles de FabricPool a StorageGRID ya no puede continuar. Sin embargo, debido a que el nivel local aún está conectado al nivel de nube StorageGRID , ONTAP System Manager devolverá mensajes de error que indican que el depósito es inaccesible.

Para evitar estos mensajes de error, realice una de las siguientes acciones:

- Utilice FabricPool Mirror para adjuntar un nivel de nube diferente al agregado.
- Mueva los datos del agregado FabricPool a un agregado que no sea FabricPool y luego elimine el agregado no utilizado.

Ver el ["Documentación de ONTAP para FabricPool"](#) para obtener instrucciones.

Utilice inquilinos y clientes de StorageGRID

Utilice una cuenta de inquilino

Utilice una cuenta de inquilino

Una cuenta de inquilino le permite utilizar la API REST de Simple Storage Service (S3) o la API 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 federados o locales, usuarios, depósitos S3 o contenedores Swift y objetos.

Las cuentas de inquilino se pueden utilizar para segregar objetos almacenados por diferentes entidades. Por ejemplo, se pueden utilizar varias cuentas de inquilino para cualquiera de estos casos de uso:

- **Caso de uso empresarial:** si el sistema StorageGRID se utiliza dentro de una empresa, el almacenamiento de objetos de la red podría estar segregado por los diferentes departamentos de la organización. Por ejemplo, podría haber cuentas de inquilinos para el departamento de Marketing, el departamento de Atención al Cliente, el departamento de Recursos Humanos, etc.



Si utiliza el protocolo de cliente S3, también puede usar depósitos S3 y políticas de depósitos para segregar objetos entre los departamentos de una empresa. No es necesario crear cuentas de inquilino separadas. Consulte las instrucciones para la implementación "[Cubos S3 y políticas de cubos](#)" Para más información.

- **Caso de uso de proveedor de servicios:** si un proveedor de servicios utiliza el sistema StorageGRID , el almacenamiento de objetos de la red puede estar segregado por las diferentes entidades que alquilan el almacenamiento. Por ejemplo, podría haber cuentas de inquilinos para la Empresa A, la Empresa B, la Empresa C, etc.

Cómo crear una cuenta de inquilino

Las cuentas de inquilinos son creadas por un "[Administrador de red StorageGRID que utiliza el Administrador de red](#)". Al crear una cuenta de inquilino, el administrador de la red especifica lo siguiente:

- Información básica que incluye el nombre del inquilino, el tipo de cliente (S3) y la cuota de almacenamiento opcional.
- Permisos para la cuenta de inquilino, como si la cuenta de inquilino puede usar servicios de la plataforma S3, configurar su propia fuente de identidad, usar S3 Select o usar una conexión de federación de red.
- El acceso raíz inicial para el inquilino, en función de si el sistema StorageGRID utiliza grupos y usuarios locales, federación de identidad o inicio de sesión único (SSO).

Además, los administradores de la red pueden habilitar la configuración de Bloqueo de objetos S3 para el sistema StorageGRID si las cuentas de inquilinos S3 necesitan cumplir con los requisitos reglamentarios. Cuando el bloqueo de objetos S3 está habilitado, todas las cuentas de inquilinos de S3 pueden crear y administrar depósitos compatibles.

Configurar inquilinos de S3

Después de un ["Se crea una cuenta de inquilino S3"](#) , puede acceder al Administrador de inquilinos para realizar tareas como las siguientes:

- Configurar la federación de identidad (a menos que la fuente de identidad se comparta con la red)
- Administrar grupos y usuarios
- Utilice la federación de red para la clonación de cuentas y la replicación entre redes
- Administrar claves de acceso S3
- Crear y administrar depósitos S3
- Utilice los servicios de la plataforma S3
- Utilice S3 Select
- Monitorear el uso del almacenamiento



Si bien puede crear y administrar depósitos S3 con el Administrador de inquilinos, debe usar un ["Cliente S3"](#) o ["Consola S3"](#) para ingerir y gestionar objetos.

Cómo iniciar y cerrar sesión

Sign in en el Administrador de inquilinos

Puede acceder al Administrador de inquilinos ingresando la URL del inquilino en la barra de direcciones de un ["navegador web compatible"](#) .

Antes de empezar

- Tienes tus credenciales de inicio de sesión.
- Tiene una URL para acceder al Administrador de inquilinos, proporcionada por su administrador de red. La URL se verá como uno de estos ejemplos:

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

```
https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id
```

```
https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

La URL siempre incluye un nombre de dominio completo (FQDN), la dirección IP de un nodo de administración o la dirección IP virtual de un grupo de alta disponibilidad de nodos de administración. También podría incluir un número de puerto, el ID de la cuenta del inquilino de 20 dígitos o ambos.

- Si la URL no incluye el ID de cuenta de 20 dígitos del inquilino, tendrá este ID de cuenta.
- Estás usando un ["navegador web compatible"](#) .
- Las cookies están habilitadas en su navegador web.
- Pertenece a un grupo de usuarios que tiene ["permisos de acceso específicos"](#) .

Pasos

1. Lanzar un ["navegador web compatible"](#) .

2. En la barra de direcciones del navegador, ingrese la URL para acceder al Administrador de inquilinos.
3. Si aparece una alerta de seguridad, instale el certificado utilizando el asistente de instalación del navegador.
4. Sign in en el Administrador de inquilinos.

La pantalla de inicio de sesión que aparece depende de la URL ingresada y de si se ha configurado el inicio de sesión único (SSO) para StorageGRID.

No usar SSO

Si StorageGRID no utiliza SSO, aparecerá una de las siguientes pantallas:

- La página de inicio de sesión de Grid Manager. Seleccione el enlace **Inicio de sesión de inquilino**.



NetApp StorageGRID®

Grid Manager

Username

Password

[Sign in](#)

[Tenant sign in](#) | [NetApp support](#) | [NetApp.com](#)

- La página de inicio de sesión del administrador de inquilinos. Es posible que el campo **Cuenta** ya esté completado, como se muestra a continuación.

The screenshot shows the NetApp StorageGRID Tenant Manager login interface. At the top is the NetApp StorageGRID logo. Below it is the title 'Tenant Manager'. The form includes a 'Recent' section with a dropdown menu currently showing '-- Optional --'. Below that is an 'Account' section with a text box containing the ID '64600207336181242061'. The 'Username' section has an empty text box with a cursor. The 'Password' section has an empty text box. A blue 'Sign in' button is located below the password field. At the bottom, there are links for 'NetApp support' and 'NetApp.com'.

- i. Si no se muestra el ID de cuenta de 20 dígitos del inquilino, seleccione el nombre de la cuenta del inquilino si aparece en la lista de cuentas recientes o ingrese el ID de cuenta.
- ii. Introduzca su nombre de usuario y contraseña.
- iii. Seleccionar * Sign in*.

Aparece el panel del Administrador de inquilinos.

- iv. Si recibió una contraseña inicial de otra persona, seleccione **nombre de usuario > Cambiar contraseña** para proteger su cuenta.

Usando SSO

Si StorageGRID utiliza SSO, aparecerá una de las siguientes pantallas:

- La página SSO de su organización. Por ejemplo:

Sign in with your organizational account

someone@example.com

Password

Sign in

Ingrese sus credenciales SSO estándar y seleccione * Sign in*.

- La página de inicio de sesión SSO del administrador de inquilinos.

NetApp StorageGRID®

Tenant Manager

Recent

S3 tenant ▼

Account

62984032838045582045

Sign in

[NetApp support](#) | [NetApp.com](#)

- Si no se muestra el ID de cuenta de 20 dígitos del inquilino, seleccione el nombre de la cuenta del inquilino si aparece en la lista de cuentas recientes o ingrese el ID de cuenta.
- Seleccionar * Sign in*.
- Sign in con sus credenciales SSO estándar en la página de inicio de sesión SSO de su organización.

Aparece el panel del Administrador de inquilinos.

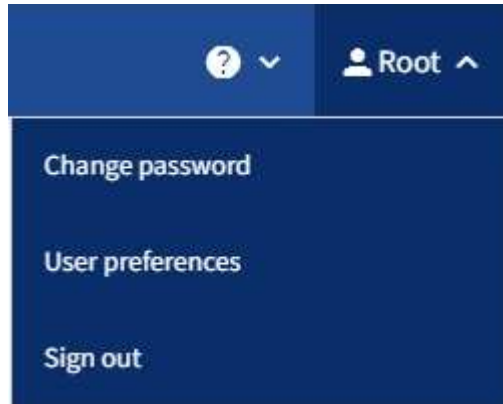
Cerrar sesión en el Administrador de inquilinos

Cuando termine de trabajar con el Administrador de inquilinos, deberá cerrar la sesión

para asegurarse de que usuarios no autorizados no puedan acceder al sistema StorageGRID . Es posible que cerrar su navegador no cierre su sesión del sistema, según la configuración de cookies del navegador.

Pasos

1. Localice el menú desplegable de nombre de usuario en la esquina superior derecha de la interfaz de usuario.



2. Seleccione el nombre de usuario y luego seleccione **Cerrar sesión**.

- Si no se utiliza SSO:

Has cerrado la sesión del nodo de administración. Se muestra la página de inicio de sesión del Administrador de inquilinos.



Si inició sesión en más de un nodo de administración, deberá cerrar sesión en cada nodo.

- Si SSO está habilitado:

Has cerrado la sesión de todos los nodos de administración a los que estabas accediendo. Se muestra la página de Sign in de StorageGRID . El nombre de la cuenta de inquilino a la que acaba de acceder aparece como predeterminado en el menú desplegable **Cuentas recientes** y se muestra el **ID de cuenta** del inquilino.



Si SSO está habilitado y también ha iniciado sesión en Grid Manager, también debe cerrar sesión en Grid Manager para cerrar sesión en SSO.

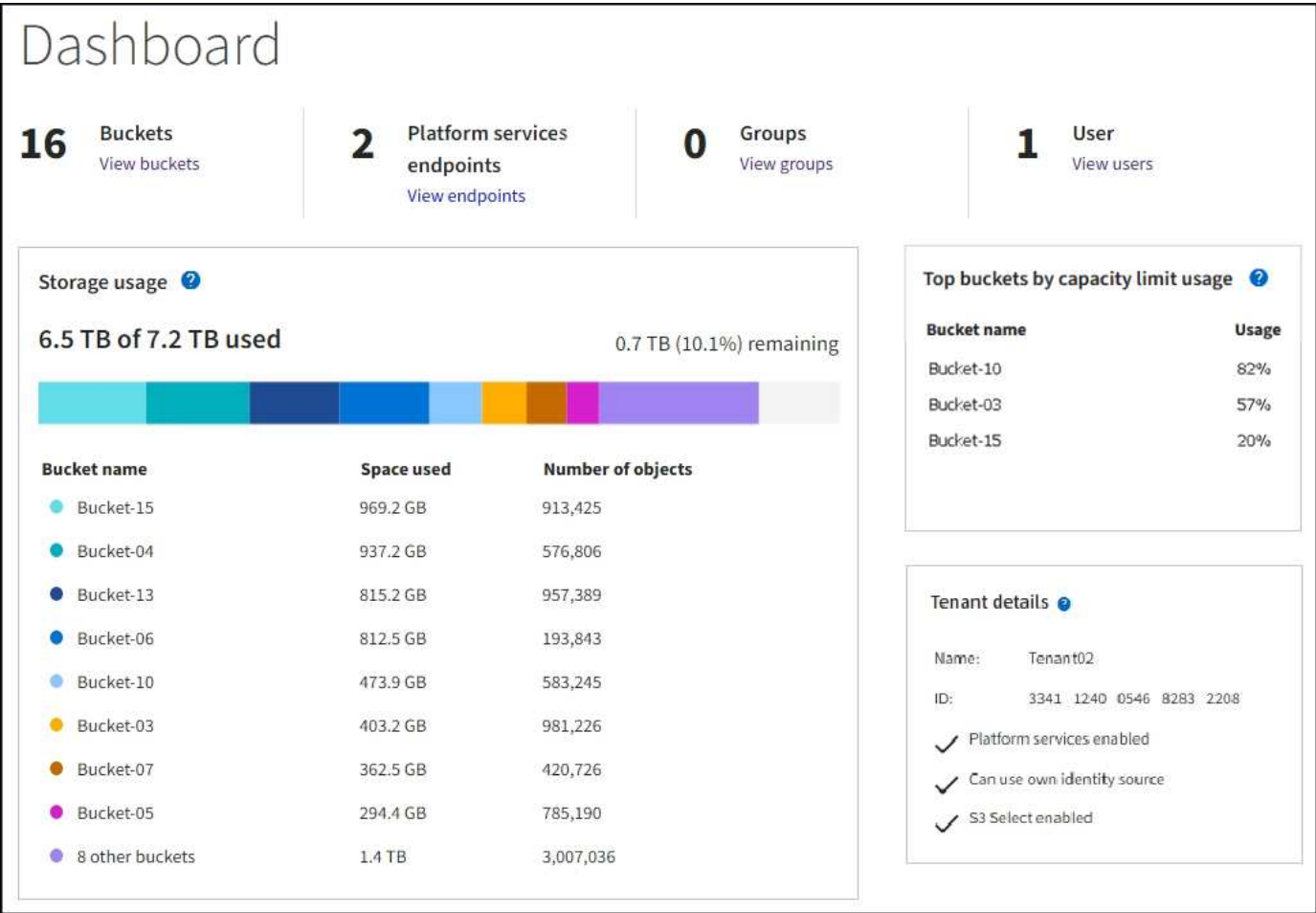
Comprender el panel de control de Tenant Manager

El panel de Tenant Manager proporciona una descripción general de la configuración de una cuenta de inquilino y la cantidad de espacio utilizado por los objetos en los depósitos (S3) o contenedores (Swift) del inquilino. Si el inquilino tiene una cuota, el panel muestra cuánto de la cuota se utiliza y cuánto queda. Si hay algún error relacionado con la cuenta del inquilino, los errores se muestran en el panel de control.



Los valores de espacio utilizado son estimaciones. Estas estimaciones se ven afectadas por el momento de la ingesta, la conectividad de la red y el estado del nodo.

Una vez cargados los objetos, el panel de control se verá como el siguiente ejemplo:



Información de la cuenta del inquilino

En la parte superior del panel se muestra la cantidad de depósitos o contenedores, grupos y usuarios configurados. También muestra el número de puntos finales de servicios de la plataforma, si se ha configurado alguno. Seleccione los enlaces para ver los detalles.

Dependiendo de la"permisos de gestión de inquilinos" Tiene las opciones que ha configurado y el resto del panel muestra varias combinaciones de pautas, uso de almacenamiento, información de objetos y detalles del inquilino.

Uso de almacenamiento y cuotas

El panel de uso de almacenamiento contiene la siguiente información:

- La cantidad de datos de objetos para el inquilino.

Este valor indica la cantidad total de datos de objetos 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 ingerir.



El uso de la cuota se basa en estimaciones internas y podría superarse en algunos casos. Por ejemplo, StorageGRID verifica la cuota cuando un inquilino comienza a cargar objetos y rechaza nuevas ingestas si el inquilino ha excedido la cuota. Sin embargo, StorageGRID no tiene en cuenta el tamaño de la carga actual al determinar si se ha excedido la cuota. Si se eliminan objetos, es posible que a un inquilino se le impida temporalmente cargar nuevos objetos hasta que se vuelva a calcular el uso de la cuota. Los cálculos de uso de cuota pueden tardar 10 minutos o más.

- Un gráfico de barras que representa los tamaños relativos de los cubos o contenedores más grandes.

Puede colocar el cursor sobre cualquiera de los segmentos del gráfico para ver el espacio total consumido por ese contenedor o depósito.



- Para corresponder con el gráfico de barras, una lista de los depósitos o contenedores más grandes, incluida la cantidad total de datos de objetos y la cantidad de objetos para cada depósito 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 contenedores o cubos, todos los demás contenedores o cubos se combinan en una sola entrada en la parte inferior de la lista.



Para cambiar las unidades de los valores de almacenamiento que se muestran en el Administrador de inquilinos, seleccione el menú desplegable de usuario en la parte superior derecha del Administrador de inquilinos y luego seleccione **Preferencias de usuario**.

Alertas de uso de cuota

Si se han habilitado las alertas de uso de cuota en el Administrador de red, estas alertas aparecerán en el Administrador de inquilinos cuando la cuota sea baja o se exceda, de la siguiente manera:

- Si se ha utilizado el 90 % o más de la cuota de un inquilino, se activa la alerta **Uso de cuota de inquilino alto**.

Considere pedirle a su administrador de red que aumente la cuota.

- Si excede su cuota, una notificación le indicará que no puede cargar nuevos objetos.

Uso del límite de capacidad

Si ha establecido un límite de capacidad para sus grupos, el panel del Administrador de inquilinos muestra una lista de los grupos principales según el uso del límite de capacidad.

Si no se establece ningún límite para un depósito, su capacidad es ilimitada. Sin embargo, si su cuenta de inquilino tiene una cuota de almacenamiento total y dicha cuota se alcanza, no podrá ingerir más objetos independientemente del límite de capacidad restante en un depósito.

Errores de punto final

Si ha utilizado Grid Manager para configurar uno o más puntos finales para su uso con servicios de plataforma, el panel de Tenant Manager muestra una alerta si se ha producido algún error en los puntos finales en los últimos siete días.



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.

Para ver detalles sobre "errores de punto final de servicios de plataforma", seleccione **Puntos finales** para mostrar la página Puntos finales.

API de gestión de inquilinos

Comprender la API de gestión de inquilinos

Puede realizar tareas de administración del sistema utilizando la API REST de administración de inquilinos en lugar de la interfaz de usuario del administrador de inquilinos. Por ejemplo, es posible que desee utilizar la API para automatizar operaciones o crear múltiples entidades, como usuarios, más rápidamente.

La API de gestión de inquilinos:

- Utiliza la plataforma API de código abierto 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 completos y documentación para cada operación de API.
- Usos "control de versiones para soportar actualizaciones sin interrupciones" .

Para acceder a la documentación de Swagger para la API de administración de inquilinos:

1. Sign in en el Administrador de inquilinos.
2. Desde la parte superior del Administrador de inquilinos, seleccione el ícono de ayuda y seleccione **Documentación de API**.

Operaciones de API

La API de administración de inquilinos organiza las operaciones de API disponibles en las siguientes secciones:

- **cuenta:** Operaciones en la cuenta del inquilino actual, incluida la obtención de información sobre el uso del almacenamiento.
- **auth:** Operaciones para realizar la autenticación de la sesión del usuario.

La API de administración de inquilinos admite el esquema de autenticación de token de portador. Para iniciar sesión en 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 debe proporcionarse en el encabezado de las solicitudes de API posteriores ("Autorización: Token de portador").

Para obtener información sobre cómo mejorar la seguridad de la autenticación, consulte ["Protección contra la falsificación de solicitudes entre sitios"](#).



Si el inicio de sesión único (SSO) está habilitado para el sistema StorageGRID, debe realizar diferentes pasos para autenticarse. Ver el ["Instrucciones para utilizar la API de administración de red"](#).

- **config:** Operaciones relacionadas con el lanzamiento del producto y las versiones de la API de administración de inquilinos. Puede enumerar la versión de lanzamiento del producto y las versiones principales de la API compatibles con esa versión.
- **contenedores:** Operaciones en buckets S3 o contenedores Swift.
- **funciones-desactivadas:** Operaciones para ver funciones que podrían haber sido desactivadas.
- **endpoints:** Operaciones para administrar un punto final. Los puntos finales permiten que un bucket S3 utilice un servicio externo para la replicación, las notificaciones o la integración de búsqueda de StorageGRID CloudMirror.
- **grid-federation-connections:** Operaciones en conexiones de federación de redes y replicación entre redes.
- **grupos:** Operaciones para administrar grupos de inquilinos locales y recuperar grupos de inquilinos federados desde una fuente de identidad externa.
- **identity-source:** Operaciones para configurar una fuente de identidad externa y sincronizar manualmente la información de usuarios y grupos federados.
- **ilm:** Operaciones en configuraciones de gestión del ciclo de vida de la información (ILM).
- **regiones:** Operaciones para determinar qué regiones se han configurado para el sistema StorageGRID.
- **s3:** Operaciones para administrar las claves de acceso S3 para los usuarios inquilinos.
- **s3-object-lock:** Operaciones en la configuración global de bloqueo de objetos S3, utilizadas para respaldar el cumplimiento normativo.
- **usuarios:** Operaciones para ver y administrar los usuarios del inquilino.

Detalles de la operación

Al expandir cada operación de API, puede ver su acción HTTP, la URL del punto final, una lista de parámetros obligatorios u opcionales, un ejemplo del cuerpo de la solicitud (cuando sea necesario) y las posibles respuestas.

groups
Operations on groups

GET

/org/groups

Lists Tenant User Groups

Parameters

Try it out

Name	Description
type string (query)	filter by group type
limit integer (query)	maximum number of results
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order string (query)	pagination order (desc requires marker)

Responses

Response content type

application/json

Code	Description
200	Example Value Model <pre>{ "responseTime": "2018-02-01T16:22:31.066Z", "status": "success", "apiVersion": "2.1" }</pre>

Emitir solicitudes de API



Cualquier operación de API que realice utilizando la página web de Documentación de API son operaciones en vivo. 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. Determinar si la solicitud requiere parámetros adicionales, como un ID de grupo o usuario. Luego, obtenga estos valores. Es posible que primero debas emitir una solicitud API diferente para obtener la información que necesitas.
3. Determina si necesitas modificar el cuerpo de la solicitud de ejemplo. Si es así, puede seleccionar **Modelo** para conocer los requisitos de cada campo.

4. Seleccione **Probarlo**.
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 fue exitosa.

Control de versiones de la API de gestión de inquilinos

La API de administración de inquilinos utiliza versiones para admitir actualizaciones sin interrupciones.

Por ejemplo, esta URL de solicitud especifica la versión 4 de la API.

```
https://hostname_or_ip_address/api/v4/authorize
```

La versión principal de la API se actualiza cuando se realizan cambios que *no son compatibles* con versiones anteriores. La versión menor de la API se actualiza cuando se realizan cambios que *son compatibles* con versiones anteriores. Los cambios compatibles incluyen la adición de nuevos puntos finales o nuevas propiedades.

El siguiente ejemplo ilustra cómo se actualiza la versión de la API según el tipo de cambios realizados.

Tipo de cambio en la API	Versión antigua	Nueva versión
Compatible con versiones anteriores	2,1	2,2
No compatible con versiones anteriores	2,1	3,0

Cuando instala el software StorageGRID por primera vez, solo se habilita la versión más reciente de la API. Sin embargo, cuando actualiza a una nueva versión de funciones de StorageGRID, continúa teniendo acceso a la versión anterior de API durante al menos una versión de funciones de StorageGRID .



Puede configurar las versiones compatibles. Consulte la sección **config** de la documentación de la API de Swagger para obtener más información. ["API de gestión de red"](#) Para más información. Debe desactivar el soporte para la versión anterior después de actualizar todos los clientes API para usar la versión más nueva.

Las solicitudes obsoletas se marcan como obsoletas de las siguientes maneras:

- El encabezado de respuesta es "Obsoleto: verdadero".
- El cuerpo de la respuesta JSON incluye "deprecated": true
- Se agrega una advertencia obsoleta a nms.log. Por ejemplo:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determinar qué versiones de API son compatibles con la versión actual

Utilice el GET `/versions` Solicitud de API para devolver una lista de las principales versiones de API compatibles. Esta solicitud se encuentra en la sección **config** de la documentación de la API de Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Especificar una versión de API para una solicitud

Puede especificar la versión de la API utilizando un parámetro de ruta (`/api/v4`) o un encabezado (`Api-Version: 4`). Si proporciona ambos valores, el valor del encabezado anula el valor de la ruta.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protección contra la falsificación de solicitudes entre sitios (CSRF)

Puede ayudar a protegerse contra ataques de falsificación de solicitud entre sitios (CSRF) contra StorageGRID mediante el uso de tokens CSRF para mejorar la autenticación que utiliza cookies. El administrador de red y el administrador de inquilinos habilitan automáticamente esta función de seguridad; otros clientes de API pueden elegir si habilitarla cuando inician sesión.

Un atacante que puede activar una solicitud a un sitio diferente (por ejemplo, con un formulario HTTP POST) puede provocar que ciertas solicitudes se realicen utilizando las cookies del usuario que inició sesión.

StorageGRID ayuda a proteger contra ataques CSRF mediante el uso de tokens CSRF. Cuando está habilitada, el contenido de una cookie específica debe coincidir con el contenido de un encabezado específico o de un parámetro de cuerpo POST específico.

Para habilitar la función, configure el `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 cierto, una `GridCsrfToken` La cookie se establece con un valor aleatorio para los inicios de sesión en Grid Manager y `AccountCsrfToken` La cookie se establece con un valor aleatorio para los inicios 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 uno de los siguientes:

- El `X-Csrf-Token` encabezado, con el valor del encabezado establecido en el valor de la cookie del token CSRF.
- Para los puntos finales que aceptan un cuerpo codificado por formulario: A `csrfToken` parámetro del cuerpo de la solicitud codificado en formulario.

Para configurar la protección CSRF, utilice el ["API de gestión de red"](#) o ["API de gestión de inquilinos"](#).



Las solicitudes que tienen una cookie de token CSRF configurada también aplicarán el encabezado `"Content-Type: application/json"` para cualquier solicitud que espere un cuerpo de solicitud JSON como protección adicional contra ataques CSRF.

Utilizar conexiones de federación de red

Clonar grupos de inquilinos y usuarios

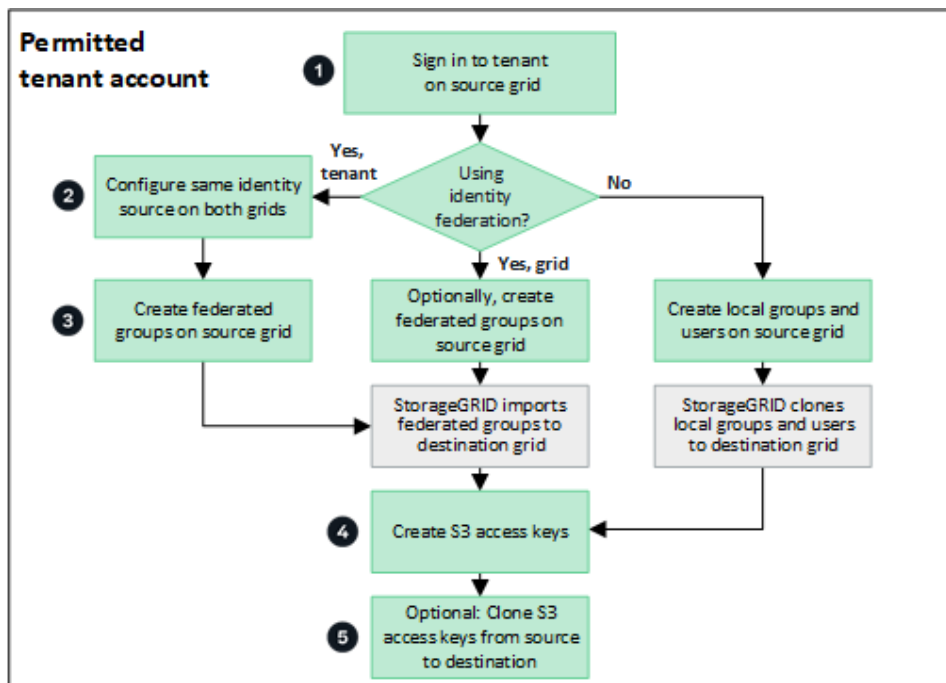
Si se creó o editó un inquilino para usar una conexión de federación de red, ese inquilino se replica desde un sistema StorageGRID (el inquilino de origen) a otro sistema StorageGRID (el inquilino de réplica). Una vez replicado el inquilino, todos los grupos y usuarios agregados al inquilino de origen se clonan en el inquilino de réplica.

El sistema StorageGRID donde se crea originalmente el inquilino es la *cuadrícula de origen* del inquilino. El sistema StorageGRID donde se replica el inquilino es la *red de destino* del inquilino. Ambas cuentas de inquilino tienen el mismo ID de cuenta, nombre, descripción, cuota de almacenamiento y permisos asignados, pero el inquilino de destino no tiene inicialmente una contraseña de usuario raíz. Para más detalles, véase ["¿Qué es la clonación de cuenta?"](#) y ["Gestionar inquilinos permitidos"](#).

La clonación de la información de la cuenta del inquilino es necesaria para ["replicación entre redes"](#) de objetos de cubo. Tener los mismos grupos de inquilinos y usuarios en ambas redes garantiza que pueda acceder a los depósitos y objetos correspondientes en cualquiera de las redes.

Flujo de trabajo del inquilino para la clonación de cuentas

Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, revise el diagrama de flujo de trabajo para ver los pasos que realizará para clonar grupos, usuarios y claves de acceso S3.



Estos son los pasos principales del flujo de trabajo:

1

Sign in en el inquilino

Sign in en la cuenta del inquilino en la cuadrícula de origen (la cuadrícula donde se creó inicialmente el inquilino).

2

Opcionalmente, configure la federación de identidad

Si su cuenta de inquilino tiene el permiso **Usar fuente de identidad propia** para usar grupos y usuarios federados, configure la misma fuente de identidad (con la misma configuración) para las cuentas de inquilino de origen y de destino. Los grupos y usuarios federados no se pueden clonar a menos que ambas redes utilicen la misma fuente de identidad. Para obtener instrucciones, consulte ["Utilizar la federación de identidades"](#).

3

Crear grupos y usuarios

Al crear grupos y usuarios, comience siempre desde la cuadrícula de origen del inquilino. Cuando agrega un nuevo grupo, StorageGRID lo clona automáticamente en la cuadrícula de destino.

- Si la federación de identidad está configurada para todo el sistema StorageGRID o para su cuenta de inquilino, ["crear nuevos grupos de inquilinos"](#) importando grupos federados desde la fuente de identidad.
- Si no está utilizando la federación de identidad, ["crear nuevos grupos locales"](#) y luego ["crear usuarios locales"](#).

4

Crear claves de acceso S3

Puede ["crea tus propias claves de acceso"](#) o a ["crear las claves de acceso de otro usuario"](#) en la red de origen o en la red de destino para acceder a los contenedores en esa red.

Opcionalmente, clonar claves de acceso S3

Si necesita acceder a depósitos con las mismas claves de acceso en ambas cuadrículas, cree las claves de acceso en la cuadrícula de origen y luego use la API de Tenant Manager para clonarlas manualmente en la cuadrícula de destino. Para obtener instrucciones, consulte ["Clonar claves de acceso S3 usando la API"](#).

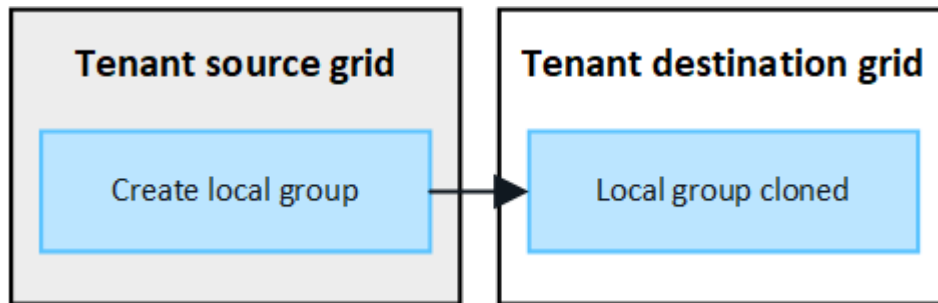
¿Cómo se clonan grupos, usuarios y claves de acceso S3?

Revise esta sección para comprender cómo se clonan los grupos, los usuarios y las claves de acceso de S3 entre la red de origen del inquilino y la red de destino del inquilino.

Los grupos locales creados en la red de origen se clonan

Una vez que se crea una cuenta de inquilino y se replica en la red de destino, StorageGRID clona automáticamente cualquier grupo local que agregue a la red de origen del inquilino en la red de destino del inquilino.

Tanto el grupo original como su clon tienen el mismo modo de acceso, permisos de grupo y política de grupo S3. Para obtener instrucciones, consulte ["Crear grupos para el inquilino S3"](#).

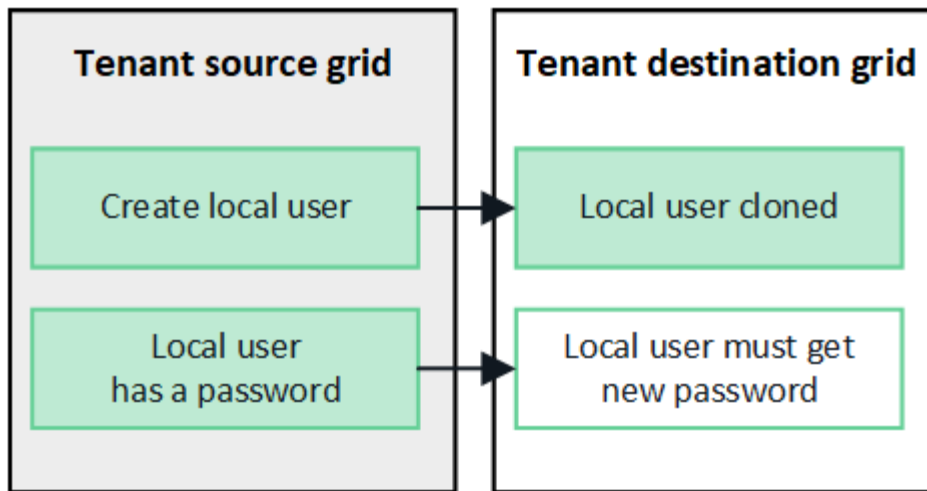


Cualquier usuario que seleccione al crear un grupo local en la cuadrícula de origen no se incluirá cuando el grupo se clone en la cuadrícula de destino. Por este motivo, no seleccione usuarios al crear el grupo. En su lugar, seleccione el grupo cuando cree los usuarios.

Los usuarios locales creados en la red de origen se clonan

Cuando crea un nuevo usuario local en la red de origen, StorageGRID clona automáticamente ese usuario en la red de destino. Tanto el usuario original como su clon tienen el mismo nombre completo, nombre de usuario y configuración **Denegar acceso**. Ambos usuarios también pertenecen a los mismos grupos. Para obtener instrucciones, consulte ["Administrar usuarios locales"](#).

Por razones de seguridad, las contraseñas de los usuarios locales no se clonan en la red de destino. Si un usuario local necesita acceder a Tenant Manager en la red de destino, el usuario raíz de la cuenta de inquilino debe agregar una contraseña para ese usuario en la red de destino. Para obtener instrucciones, consulte ["Administrar usuarios locales"](#).

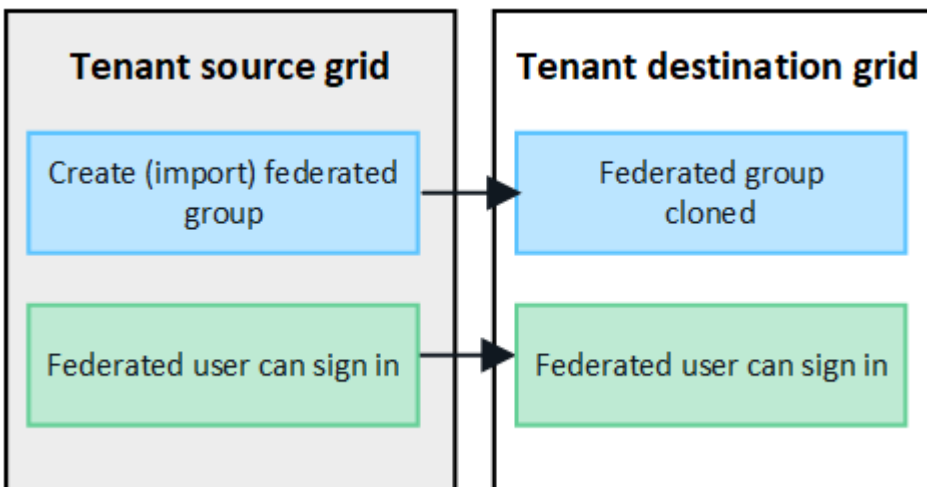


Los grupos federados creados en la red de origen se clonan

Suponiendo que se cumplen los requisitos para usar la clonación de cuenta con ["inicio de sesión único"](#) y ["federación de identidades"](#) Una vez cumplidos, los grupos federados que cree (importe) para el inquilino en la red de origen se clonan automáticamente en el inquilino en la red de destino.

Ambos grupos tienen el mismo modo de acceso, permisos de grupo y política de grupo S3.

Una vez creados los grupos federados para el inquilino de origen y clonados en el inquilino de destino, los usuarios federados pueden iniciar sesión en el inquilino en cualquiera de las cuadrículas.

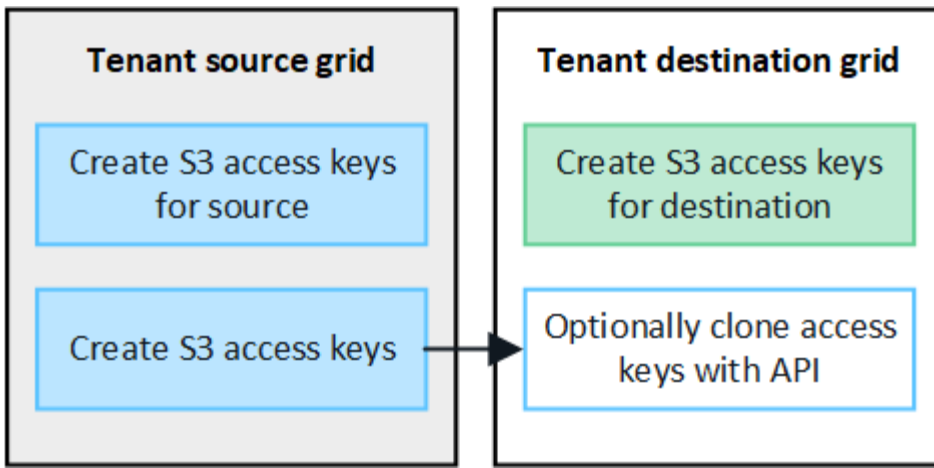


Las claves de acceso S3 se pueden clonar manualmente

StorageGRID no clona automáticamente las claves de acceso de S3 porque la seguridad se mejora al tener claves diferentes en cada cuadrícula.

Para administrar las claves de acceso en las dos cuadrículas, puede realizar una de las siguientes acciones:

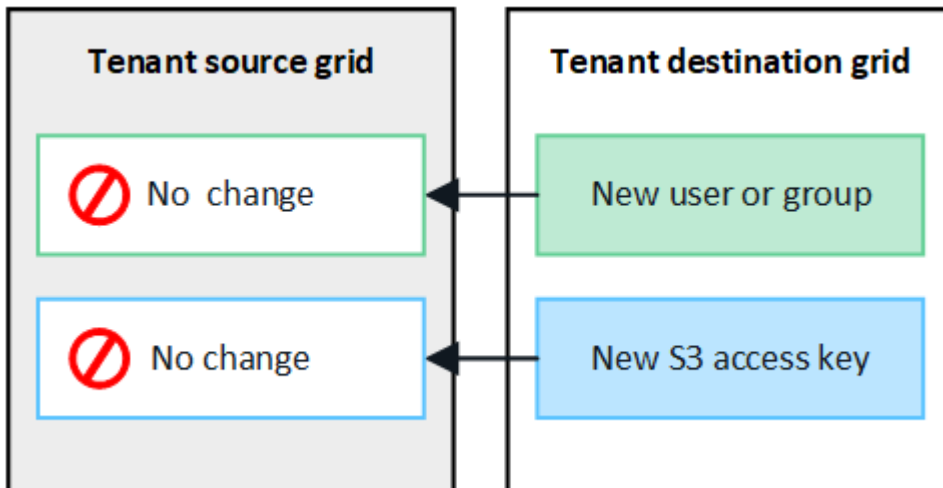
- Si no necesita utilizar las mismas claves para cada cuadrícula, puede ["crea tus propias claves de acceso"](#) o ["crear las claves de acceso de otro usuario"](#) en cada cuadrícula.
- Si necesita usar las mismas claves en ambas cuadrículas, puede crear claves en la cuadrícula de origen y luego usar la API de Tenant Manager para hacerlo manualmente. ["clonar las claves"](#) a la red de destino.



Cuando se clonan claves de acceso S3 para un usuario federado, tanto el usuario como las claves de acceso S3 se clonan en el inquilino de destino.

Los grupos y usuarios agregados a la cuadrícula de destino no se clonan

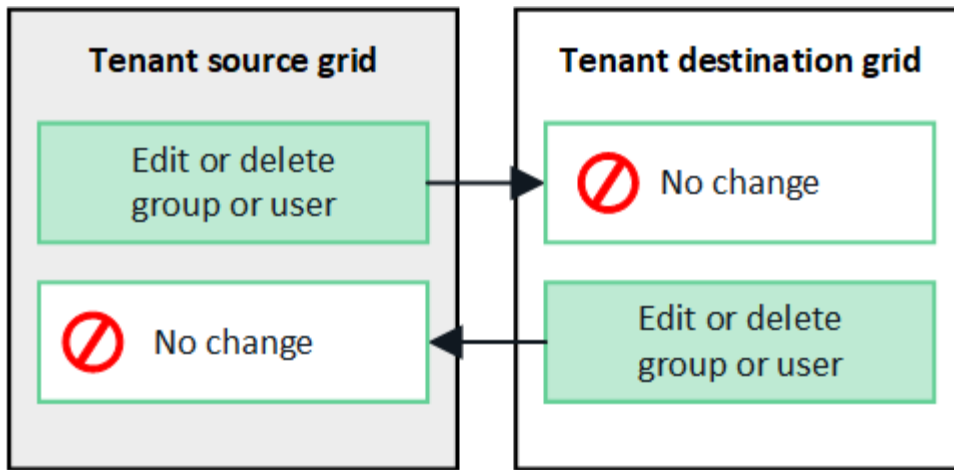
La clonación se produce únicamente desde la red de origen del inquilino a la red de destino del inquilino. Si crea o importa grupos y usuarios en la cuadrícula de destino del inquilino, StorageGRID no clonará estos elementos en la cuadrícula de origen del inquilino.



Los grupos, usuarios y claves de acceso editados o eliminados no se clonan

La clonación ocurre solo cuando se crean nuevos grupos y usuarios.

Si edita o elimina grupos, usuarios o claves de acceso en cualquiera de las cuadrículas, sus cambios no se clonarán en la otra cuadrícula.



Clonar claves de acceso S3 usando la API

Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, puede usar la API de administración de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en la red de origen al inquilino en la red de destino.

Antes de empezar

- La cuenta de inquilino tiene el permiso **Usar conexión de federación de red**.
- La conexión de la federación de red tiene un **Estado de conexión** de **Conectado**.
- Ha iniciado sesión en el Administrador de inquilinos en la cuadrícula de origen del inquilino mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene la ["Administre sus propias credenciales S3 o permiso de acceso root"](#).
- Si está clonando claves de acceso para un usuario local, el usuario ya existe en ambas cuadrículas.



Cuando se clonan claves de acceso S3 para un usuario federado, tanto el usuario como las claves de acceso S3 se agregan al inquilino de destino.

Clona tus propias claves de acceso

Puede clonar sus propias claves de acceso si necesita acceder a los mismos depósitos en ambas cuadrículas.

Pasos

1. Usando el Administrador de inquilinos en la red de origen, ["crea tus propias claves de acceso"](#) y descargar el `.csv` archivo.
2. Desde la parte superior del Administrador de inquilinos, seleccione el ícono de ayuda y seleccione **Documentación de API**.
3. En la sección **s3**, seleccione el siguiente punto final:

```
POST /org/users/current-user/replicate-s3-access-key
```

POST

`/org/users/current-user/replicate-s3-access-key` Clone the current user's S3 key to the other grids.



4. Seleccione **Probarlo**.

5. En el cuadro de texto **body**, reemplace las entradas de ejemplo para **accessKey** y **secretAccessKey** con los valores del archivo **.csv** que descargó.

Asegúrese de conservar las comillas dobles alrededor de cada cadena.



The screenshot shows a REST client interface with a 'body' field marked as '* required'. Below the field name, there are tabs for 'Edit Value' and 'Model'. The 'Model' tab is selected, displaying a JSON object:

```
{  "accessKey": "AKIAIOSFODNN7EXAMPLE",  "secretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY",  "expires": "2028-09-04T00:00:00.000Z"}
```

6. Si la clave caducará, reemplace la entrada de ejemplo para **expires** con la fecha y hora de caducidad como una cadena en formato de datos y tiempo ISO 8601 (por ejemplo, 2024-02-28T22:46:33-08:00). Si la clave no caducará, ingrese **null** como valor para la entrada **expires** (o elimine la línea **Expires** y la coma anterior).
7. Seleccione **Ejecutar**.
8. Confirme que el código de respuesta del servidor es **204**, lo que indica que la clave se clonó correctamente en la red de destino.

Clonar las claves de acceso de otro usuario

Puede clonar las claves de acceso de otro usuario si necesita acceder a los mismos depósitos en ambas cuadrículas.

Pasos

1. Usando el Administrador de inquilinos en la red de origen, "[crear las claves de acceso S3 del otro usuario](#)" y descargar el **.csv** archivo.
2. Desde la parte superior del Administrador de inquilinos, seleccione el ícono de ayuda y seleccione **Documentación de API**.
3. Obtener el ID del usuario. Necesitará este valor para clonar las claves de acceso del otro usuario.
 - a. Desde la sección **usuarios**, seleccione el siguiente punto final:

```
GET /org/users
```

- b. Seleccione **Probarlo**.
 - c. Especifique cualquier parámetro que desee utilizar al buscar usuarios.
 - d. Seleccione **Ejecutar**.
 - e. Busque el usuario cuyas claves desea clonar y copie el número en el campo **id**.
4. En la sección **s3**, seleccione el siguiente punto final:

```
POST /org/users/{userId}/replicate-s3-access-key
```



The screenshot shows a REST client interface with a 'POST' button and the endpoint `/org/users/{userId}/replicate-s3-access-key`. To the right of the endpoint, there is a description: 'Clone an S3 key to the other grids.' and a lock icon.

5. Seleccione **Probarlo**.

6. En el cuadro de texto **userid**, pegue el ID de usuario que copió.
7. En el cuadro de texto **body**, reemplace las entradas de ejemplo para **example access key** y **secret access key** con los valores del archivo **.csv** para ese usuario.

Asegúrese de conservar las comillas dobles alrededor de la cadena.

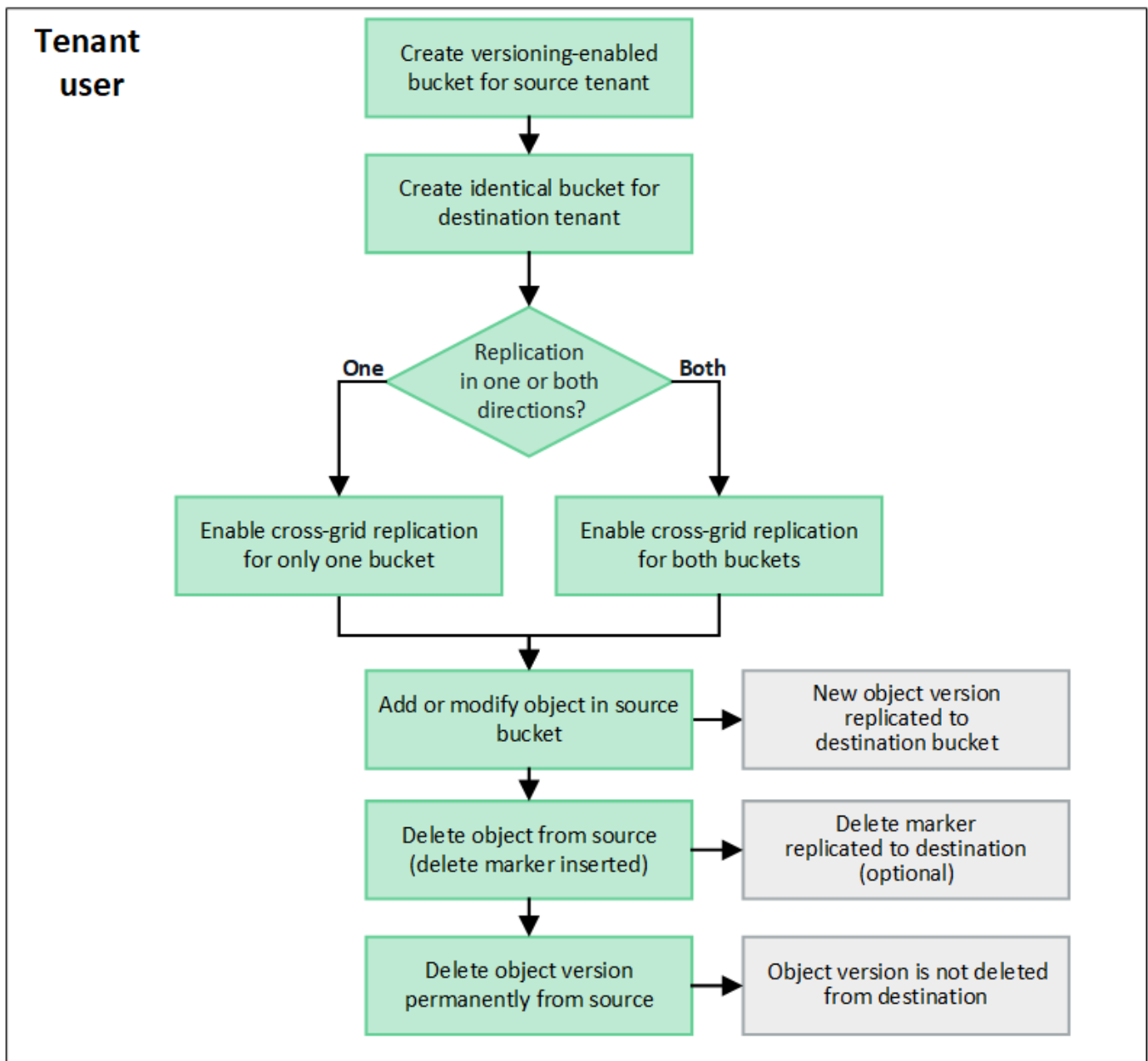
8. Si la clave caducará, reemplace la entrada de ejemplo para **expires** con la fecha y hora de caducidad como una cadena en formato de datos y tiempo ISO 8601 (por ejemplo, **2023-02-28T22:46:33-08:00**). Si la clave no caducará, ingrese **null** como valor para la entrada **expires** (o elimine la línea **Expires** y la coma anterior).
9. Seleccione **Ejecutar**.
10. Confirme que el código de respuesta del servidor es **204**, lo que indica que la clave se clonó correctamente en la red de destino.

Administrar la replicación entre redes

Si a su cuenta de inquilino se le asignó el permiso **Usar conexión de federación de red** cuando se creó, puede usar la replicación entre redes para replicar automáticamente objetos entre depósitos en la red de origen del inquilino y depósitos en la red de destino del inquilino. La replicación entre redes puede ocurrir en una o ambas direcciones.

Flujo de trabajo para la replicación entre redes

El diagrama de flujo de trabajo resume los pasos que realizará para configurar la replicación entre cuadrículas entre depósitos en dos cuadrículas. Estos pasos se describen con más detalle a continuación.



Configurar la replicación entre redes

Antes de poder utilizar la replicación entre redes, debe iniciar sesión en las cuentas de inquilino correspondientes en cada red y crear grupos idénticos. Luego, puedes habilitar la replicación entre redes en uno o ambos depósitos.

Antes de empezar

- Ha revisado los requisitos para la replicación entre redes. Ver "[¿Qué es la replicación entre redes?](#)".
- Estás usando un "[navegador web compatible](#)".
- La cuenta de inquilino tiene el permiso **Usar conexión de federación de red** y existen cuentas de inquilino idénticas en ambas redes. Ver "[Administrar los inquilinos permitidos para la conexión de la federación de red](#)".
- El usuario inquilino con el que iniciará sesión ya existe en ambas redes y pertenece a un grupo de usuarios que tiene la "[Permiso de acceso root](#)".

- Si va a iniciar sesión en la red de destino del inquilino como usuario local, el usuario raíz de la cuenta del inquilino ha establecido una contraseña para su cuenta de usuario en esa red.

Crea dos cubos idénticos

Como primer paso, inicie sesión en las cuentas de inquilino correspondientes en cada red y cree grupos idénticos.

Pasos

1. A partir de cualquiera de las cuadrículas en la conexión de la federación de cuadrículas, cree un nuevo depósito:

- a. Sign in en la cuenta del inquilino utilizando las credenciales de un usuario inquilino que exista en ambas redes.



Si no puede iniciar sesión en la red de destino del inquilino como usuario local, confirme que el usuario raíz de la cuenta del inquilino haya establecido una contraseña para su cuenta de usuario.

- b. Siga las instrucciones para ["crear un bucket S3"](#).
 - c. En la pestaña **Administrar configuración de objetos**, seleccione **Habilitar control de versiones de objetos**.
 - d. Si el Bloqueo de objetos S3 está habilitado para su sistema StorageGRID, no habilite el Bloqueo de objetos S3 para el depósito.
 - e. Seleccione **Crear depósito**.
 - f. Seleccione **Finalizar**.
2. Repita estos pasos para crear un depósito idéntico para la misma cuenta de inquilino en la otra red en la conexión de federación de red.



Según sea necesario, cada bucket puede utilizar una región diferente.

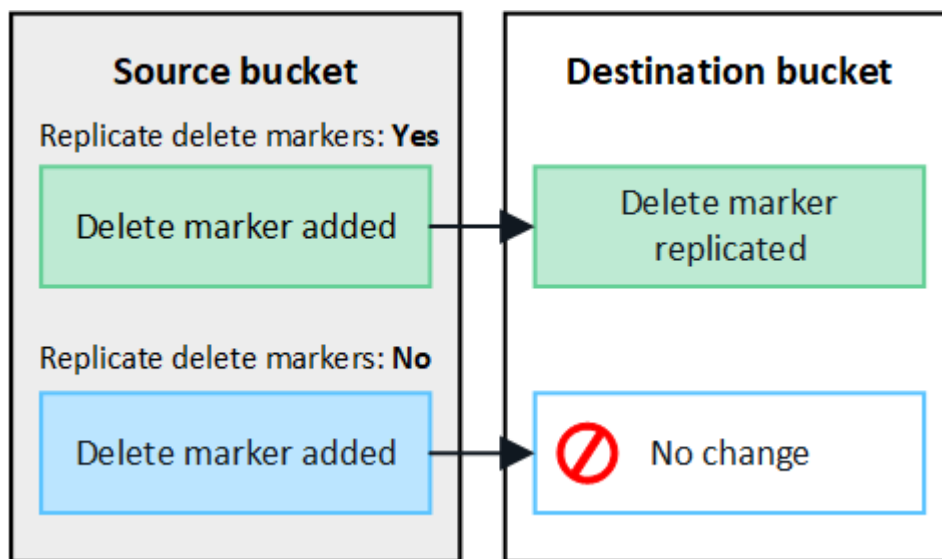
Habilitar la replicación entre redes

Debes realizar estos pasos antes de agregar cualquier objeto a cualquiera de los depósitos.

Pasos

1. A partir de una cuadrícula cuyos objetos desea replicar, habilite ["replicación entre redes en una dirección"](#) :
 - a. Sign in en la cuenta de inquilino del depósito.
 - b. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.
 - c. Seleccione el nombre del depósito de la tabla para acceder a la página de detalles del depósito.
 - d. Seleccione la pestaña **Replicación entre cuadrículas**.
 - e. Seleccione **Habilitar** y revise la lista de requisitos.
 - f. Si se cumplen todos los requisitos, seleccione la conexión de federación de red que desea utilizar.
 - g. De manera opcional, cambie la configuración de **Replicar marcadores de eliminación** para determinar qué sucede en la cuadrícula de destino si un cliente S3 emite una solicitud de eliminación a la cuadrícula de origen que no incluye un ID de versión:

- **Sí** (predeterminado): se agrega un marcador de eliminación al depósito de origen y se replica en el depósito de destino.
- **No**: Se agrega un marcador de eliminación al depósito de origen, pero no se replica en el depósito de destino.



Si la solicitud de eliminación incluye un ID de versión, esa versión del objeto se elimina de forma permanente del depósito de origen. StorageGRID no replica las solicitudes de eliminación que incluyen un ID de versión, por lo que la misma versión del objeto no se elimina del destino.

Ver "[¿Qué es la replicación entre redes?](#)" Para más detalles.

- De manera opcional, cambie la configuración de la categoría de auditoría **Replicación entre redes** para administrar el volumen de mensajes de auditoría:
 - **Error** (predeterminado): solo las solicitudes de replicación entre redes fallidas se incluyen en la salida de auditoría.
 - **Normal**: Se incluyen todas las solicitudes de replicación entre redes, lo que aumenta significativamente el volumen de la salida de auditoría.
- Revise sus selecciones. No podrás cambiar estas configuraciones a menos que ambos depósitos estén vacíos.
- Seleccione **Habilitar y probar**.

Después de unos momentos, aparece un mensaje de éxito. Los objetos agregados a este depósito ahora se replicarán automáticamente en la otra cuadrícula. La **replicación entre redes** se muestra como una función habilitada en la página de detalles del depósito.

- Opcionalmente, vaya al bucket correspondiente en la otra cuadrícula y "[Permitir la replicación entre redes en ambas direcciones](#)".

Prueba de replicación entre redes

Si la replicación entre redes está habilitada para un depósito, es posible que deba verificar que la conexión y la replicación entre redes funcionen correctamente y que los depósitos de origen y destino aún cumplan con todos los requisitos (por ejemplo, el control de versiones aún esté habilitado).

Antes de empezar

- Estás usando un ["navegador web compatible"](#) .
- Pertenece a un grupo de usuarios que tiene la ["Permiso de acceso root"](#) .

Pasos

1. Sign in en la cuenta de inquilino del depósito.
2. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.
3. Seleccione el nombre del depósito de la tabla para acceder a la página de detalles del depósito.
4. Seleccione la pestaña **Replicación entre cuadrículas**.
5. Seleccione **Probar conexión**.

Si la conexión es saludable, aparece un banner de éxito. De lo contrario, aparecerá un mensaje de error que usted y el administrador de la red pueden utilizar para resolver el problema. Para obtener más información, consulte ["Solucionar errores de federación de red"](#) .

6. Si la replicación entre redes está configurada para que ocurra en ambas direcciones, vaya al depósito correspondiente en la otra red y seleccione **Probar conexión** para verificar que la replicación entre redes esté funcionando en la otra dirección.

Deshabilitar la replicación entre redes

Puede detener permanentemente la replicación entre cuadrículas si ya no desea copiar objetos a la otra cuadrícula.

Antes de deshabilitar la replicación entre redes, tenga en cuenta lo siguiente:

- Deshabilitar la replicación entre cuadrículas no elimina ningún objeto que ya se haya copiado entre cuadrículas. Por ejemplo, los objetos en `my-bucket` en la cuadrícula 1 que se han copiado a `my-bucket` en Grid 2 no se eliminan si deshabilita la replicación entre redes para ese depósito. Si desea eliminar estos objetos, deberá eliminarlos manualmente.
- Si se habilitó la replicación entre redes para cada uno de los buckets (es decir, si la replicación ocurre en ambas direcciones), puede deshabilitar la replicación entre redes para uno o ambos buckets. Por ejemplo, es posible que desee deshabilitar la replicación de objetos desde `my-bucket` en la cuadrícula 1 a `my-bucket` en la cuadrícula 2, mientras continúa replicando objetos desde `my-bucket` en la red 2 a `my-bucket` en la cuadrícula 1.
- Debe deshabilitar la replicación entre redes antes de poder quitar el permiso de un inquilino para usar la conexión de federación de red. Ver ["Gestionar inquilinos permitidos"](#) .
- Si deshabilita la replicación entre cuadrículas para un depósito que contiene objetos, no podrá volver a habilitarla a menos que elimine todos los objetos de los depósitos de origen y destino.



No se puede volver a habilitar la replicación a menos que ambos depósitos estén vacíos.

Antes de empezar

- Estás usando un ["navegador web compatible"](#) .
- Pertenece a un grupo de usuarios que tiene la ["Permiso de acceso root"](#) .

Pasos

1. A partir de la cuadrícula cuyos objetos ya no desea replicar, detenga la replicación entre cuadrículas para el depósito:

- Sign in en la cuenta de inquilino del depósito.
- Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.
- Seleccione el nombre del depósito de la tabla para acceder a la página de detalles del depósito.
- Seleccione la pestaña **Replicación entre cuadrículas**.
- Seleccione **Deshabilitar replicación**.
- Si está seguro de que desea deshabilitar la replicación entre redes para este bucket, escriba **Sí** en el cuadro de texto y seleccione **Deshabilitar**.

Después de unos momentos, aparece un mensaje de éxito. Los nuevos objetos agregados a este depósito ya no se pueden replicar automáticamente en la otra cuadrícula. **La replicación entre cuadrículas** ya no se muestra como una función habilitada en la página de Cubos.

- Si la replicación entre redes se configuró para que ocurriera en ambas direcciones, vaya al depósito correspondiente en la otra red y detenga la replicación entre redes en la otra dirección.

Ver las conexiones de la federación de red

Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, puede ver las conexiones permitidas.

Antes de empezar

- La cuenta de inquilino tiene el permiso **Usar conexión de federación de red**.
- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Perteneces a un grupo de usuarios que tiene la ["Permiso de acceso root"](#).

Pasos

- Seleccione **ALMACENAMIENTO (S3) > Conexiones de federación de red**.

Aparece la página de conexión de la federación Grid e incluye una tabla que resume la siguiente información:

Columna	Descripción
Nombre de la conexión	Las conexiones de la federación de red que este inquilino tiene permiso para utilizar.
Cubos con replicación entre redes	Para cada conexión de federación de red, los grupos de inquilinos que tienen habilitada la replicación entre redes. Los objetos agregados a estos depósitos se replicarán en la otra cuadrícula de la conexión.
Último error	Para cada conexión de federación de red, el error más reciente que ocurrió, si lo hubo, cuando se replicaron los datos a la otra red. Ver Borrar el último error .

- Opcionalmente, seleccione un nombre de depósito para ["ver detalles del depósito"](#).

Borrar el último error

Podría aparecer un error en la columna **Último error** por uno de estos motivos:

- No se encontró la versión del objeto de origen.
- No se encontró el depósito de origen.
- Se eliminó el depósito de destino.
- El depósito de destino fue recreado por una cuenta diferente.
- El bucket de destino tiene la versión suspendida.
- El depósito de destino fue recreado por la misma cuenta pero ahora no tiene versión.



Esta columna solo muestra el último error de replicación entre redes que ocurrió; no se mostrarán los errores anteriores que pudieran haber ocurrido.

Pasos

1. Si aparece un mensaje en la columna **Último error**, vea el texto del mensaje.

Por ejemplo, este error indica que el depósito de destino para la replicación entre redes estaba en un estado no válido, posiblemente porque se suspendió el control de versiones o se habilitó el bloqueo de objetos S3.

2. Realice cualquier acción recomendada. Por ejemplo, si se suspendió el control de versiones en el depósito de destino para la replicación entre redes, vuelva a habilitar el control de versiones para ese depósito.
3. Seleccione la conexión de la tabla.
4. Seleccione **Borrar error**.
5. Seleccione **Sí** para borrar el mensaje y actualizar el estado del sistema.
6. Espere 5-6 minutos y luego ingiera un nuevo objeto en el balde. Confirme que el mensaje de error no vuelva a aparecer.



Para garantizar que se borre el mensaje de error, espere al menos 5 minutos después de la marca de tiempo en el mensaje antes de ingerir un nuevo objeto.

7. Para determinar si algún objeto no se pudo replicar debido al error del depósito, consulte ["Identificar y reintentar operaciones de replicación fallidas"](#).

Administrar grupos y usuarios

Utilizar la federación de identidades

El uso de la federación de identidades agiliza la configuración de grupos de inquilinos y usuarios, y permite a los usuarios inquilinos iniciar sesión en la cuenta de inquilino usando credenciales familiares.

Configurar la federación de identidades para Tenant Manager

Puede configurar la federación de identidad para el Administrador de inquilinos si desea que los grupos de inquilinos y los usuarios se administren en otro sistema, como Active Directory, Azure Active Directory (Azure AD), OpenLDAP u Oracle Directory Server.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#) .
- Pertenece a un grupo de usuarios que tiene la ["Permiso de acceso root"](#) .
- Está utilizando Active Directory, Azure AD, OpenLDAP u Oracle Directory Server como proveedor de identidad.



Si desea utilizar un servicio LDAP v3 que no figura en la lista, comuníquese con el soporte técnico.

- Si planea utilizar OpenLDAP, debe configurar el servidor OpenLDAP. Ver [Directrices para configurar el servidor OpenLDAP](#) .
- Si planea utilizar Seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidad debe utilizar TLS 1.2 o 1.3. Ver ["Cifrados compatibles para conexiones TLS salientes"](#) .

Acerca de esta tarea

La posibilidad de configurar un servicio de federación de identidad para su inquilino depende de cómo se configuró su cuenta de inquilino. Es posible que su inquilino comparta el servicio de federación de identidad que se configuró para Grid Manager. Si ve este mensaje cuando accede a la página Federación de identidad, no puede configurar una fuente de identidad federada separada para este inquilino.



This tenant account uses the LDAP server that is configured for the Grid Manager.
Contact the grid administrator for information or to change this setting.

Ingresar configuración

Cuando configura la federación de identidad, proporciona los valores que StorageGRID necesita para conectarse a un servicio LDAP.

Pasos

1. Seleccione **GESTIÓN DE ACCESO > Federación de identidades**.
2. Seleccione **Habilitar federación de identidad**.
3. En la sección Tipo de servicio LDAP, seleccione el tipo de servicio LDAP que desea configurar.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Azure	OpenLDAP	Other

Seleccione **Otro** para configurar valores para un servidor LDAP que utiliza Oracle Directory Server.

4. Si seleccionó **Otro**, complete los campos en la sección Atributos LDAP. De lo contrario, vaya al siguiente paso.
 - **Nombre único de usuario**: el 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 está configurando Oracle Directory Server, ingrese `uid`.

- **UUID de usuario:** el 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 está configurando Oracle Directory Server, ingrese `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:** el 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 está configurando Oracle Directory Server, ingrese `cn`.
- **UUID de grupo:** el 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 está configurando Oracle Directory Server, ingrese `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 servicios LDAP, ingrese la información de conexión de red y servidor LDAP requerida en la sección Configurar servidor LDAP.

- **Nombre de host:** 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, puedes utilizar cualquier puerto siempre que tu firewall esté configurado correctamente.

- **Nombre de usuario:** La ruta completa del nombre distinguido (DN) del 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 acceder a los siguientes atributos:

- `sAMAccountName` o `uid`
- `objectGUID`, `entryUUID`, o `nsuniqueid`
- `cn`
- `memberOf` o `isMemberOf`
- **Directorio Activo:** `objectSid`, `primaryGroupID`, `userAccountControl`, y `userPrincipalName`
- **Azur:** `accountEnabled` y `userPrincipalName`

- **Contraseña:** La contraseña asociada al nombre de usuario.



Si cambia la contraseña en el futuro, deberá actualizarla en esta página.

- **DN base de grupo:** la ruta completa del nombre distinguido (DN) de un subárbol LDAP en el que desea buscar grupos. En el ejemplo de Active Directory (abajo), todos los grupos cuyo nombre distintivo es relativo al DN base (`DC=storagegrid,DC=example,DC=com`) se pueden usar como grupos

federados.



Los valores de **Nombre único del grupo** deben ser únicos dentro del **DN base del grupo** al que pertenecen.

- **DN base de usuario:** la ruta completa del nombre distinguido (DN) de un subárbol LDAP en el 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 vinculado** (opcional): el patrón de nombre de usuario predeterminado que StorageGRID debe usar si el patrón no se puede determinar automáticamente.

Se recomienda proporcionar **Formato de nombre de usuario de enlace** porque puede permitir que los usuarios inicien sesión si StorageGRID no puede vincularse 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 distinguido:** CN=[USERNAME], CN=Users, DC=example, DC=com

Incluya **[NOMBRE DE USUARIO]** exactamente como está escrito.

6. En la sección Seguridad de la capa de transporte (TLS), seleccione una configuración de seguridad.

- **Usar STARTTLS:** utilice STARTTLS para proteger 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.
- **Usar LDAPS:** La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debe seleccionar esta opción para Azure.
- **No utilizar TLS:** El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Azure.



No se admite el uso de la opción **No usar TLS** si su servidor de Active Directory aplica la firma LDAP. Debe utilizar STARTTLS o LDAPS.

7. Si seleccionó STARTTLS o LDAPS, elija el certificado utilizado para proteger la conexión.

- **Usar certificado CA del sistema operativo:** utilice el certificado CA de Grid predeterminado instalado en el sistema operativo para proteger las conexiones.
- **Usar certificado CA personalizado:** utilice un certificado de seguridad personalizado.

Si selecciona esta configuración, copie y pegue el certificado de seguridad personalizado en el cuadro de texto del certificado de CA.

Pruebe la conexión y guarde la configuración

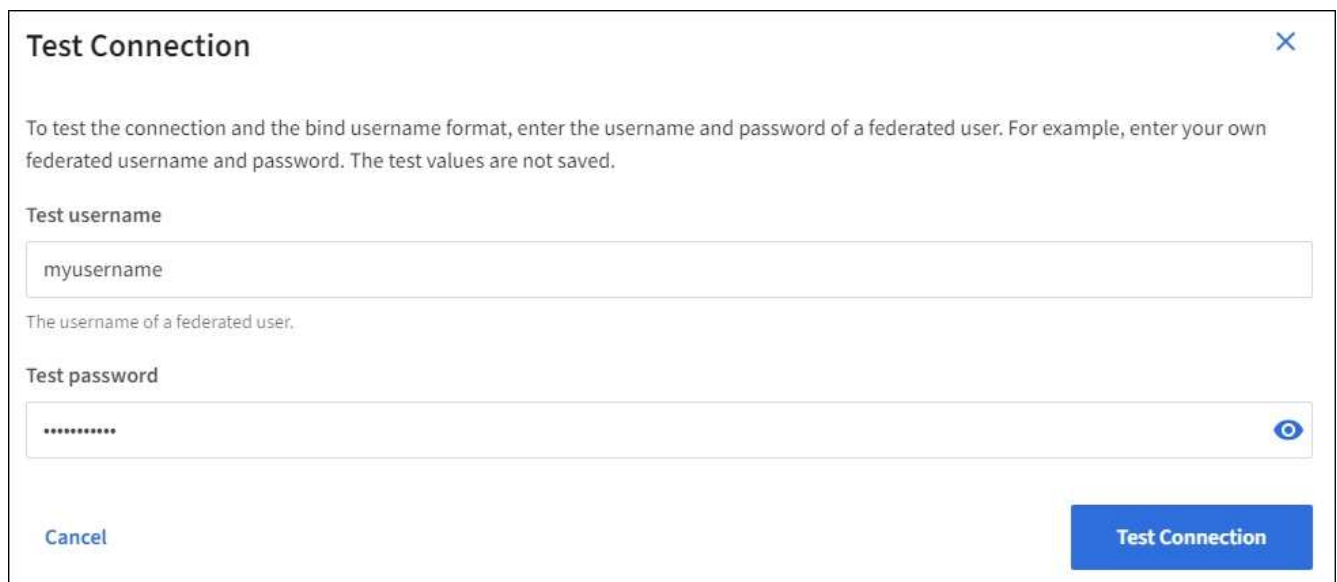
Después de ingresar todos los valores, debe probar la conexión antes de poder guardar la configuración.

StorageGRID verifica la configuración de conexión para el servidor LDAP y el formato de nombre de usuario vinculado, si proporcionó uno.

Pasos

1. Seleccione **Probar conexión**.
2. Si no proporcionó un formato de nombre de usuario vinculado:
 - Aparecerá el mensaje "Conexión de prueba exitosa" si la configuración de conexión es válida. Seleccione **Guardar** para guardar la configuración.
 - Aparece el mensaje "No se pudo establecer la conexión de prueba" si la configuración de conexión no es válida. Seleccione **Cerrar**. Luego, resuelva cualquier problema y pruebe la conexión nuevamente.
3. Si proporcionó un formato de nombre de usuario vinculado, ingrese el nombre de usuario y la contraseña de un usuario federado válido.

Por ejemplo, ingrese su propio nombre de usuario y contraseña. No incluya ningún carácter especial en el nombre de usuario, como @ o /.



- Aparecerá el mensaje "Conexión de prueba exitosa" si la configuración de conexión es válida. Seleccione **Guardar** para guardar la configuración.
- Aparece un mensaje de error si la configuración de conexión, el formato de nombre de usuario vinculado o el nombre de usuario y la contraseña de prueba no son válidos. Resuelva cualquier problema y pruebe la conexión nuevamente.

Forzar la sincronización con la fuente de identidad

El sistema StorageGRID sincroniza periódicamente los grupos y usuarios federados desde la fuente de identidad. Puede forzar el inicio de la sincronización si desea habilitar o restringir los permisos de usuario lo más rápido posible.

Pasos

1. Vaya a la página de federación de identidad.
2. Seleccione **Servidor de sincronización** en la parte superior de la página.

El proceso de sincronización puede tardar algún tiempo dependiendo de su entorno.



La alerta **Error de sincronización de federación de identidad** se activa si hay un problema al sincronizar grupos y usuarios federados desde la fuente de identidad.

Deshabilitar la federación de identidades

Puede deshabilitar temporal o permanentemente la federación de identidad para grupos y usuarios. Cuando la federación de identidad está deshabilitada, no hay comunicación entre StorageGRID y la fuente de identidad. Sin embargo, cualquier configuración que haya realizado se conservará, lo que le permitirá volver a habilitar fácilmente la federación de identidad en el futuro.

Acerca de esta tarea

Antes de deshabilitar la federación de identidad, debe tener en cuenta lo siguiente:

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que actualmente hayan iniciado sesión conservarán el acceso al sistema StorageGRID hasta que su sesión expire, pero no podrán iniciar sesión una vez que expire su sesión.
- No se producirá sincronización entre el sistema StorageGRID y la fuente de identidad, y no se generarán alertas para las cuentas que no se hayan sincronizado.
- La casilla de verificación **Habilitar federación de identidad** está deshabilitada si el inicio de sesión único (SSO) está configurado en **Habilitado** o **Modo Sandbox**. El estado de SSO en la página de inicio de sesión único debe ser **Deshabilitado** antes de poder deshabilitar la federación de identidad. Ver ["Deshabilitar el inicio de sesión único"](#).

Pasos

1. Vaya a la página de federación de identidad.
2. Desmarque la casilla de verificación **Habilitar federación de identidad**.

Directrices para configurar el servidor OpenLDAP

Si desea utilizar un servidor OpenLDAP para la federación de identidad, debe configurar ajustes específicos en el servidor OpenLDAP.



Para las fuentes de identidad que no sean ActiveDirectory o Azure, StorageGRID no bloqueará automáticamente el acceso a S3 a los usuarios que estén deshabilitados externamente. Para bloquear el acceso a S3, elimine todas las claves S3 del usuario o elimine el usuario de todos los grupos.

Superposiciones de miembros y refinaciones

Las superposiciones memberof y refint deben estar habilitadas. Para obtener más información, consulte las instrucciones para el mantenimiento inverso de la membresía del grupo en <http://www.openldap.org/doc/admin24/index.html> ["Documentación de OpenLDAP: Guía del administrador de la versión 2.4"].

Indexación

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 el nombre de usuario estén indexados para un rendimiento óptimo.

Consulte la información sobre el mantenimiento de la membresía del grupo inverso en <http://www.openldap.org/doc/admin24/index.html> ["Documentación de OpenLDAP: Guía del administrador de la versión 2.4"] .

Administrar grupos de inquilinos

Crear grupos para un inquilino de S3

Puede administrar permisos para grupos de usuarios de S3 importando grupos federados o creando grupos locales.

Antes de empezar

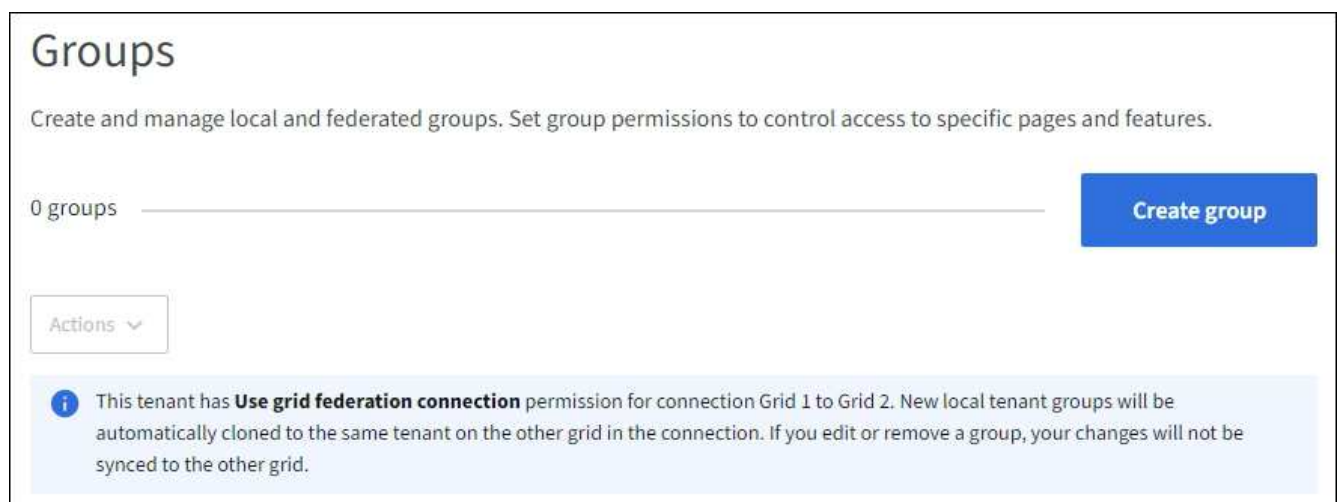
- Ha iniciado sesión en el Administrador de inquilinos mediante un [navegador web compatible](#) .
- Pertenece a un grupo de usuarios que tiene la [Permiso de acceso root](#) .
- Si planea importar un grupo federado, debe [federación de identidad configurada](#) , y el grupo federado ya existe en la fuente de identidad configurada.
- Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, ha revisado el flujo de trabajo y las consideraciones para [Clonación de grupos de inquilinos y usuarios](#) , y ha iniciado sesión en la red de origen del inquilino.

Acceder al asistente para crear grupos

Como primer paso, acceda al asistente para crear grupos.

Pasos

1. Seleccione **GESTIÓN DE ACCESO > Grupos**.
2. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, confirme que aparece un banner azul que indica que los nuevos grupos creados en esta red se clonarán en el mismo inquilino en la otra red de la conexión. Si este banner no aparece, es posible que haya iniciado sesión en la cuadrícula de destino del inquilino.



3. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

Pasos

1. Seleccione la pestaña **Grupo local** para crear un grupo local, o seleccione la pestaña **Grupo federado** para importar un grupo desde la fuente de identidad configurada previamente.

Si el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID , los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Administrador de inquilinos, aunque podrán usar aplicaciones cliente para administrar los recursos del inquilino, según los permisos del grupo.

2. Introduzca el nombre del grupo.

- **Grupo local:** Ingrese un nombre para mostrar y un nombre único. Podrás editar el nombre para mostrar más tarde.



Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, se producirá un error de clonación si ya existe el mismo **Nombre único** para el inquilino en la red de destino.

- **Grupo federado:** Ingrese el nombre único. Para Active Directory, el nombre único es el nombre asociado con el `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con el `uid` atributo.

3. Seleccione **Continuar**.

Administrar permisos de grupo

Los permisos de grupo controlan qué tareas pueden realizar los usuarios en el Administrador de inquilinos y la API de administración de inquilinos.

Pasos

1. Para **Modo de acceso**, seleccione una de las siguientes opciones:

- **Lectura y escritura** (predeterminado): los usuarios pueden iniciar sesión en Tenant Manager y administrar la configuración del inquilino.
- **Solo lectura:** los usuarios solo pueden ver configuraciones y funciones. No pueden realizar ningún cambio ni realizar ninguna operación en el Administrador de inquilinos ni en la API de administración de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.



Si un usuario pertenece a varios grupos y alguno de ellos está configurado como de solo lectura, el usuario tendrá acceso de solo lectura a todas las configuraciones y funciones seleccionadas.

2. Seleccione uno o más permisos para este grupo.

Ver "[Permisos de gestión de inquilinos](#)".

3. Seleccione **Continuar**.

Establecer la política de grupo de S3

La política de grupo determina qué permisos de acceso a S3 tendrán los usuarios.

Pasos

1. Seleccione la política que desea utilizar para este grupo.

Política de grupo	Descripción
Sin acceso a S3	Por defecto. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que se les conceda acceso con una política de bucket. Si selecciona esta opción, solo el usuario root tendrá acceso a los recursos de S3 de forma predeterminada.
Acceso de solo lectura	Los usuarios de este grupo tienen acceso de solo lectura a los recursos de S3. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas. Cuando selecciona esta opción, la cadena JSON para una política de grupo de solo lectura aparece en el cuadro de texto. No puedes editar esta cadena.
Acceso completo	Los usuarios de este grupo tienen acceso completo a los recursos de S3, incluidos los buckets. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puedes editar esta cadena.
Mitigación de ransomware	Esta política de ejemplo se aplica a todos los depósitos de este inquilino. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden eliminar de forma permanente objetos de los depósitos que tienen habilitada la versión de objetos. Los usuarios del administrador de inquilinos que tienen el permiso Administrar todos los depósitos pueden anular esta política de grupo. Limite el permiso Administrar todos los depósitos a usuarios de confianza y utilice la autenticación multifactor (MFA) cuando esté disponible.
Costumbre	A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto.

2. Si seleccionó **Personalizado**, ingrese la política de grupo. Cada política de grupo tiene un límite de tamaño de 5120 bytes. Debe ingresar una cadena con formato JSON válida.

Para obtener información detallada sobre las políticas de grupo, incluida la sintaxis del lenguaje y ejemplos, consulte "[Políticas de grupo de ejemplo](#)".

3. Si está creando un grupo local, seleccione **Continuar**. Si está creando un grupo federado, seleccione **Crear grupo y Finalizar**.

Agregar usuarios (solo grupos locales)

Puede guardar el grupo sin agregar usuarios o, opcionalmente, puede agregar cualquier usuario local que ya

exista.



Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, cualquier usuario que seleccione al crear un grupo local en la red de origen no se incluirá cuando el grupo se clone en la red de destino. Por este motivo, no seleccione usuarios al crear el grupo. En su lugar, seleccione el grupo cuando cree los usuarios.

Pasos

1. Opcionalmente, seleccione uno o más usuarios locales para este grupo.
2. Seleccione **Crear grupo** y **Finalizar**.

El grupo que usted creó aparece en la lista de grupos.

Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red** y usted está en la red de origen del inquilino, el nuevo grupo se clona en la red de destino del inquilino. **Éxito** aparece como **Estado de clonación** en la sección Descripción general de la página de detalles del grupo.

Crear grupos para un inquilino de Swift

Puede administrar los permisos de acceso para una cuenta de inquilino de Swift importando grupos federados o creando grupos locales. Al menos un grupo debe tener el permiso de administrador de Swift, que es necesario para administrar los contenedores y objetos de una cuenta de inquilino de Swift.



La compatibilidad con aplicaciones cliente Swift ha quedado obsoleta y se eliminará en una versión futura.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene la ["Permiso de acceso root"](#).
- Si planea importar un grupo federado, debe ["federación de identidad configurada"](#), y el grupo federado ya existe en la fuente de identidad configurada.

Acceder al asistente para crear grupos

Pasos

Como primer paso, acceda al asistente para crear grupos.

1. Seleccione **GESTIÓN DE ACCESO > Grupos**.
2. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

Pasos

1. Seleccione la pestaña **Grupo local** para crear un grupo local, o seleccione la pestaña **Grupo federado** para importar un grupo desde la fuente de identidad configurada previamente.

Si el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID, los usuarios que

pertenecen a grupos locales no podrán iniciar sesión en el Administrador de inquilinos, aunque podrán usar aplicaciones cliente para administrar los recursos del inquilino, según los permisos del grupo.

2. Introduzca el nombre del grupo.

- **Grupo local:** Ingrese un nombre para mostrar y un nombre único. Podrás editar el nombre para mostrar más tarde.
- **Grupo federado:** Ingrese el nombre único. Para Active Directory, el nombre único es el nombre asociado con el `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con el `uid` atributo.

3. Seleccione **Continuar**.

Administrar permisos de grupo

Los permisos de grupo controlan qué tareas pueden realizar los usuarios en el Administrador de inquilinos y la API de administración de inquilinos.

Pasos

1. Para **Modo de acceso**, seleccione una de las siguientes opciones:

- **Lectura y escritura** (predeterminado): los usuarios pueden iniciar sesión en Tenant Manager y administrar la configuración del inquilino.
- **Solo lectura:** los usuarios solo pueden ver configuraciones y funciones. No pueden realizar ningún cambio ni realizar ninguna operación en el Administrador de inquilinos ni en la API de administración de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.



Si un usuario pertenece a varios grupos y alguno de ellos está configurado como de solo lectura, el usuario tendrá acceso de solo lectura a todas las configuraciones y funciones seleccionadas.

2. Seleccione la casilla de verificación **Acceso raíz** si los usuarios del grupo necesitan iniciar sesión en el Administrador de inquilinos o en la API de administración de inquilinos.

3. Seleccione **Continuar**.

Establecer la política de grupo de Swift

Los usuarios de Swift necesitan permiso de administrador para autenticarse en la API REST de Swift para crear contenedores e ingerir objetos.

1. Seleccione la casilla de verificación **Administrador de Swift** si los usuarios del grupo necesitan usar la API REST de Swift para administrar contenedores y objetos.
2. Si está creando un grupo local, seleccione **Continuar**. Si está creando un grupo federado, seleccione **Crear grupo y Finalizar**.

Agregar usuarios (solo grupos locales)

Puede guardar el grupo sin agregar usuarios o, opcionalmente, puede agregar cualquier usuario local que ya exista.

Pasos

1. Opcionalmente, seleccione uno o más usuarios locales para este grupo.

Si aún no ha creado usuarios locales, puede agregar este grupo al usuario en la página Usuarios. Ver ["Administrar usuarios locales"](#) .

2. Seleccione **Crear grupo** y **Finalizar**.

El grupo que usted creó aparece en la lista de grupos.

Permisos de gestión de inquilinos

Antes de crear un grupo de inquilinos, considere qué permisos desea asignar a ese grupo. Los permisos de administración de inquilinos determinan qué tareas pueden realizar los usuarios mediante el Administrador de inquilinos o la API de administración 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 inquilinos o utilizar la API de administración de inquilinos, los usuarios deben pertenecer a un grupo que tenga al menos un permiso. Todos los usuarios que puedan iniciar sesión podrán realizar las siguientes tareas:

- Ver el panel de control
- 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 configuraciones y realizar operaciones o si solo pueden ver las configuraciones y funciones relacionadas.



Si un usuario pertenece a varios grupos y alguno de ellos está configurado como de solo lectura, el usuario tendrá acceso de solo lectura a todas las configuraciones y funciones seleccionadas.

Puede asignar los siguientes permisos a un grupo. Tenga en cuenta que los inquilinos de S3 y los inquilinos de Swift tienen diferentes permisos de grupo.

Permiso	Descripción	Detalles
Acceso root	Proporciona acceso completo al Administrador de inquilinos y a la API de administración de inquilinos.	Los usuarios de Swift deben tener permiso de acceso de root para iniciar sesión en la cuenta del inquilino.
Administrador	Solo inquilinos rápidos. Proporciona acceso completo a los contenedores y objetos Swift para esta cuenta de inquilino	Los usuarios de Swift deben tener permiso de administrador de Swift para realizar cualquier operación con la API REST de Swift.
Administre sus propias credenciales 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 ALMACENAMIENTO (S3) > Mis claves de acceso S3 .

Permiso	Descripción	Detalles
Ver todos los buckets	Inquilinos de S3: permite a los usuarios ver todos los depósitos y sus configuraciones. Inquilinos de Swift: permite a los usuarios de Swift ver todos los contenedores y configuraciones de contenedores mediante la API de administración de inquilinos.	Los usuarios que no tienen el permiso Ver todos los depósitos o Administrar todos los depósitos no ven la opción de menú Cubos. Este permiso es reemplazado por el permiso Administrar todos los depósitos. No afecta las políticas de grupo o bucket S3 utilizadas por los clientes S3 o la consola S3. Solo puede asignar este permiso a grupos Swift desde la API de administración de inquilinos. No puedes asignar este permiso a grupos Swift mediante el Administrador de inquilinos.
Administrar todos los depósitos	Inquilinos de S3: permite a los usuarios usar el Administrador de inquilinos y la API de administración de inquilinos para crear y eliminar depósitos S3 y administrar las configuraciones de todos los depósitos S3 en la cuenta del inquilino, independientemente de las políticas de grupo o depósito S3. Inquilinos de Swift: permite a los usuarios de Swift controlar la consistencia de los contenedores de Swift mediante la API de administración de inquilinos.	Los usuarios que no tienen el permiso Ver todos los depósitos o Administrar todos los depósitos no ven la opción de menú Cubos. Este permiso reemplaza al permiso Ver todos los depósitos. No afecta las políticas de grupo o bucket S3 utilizadas por los clientes S3 o la consola S3. Solo puede asignar este permiso a grupos Swift desde la API de administración de inquilinos. No puedes asignar este permiso a grupos Swift mediante el Administrador de inquilinos.
Administrar puntos finales	Permite a los usuarios utilizar el Administrador de inquilinos o la API de administración de inquilinos para crear o editar puntos finales de servicio de la plataforma, que se utilizan como destino para los servicios de la plataforma StorageGRID .	Los usuarios que no tienen este permiso no ven la opción de menú Puntos finales de servicios de la plataforma .
Usar la pestaña Consola S3	Cuando se combina con el permiso Ver todos los depósitos o Administrar todos los depósitos, permite a los usuarios ver y administrar objetos desde la pestaña de la Consola S3 en la página de detalles de un depósito.	

Administrar grupos

Administre sus grupos de inquilinos según sea necesario para ver, editar o duplicar un grupo y más.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#) .
- Pertenece a un grupo de usuarios que tiene la ["Permiso de acceso root"](#) .

Ver o editar grupo

Puede ver y editar la información básica y los detalles de cada grupo.

Pasos

1. Seleccione **GESTIÓN DE ACCESO > Grupos**.
2. Revise la información proporcionada en la página Grupos, que enumera información básica de todos los grupos locales y federados para esta cuenta de inquilino.

Si la cuenta del inquilino tiene el permiso **Usar conexión de federación de red** y está viendo grupos en la red de origen del inquilino:

- Un mensaje de banner indica que si edita o elimina un grupo, sus cambios no se sincronizarán con la otra cuadrícula.
- Según sea necesario, un mensaje de banner indica si los grupos no se clonaron en el inquilino en la red de destino. Puede [reintentar una clonación de grupo](#) Eso falló.

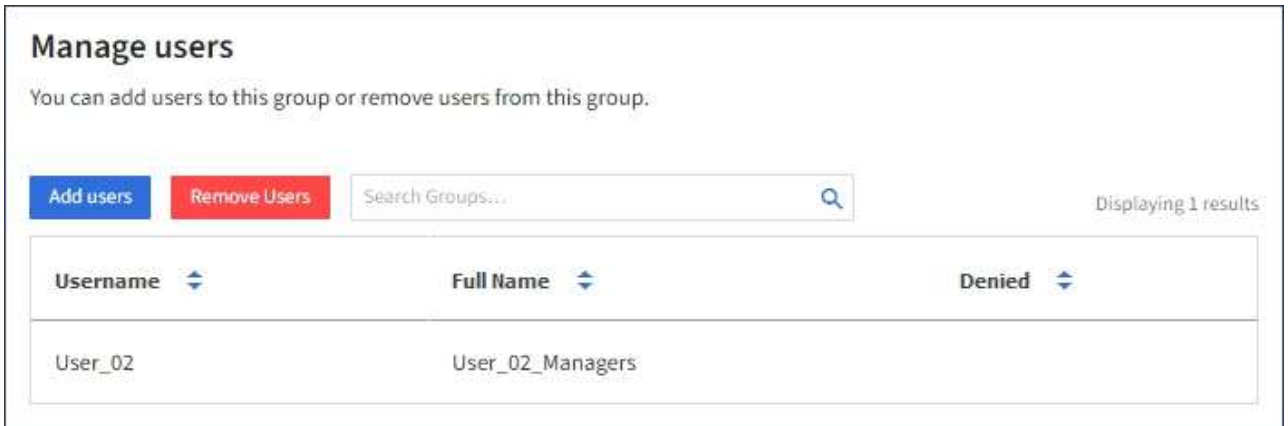
3. Si desea cambiar el nombre del grupo:
 - a. Seleccione la casilla de verificación del grupo.
 - b. Seleccione **Acciones > Editar nombre del grupo**.
 - c. Introduzca el nuevo nombre.
 - d. Seleccione **Guardar cambios**.
4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
 - Seleccione el nombre del grupo.
 - Seleccione la casilla de verificación del grupo y seleccione **Acciones > Ver detalles del grupo**.
5. Revise la sección Descripción general, que muestra la siguiente información para cada grupo:
 - Nombre para mostrar
 - Nombre único
 - Tipo
 - Modo de acceso
 - Permisos
 - Política S3
 - Número de usuarios en este grupo
 - Campos adicionales si la cuenta del inquilino tiene el permiso **Usar conexión de federación de red** y está viendo el grupo en la red de origen del inquilino:
 - Estado de clonación: **Éxito** o **Fracaso**
 - Un banner azul que indica que si edita o elimina este grupo, sus cambios no se sincronizarán con la otra cuadrícula.
6. Edite la configuración del grupo según sea necesario. Ver ["Crear grupos para un inquilino de S3"](#) y ["Crear grupos para un inquilino de Swift"](#) para obtener detalles sobre qué ingresar.
 - a. En la sección Descripción general, cambie el nombre para mostrar seleccionando el nombre o el ícono

de edición .

- b. En la pestaña **Permisos de grupo**, actualice los permisos y seleccione **Guardar cambios**.
- c. En la pestaña **Política de grupo**, realice los cambios necesarios y seleccione **Guardar cambios**.
 - Si está editando un grupo S3, opcionalmente seleccione una política de grupo S3 diferente o ingrese la cadena JSON para una política personalizada, según sea necesario.
 - Si está editando un grupo Swift, opcionalmente seleccione o desmarque la casilla de verificación **Administrador Swift**.

7. Para agregar uno o más usuarios locales existentes al grupo:

- a. Seleccione la pestaña Usuarios.



Manage users

You can add users to this group or remove users from this group.

Add users **Remove Users** Search Groups... Displaying 1 results

Username	Full Name	Denied
User_02	User_02_Managers	

- b. Seleccione **Agregar usuarios**.
- c. Seleccione los usuarios existentes que desea agregar y seleccione **Agregar usuarios**.

Aparece un mensaje de éxito en la parte superior derecha.

8. Para eliminar usuarios locales del grupo:

- a. Seleccione la pestaña Usuarios.
- b. Seleccione **Eliminar usuarios**.
- c. Seleccione los usuarios que desea eliminar y seleccione **Eliminar usuarios**.

Aparece un mensaje de éxito en la parte superior derecha.

9. Confirme que ha seleccionado **Guardar cambios** para cada sección que haya modificado.

Grupo duplicado

Puede duplicar un grupo existente para crear nuevos grupos más rápidamente.



Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red** y duplica un grupo de la red de origen del inquilino, el grupo duplicado se clonará en la red de destino del inquilino.

Pasos

1. Seleccione **GESTIÓN DE ACCESO > Grupos**.
2. Seleccione la casilla de verificación del grupo que desea duplicar.

3. Seleccione **Acciones** > **Duplicar grupo**.
4. Ver "[Crear grupos para un inquilino de S3](#)" o "[Crear grupos para un inquilino de Swift](#)" para obtener detalles sobre qué ingresar.
5. Seleccione **Crear grupo**.

[[grupos de clones]]Reintentar clonar grupo

Para volver a intentar una clonación que falló:

1. Seleccione cada grupo que indique (*Clonación fallida*) debajo del nombre del grupo.
2. Seleccione **Acciones** > **Clonar grupos**.
3. Vea el estado de la operación de clonación desde la página de detalles de cada grupo que esté clonando.

Para obtener información adicional, consulte "[Clonar grupos de inquilinos y usuarios](#)".

Eliminar uno o más grupos

Puedes eliminar uno o más grupos. Cualquier usuario que pertenezca únicamente a un grupo eliminado ya no podrá iniciar sesión en el Administrador de inquilinos ni usar la cuenta de inquilino.



Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red** y elimina un grupo, StorageGRID no eliminará el grupo correspondiente en la otra red. Si necesita mantener esta información sincronizada, debe eliminar el mismo grupo de ambas cuadrículas.

Pasos

1. Seleccione **GESTIÓN DE ACCESO** > **Grupos**.
2. Seleccione la casilla de verificación para cada grupo que desee eliminar.
3. Seleccione **Acciones** > **Eliminar grupo** o **Acciones** > **Eliminar grupos**.

Aparece un cuadro de diálogo de confirmación.

4. Seleccione **Eliminar grupo** o **Eliminar grupos**.

Administrar usuarios locales

Puede crear usuarios locales y asignarlos a grupos locales para determinar a qué funciones pueden acceder estos usuarios. El administrador de inquilinos incluye un usuario local predefinido, llamado "root". Aunque puedes agregar y eliminar usuarios locales, no puedes eliminar el usuario root.



Si el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID, los usuarios locales no podrán iniciar sesión en el Administrador de inquilinos ni en la API de administración de inquilinos, aunque podrán usar aplicaciones cliente para acceder a los recursos del inquilino, según los permisos del grupo.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un "[navegador web compatible](#)".
- Pertenece a un grupo de usuarios que tiene la "[Permiso de acceso root](#)".

- Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, ha revisado el flujo de trabajo y las consideraciones para "[Clonación de grupos de inquilinos y usuarios](#)", y ha iniciado sesión en la red de origen del inquilino.

Crear un usuario local

Puede crear un usuario local y asignarlo a uno o más grupos locales para controlar sus permisos de acceso.

Los usuarios de S3 que no pertenecen a ningún grupo no tienen permisos de administración ni políticas de grupo de S3 aplicadas a ellos. A estos usuarios se les podría otorgar acceso al bucket S3 a través de una política de bucket.

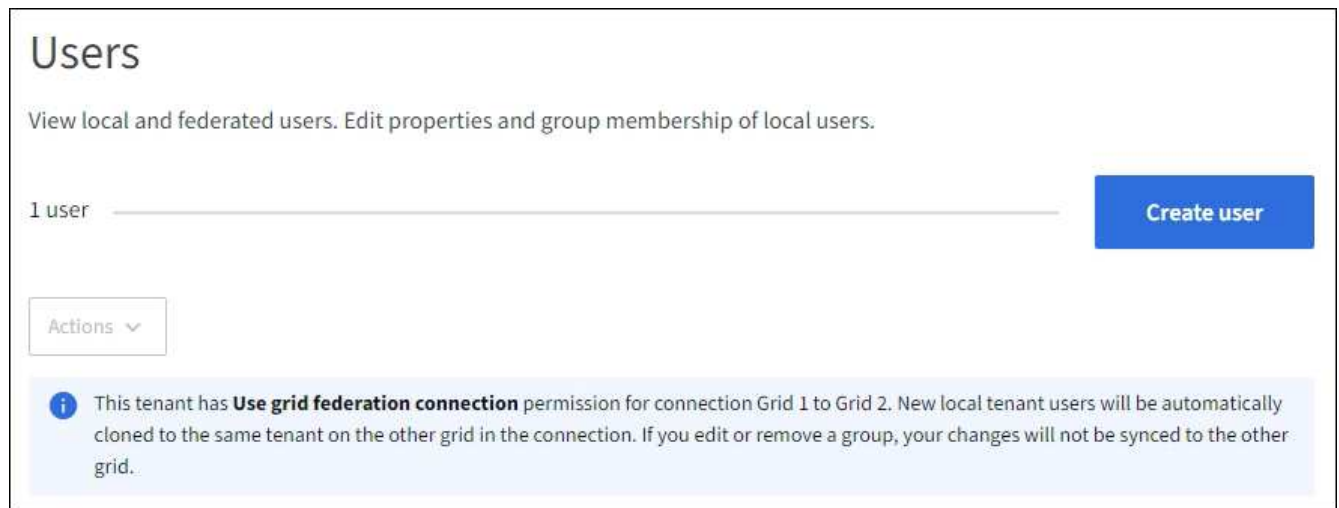
Los usuarios de Swift que no pertenecen a ningún grupo no tienen permisos de administración ni acceso al contenedor Swift.

Acceder al asistente para crear usuarios

Pasos

1. Seleccione **GESTIÓN DE ACCESO > Usuarios**.

Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, un banner azul indica que esta es la red de origen del inquilino. Cualquier usuario local que cree en esta red se clonará en la otra red de la conexión.



2. Seleccione **Crear usuario**.

Ingresar credenciales

Pasos

1. Para el paso **Ingresar credenciales de usuario**, complete los siguientes campos.

Campo	Descripción
Nombre completo	El nombre completo de este usuario, por ejemplo, el nombre y apellido de una persona o el nombre de una aplicación.

Campo	Descripción
Nombre de usuario	El nombre que este usuario usará para iniciar sesión. Los nombres de usuario deben ser únicos y no se pueden cambiar. Nota: Si su cuenta de inquilino tiene el permiso Usar conexión de federación de red, se producirá un error de clonación si ya existe el mismo Nombre de usuario para el inquilino en la red de destino.
Contraseña y Confirmar contraseña	La contraseña que el usuario utilizará inicialmente al iniciar sesión.
Denegar el acceso	Seleccione Sí para evitar que este usuario inicie sesión en la cuenta de inquilino, incluso si aún pertenece a uno o más grupos. Por ejemplo, seleccione Sí para suspender temporalmente la capacidad de un usuario de iniciar sesión.

2. Seleccione **Continuar**.

Asignar a grupos

Pasos

1. Asigne el usuario a uno o más grupos locales para determinar qué tareas puede realizar.

La asignación de un usuario a grupos es opcional. Si lo prefiere, puede seleccionar usuarios al crear o editar grupos.

Los usuarios que no 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 pertenecen. Ver ["Permisos de gestión de inquilinos"](#).

2. Seleccione **Crear usuario**.

Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red** y usted está en la red de origen del inquilino, el nuevo usuario local se clona en la red de destino del inquilino. **Éxito** aparece como **Estado de clonación** en la sección Descripción general de la página de detalles del usuario.

3. Seleccione **Finalizar** para regresar a la página Usuarios.

Ver o editar usuario local

Pasos

1. Seleccione **GESTIÓN DE ACCESO > Usuarios**.
2. Revise la información proporcionada en la página Usuarios, que enumera información básica de todos los usuarios locales y federados para esta cuenta de inquilino.

Si la cuenta del inquilino tiene el permiso **Usar conexión de federación de red** y está viendo al usuario en la red de origen del inquilino:

- Un mensaje de banner indica que si edita o elimina un usuario, sus cambios no se sincronizarán con la otra cuadrícula.

- Según sea necesario, un mensaje de banner indica si los usuarios no fueron clonados al inquilino en la red de destino. Puede [Reintentar una clonación de usuario que falló](#) Es
3. Si desea cambiar el nombre completo del usuario:
 - a. Seleccione la casilla de verificación para el usuario.
 - b. Seleccione **Acciones > Editar nombre completo**.
 - c. Introduzca el nuevo nombre.
 - d. Seleccione **Guardar cambios**.
 4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
 - Seleccione el nombre de usuario.
 - Seleccione la casilla de verificación del usuario y seleccione **Acciones > Ver detalles del usuario**.
 5. Revise la sección Descripción general, que muestra la siguiente información para cada usuario:
 - Nombre completo
 - Nombre de usuario
 - Tipo de usuario
 - Acceso denegado
 - Modo de acceso
 - Membresía grupal
 - Campos adicionales si la cuenta del inquilino tiene el permiso **Usar conexión de federación de red** y está viendo al usuario en la red de origen del inquilino:
 - Estado de clonación: **Éxito** o **Fracaso**
 - Un banner azul que indica que si edita este usuario, sus cambios no se sincronizarán con la otra cuadrícula.
 6. Edite la configuración del usuario según sea necesario. Ver [Crear usuario local](#) para obtener detalles sobre qué ingresar.
 - a. En la sección Descripción general, cambie el nombre completo seleccionando el nombre o el ícono de edición  .

No puedes cambiar el nombre de usuario.
 - b. En la pestaña **Contraseña**, cambie la contraseña del usuario y seleccione **Guardar cambios**.
 - c. En la pestaña **Acceso**, seleccione **No** para permitir que el usuario inicie sesión o seleccione **Sí** para evitar que el usuario inicie sesión. Luego, seleccione **Guardar cambios**.
 - d. En la pestaña **Teclas de acceso**, seleccione **Crear clave** y siga las instrucciones para ["creando las claves de acceso S3 de otro usuario"](#) .
 - e. En la pestaña **Grupos**, seleccione **Editar grupos** para agregar el usuario a grupos o eliminarlo de grupos. Luego, seleccione **Guardar cambios**.
 7. Confirme que ha seleccionado **Guardar cambios** para cada sección que haya modificado.

Usuario local duplicado

Puede duplicar un usuario local para crear un nuevo usuario más rápidamente.



Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red** y duplica un usuario de la red de origen del inquilino, el usuario duplicado se clonará en la red de destino del inquilino.

Pasos

1. Seleccione **GESTIÓN DE ACCESO > Usuarios**.
2. Seleccione la casilla de verificación del usuario que desea duplicar.
3. Seleccione **Acciones > Duplicar usuario**.
4. Ver [Crear usuario local](#) para obtener detalles sobre qué ingresar.
5. Seleccione **Crear usuario**.

Reintentar clonar usuario

Para volver a intentar una clonación que falló:

1. Seleccione cada usuario que indique (*Clonación fallida*) debajo del nombre de usuario.
2. Seleccione **Acciones > Clonar usuarios**.
3. Vea el estado de la operación de clonación desde la página de detalles de cada usuario que esté clonando.

Para obtener información adicional, consulte ["Clonar grupos de inquilinos y usuarios"](#) .

Eliminar uno o más usuarios locales

Puede eliminar de forma permanente uno o más usuarios locales que ya no necesiten acceder a la cuenta de inquilino de StorageGRID .



Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red** y elimina un usuario local, StorageGRID no eliminará el usuario correspondiente en la otra red. Si necesita mantener esta información sincronizada, debe eliminar el mismo usuario de ambas cuadrículas.



Debe utilizar la fuente de identidad federada para eliminar usuarios federados.

Pasos

1. Seleccione **GESTIÓN DE ACCESO > Usuarios**.
2. Seleccione la casilla de verificación para cada usuario que desee eliminar.
3. Seleccione **Acciones > Eliminar usuario** o **Acciones > Eliminar usuarios**.

Aparece un cuadro de diálogo de confirmación.

4. Seleccione **Eliminar usuario** o **Eliminar usuarios**.

Administrar claves de acceso S3

Administrar claves de acceso S3

Cada usuario de una cuenta de inquilino S3 debe tener una clave de acceso para almacenar y recuperar objetos en el sistema StorageGRID . Una clave de acceso consta

de un ID de clave de acceso y una clave de acceso secreta.

Las claves de acceso S3 se pueden gestionar de la siguiente manera:

- Los usuarios que tienen el permiso **Administrar sus propias credenciales S3** pueden crear o eliminar sus propias claves de acceso S3.
- Los usuarios que tienen permiso de **acceso root** pueden administrar las claves de acceso para la cuenta raíz S3 y todos los demás usuarios. Las claves de acceso raíz brindan acceso completo a todos los depósitos y objetos para el inquilino, a menos que una política de depósito los deshabilite explícitamente.

StorageGRID admite la autenticación Signature Version 2 y Signature Version 4. No se permite el acceso entre cuentas a menos que lo habilite explícitamente una política de bucket.

Crea tus propias claves de acceso S3

Si está utilizando un inquilino S3 y tiene el permiso adecuado, puede crear sus propias claves de acceso S3. Debe tener una clave de acceso para acceder a sus depósitos y objetos.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene la ["Administre sus propias credenciales S3 o permiso de acceso root"](#).

Acerca de esta tarea

Puede crear una o más claves de acceso S3 que le permitan crear y administrar depósitos para su cuenta de inquilino. Después de crear una nueva clave de acceso, actualice la aplicación con su nueva ID de clave de acceso y su clave de acceso secreta. Por seguridad, no cree más claves de las que necesita y elimine las claves que no esté utilizando. Si solo tiene una clave y está a punto de caducar, cree una nueva clave antes de que caduque la anterior y luego elimínela.

Cada clave puede tener un tiempo de expiración específico o no tener expiración. Siga estas pautas para el tiempo de vencimiento:

- Establezca un tiempo de vencimiento para sus claves para limitar su acceso a un período de tiempo determinado. Establecer un tiempo de vencimiento corto puede ayudar a reducir el riesgo si su ID de clave de acceso y su clave de acceso secreta se exponen accidentalmente. Las claves caducadas se eliminan automáticamente.
- Si el riesgo de seguridad en su entorno es bajo y no necesita crear nuevas claves periódicamente, no es necesario establecer un tiempo de vencimiento para sus claves. Si más adelante decide crear nuevas claves, elimine las claves antiguas manualmente.



Se puede acceder a los depósitos y objetos S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de su cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ALMACENAMIENTO (S3) > Mis claves de acceso**.

Aparece la página Mis claves de acceso y enumera todas las claves de acceso existentes.

2. Seleccione **Crear clave**.

3. Debe realizar una de las siguientes acciones:

- Seleccione **No establecer un tiempo de expiración** para crear una clave que no caduque. (Por defecto)
- Seleccione **Establecer una hora de vencimiento** y configure la fecha y hora de vencimiento.



La fecha de vencimiento puede ser de un máximo de cinco años a partir de la fecha actual. El tiempo de expiración puede ser de un mínimo de un minuto a partir de la hora actual.

4. Seleccione **Crear clave de acceso**.

Aparece el cuadro de diálogo Descargar clave de acceso, que incluye el ID de su clave de acceso y su 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 la clave de acceso y la clave de acceso secreta.



No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información. No es posible copiar ni descargar claves una vez cerrado el cuadro de diálogo.

6. Seleccione **Finalizar**.

La nueva clave aparece en la página Mis claves de acceso.

7. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, utilice opcionalmente la API de administración de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en la red de origen al inquilino en la red de destino. Ver "[Clonar claves de acceso S3 usando la API](#)".

Ver sus claves de acceso S3

Si está utilizando un inquilino S3 y tiene la "[permiso apropiado](#)", puede ver una lista de sus claves de acceso S3. Puede ordenar la lista por tiempo de expiración, para poder determinar qué claves expirarán pronto. Según sea necesario, puede "[crear nuevas claves](#)" o "[borrar teclas](#)" que ya no estas usando.



Se puede acceder a los depósitos y objetos S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de su cuenta y nunca las comparta con otros usuarios.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un "[navegador web compatible](#)".
- Pertenece a un grupo de usuarios que tiene la opción Administrar sus propias credenciales de S3 "[permiso](#)".

Pasos

1. Seleccione **ALMACENAMIENTO (S3) > Mis claves de acceso**.

2. Desde la página Mis claves de acceso, ordene las claves de acceso existentes por **Tiempo de vencimiento** o **ID de clave de acceso**.
3. Según sea necesario, cree nuevas claves o elimine aquellas que ya no utilice.

Si crea nuevas claves antes de que caduquen las claves existentes, puede comenzar a usar las nuevas claves sin perder temporalmente el acceso a los objetos de la cuenta.

Las claves caducadas se eliminan automáticamente.

Eliminar sus propias claves de acceso S3

Si está utilizando un inquilino S3 y tiene el permiso adecuado, puede eliminar sus propias claves de acceso S3. Una vez que se elimina una clave de acceso, ya no se puede usar para acceder a los objetos y depósitos en la cuenta del inquilino.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Tú tienes el ["Administrar sus propios permisos de credenciales S3"](#).



Se puede acceder a los depósitos y objetos S3 que pertenecen a su cuenta mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para su cuenta en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de su cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **ALMACENAMIENTO (S3) > Mis claves de acceso**.
2. Desde la página Mis teclas de acceso, seleccione la casilla de verificación de cada tecla de acceso que desee eliminar.
3. Seleccione **Tecla Eliminar**.
4. Desde el cuadro de diálogo de confirmación, seleccione **Eliminar tecla**.

Aparece un mensaje de confirmación en la esquina superior derecha de la página.

Crear las claves de acceso S3 de otro usuario

Si utiliza un inquilino S3 y tiene el permiso adecuado, puede crear claves de acceso S3 para otros usuarios, como aplicaciones que necesitan acceso a depósitos y objetos.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene la ["Permiso de acceso root"](#).

Acerca de esta tarea

Puede crear una o más claves de acceso S3 para otros usuarios para que puedan crear y administrar depósitos para su cuenta de inquilino. Después de crear una nueva clave de acceso, actualice la aplicación con la nueva ID de clave de acceso y la clave de acceso secreta. Por seguridad, no cree más claves de las que necesita el usuario y elimine las claves que no se estén utilizando. Si solo tiene una clave y está a punto

de caducar, cree una nueva clave antes de que caduque la anterior y luego elimínela.

Cada clave puede tener un tiempo de expiración específico o no tener expiración. Siga estas pautas para el tiempo de vencimiento:

- Establezca un tiempo de expiración para las claves para limitar el acceso del usuario a un período de tiempo determinado. Establecer un tiempo de vencimiento corto puede ayudar a reducir el riesgo si el ID de la clave de acceso y la clave de acceso secreta se exponen accidentalmente. Las claves caducadas se eliminan automáticamente.
- Si el riesgo de seguridad en su entorno es bajo y no necesita crear nuevas claves periódicamente, no es necesario establecer un tiempo de vencimiento para las claves. Si más adelante decide crear nuevas claves, elimine las claves antiguas manualmente.



Se puede acceder a los depósitos y objetos S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **GESTIÓN DE ACCESO > Usuarios**.
2. Seleccione el usuario cuyas claves de acceso S3 desea administrar.

Aparece la página de detalles del usuario.

3. Seleccione **Teclas de acceso** y luego seleccione **Crear clave**.
4. Debe realizar una de las siguientes acciones:
 - Seleccione **No establecer un tiempo de expiración** para crear una clave que no expire. (Por defecto)
 - Seleccione **Establecer una hora de vencimiento** y configure la fecha y hora de vencimiento.



La fecha de vencimiento puede ser de un máximo de cinco años a partir de la fecha actual. El tiempo de expiración puede ser de un mínimo de un minuto a partir de la hora actual.

5. Seleccione **Crear clave de acceso**.

Aparece el cuadro de diálogo Descargar clave de acceso, que enumera el ID de la 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 la clave de acceso y la clave de acceso secreta.



No cierre este cuadro de diálogo hasta que haya copiado o descargado esta información. No es posible copiar ni descargar claves una vez cerrado el cuadro de diálogo.

7. Seleccione **Finalizar**.

La nueva clave aparece en la pestaña Teclas de acceso de la página de detalles del usuario.

8. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de red**, utilice opcionalmente la

API de administración de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en la red de origen al inquilino en la red de destino. Ver ["Clonar claves de acceso S3 usando la API"](#) .

Ver las claves de acceso S3 de otro usuario

Si está utilizando un inquilino S3 y tiene los permisos adecuados, puede ver las claves de acceso S3 de otro usuario. Puede ordenar la lista por tiempo de vencimiento para poder determinar qué claves caducarán pronto. Según sea necesario, puede crear nuevas claves y eliminar claves que ya no se utilizan.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .



Se puede acceder a los depósitos y objetos S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **GESTIÓN DE ACCESO > Usuarios**.
2. Desde la página Usuarios, seleccione el usuario cuyas claves de acceso S3 desea ver.
3. Desde la página de detalles del usuario, seleccione **Teclas de acceso**.
4. Ordene las claves por **Tiempo de expiración** o **ID de clave de acceso**.
5. Según sea necesario, cree nuevas claves y elimine manualmente las claves que ya no se utilizan.

Si crea nuevas claves antes de que caduquen las claves existentes, el usuario puede comenzar a usar las nuevas claves sin perder temporalmente el acceso a los objetos de la cuenta.

Las claves caducadas se eliminan automáticamente.

Información relacionada

- ["Crear las claves de acceso S3 de otro usuario"](#)
- ["Eliminar las claves de acceso S3 de otro usuario"](#)

Eliminar las claves de acceso S3 de otro usuario

Si está utilizando un inquilino S3 y tiene los permisos adecuados, puede eliminar las claves de acceso S3 de otro usuario. Una vez que se elimina una clave de acceso, ya no se puede usar para acceder a los objetos y depósitos en la cuenta del inquilino.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .



Se puede acceder a los depósitos y objetos S3 que pertenecen a un usuario mediante el ID de clave de acceso y la clave de acceso secreta que se muestran para ese usuario en el Administrador de inquilinos. Por este motivo, proteja las claves de acceso como lo haría con una contraseña. Rote las claves de acceso periódicamente, elimine las claves no utilizadas de la cuenta y nunca las comparta con otros usuarios.

Pasos

1. Seleccione **GESTIÓN DE ACCESO > Usuarios**.
2. Desde la página Usuarios, seleccione el usuario cuyas claves de acceso S3 desea administrar.
3. Desde la página de detalles del usuario, seleccione **Teclas de acceso** y luego seleccione la casilla de verificación para cada tecla de acceso que desee eliminar.
4. Seleccione **Acciones > Eliminar clave seleccionada**.
5. Desde el cuadro de diálogo de confirmación, seleccione **Eliminar tecla**.

Aparece un mensaje de confirmación en la esquina superior derecha de la página.

Administrar depósitos S3

Crear un bucket S3

Puede utilizar el Administrador de inquilinos para crear depósitos S3 para datos de objetos.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene acceso de root o administra todos los buckets ["permiso"](#). Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.



Los permisos para establecer o modificar las propiedades de bloqueo de objetos S3 de depósitos u objetos se pueden otorgar mediante ["política de cubos o política de grupo"](#).

- Si planea habilitar el Bloqueo de objetos S3 para un depósito, un administrador de la red ha habilitado la configuración global de Bloqueo de objetos S3 para el sistema StorageGRID y usted ha revisado los requisitos para los depósitos y objetos de Bloqueo de objetos S3.
- Si cada inquilino tendrá 5000 depósitos, cada nodo de almacenamiento en la red tendrá un mínimo de 64 GB de RAM.



Cada cuadrícula puede tener un máximo de 100.000 contenedores.

Acceder al asistente

Pasos

1. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.
2. Seleccione **Crear depósito**.

Introducir detalles

Pasos

1. Introduzca detalles para el depósito.

Campo	Descripción
Nombre del depósito	Un nombre para el depósito que cumple con estas reglas: • Debe ser único en cada sistema StorageGRID (no solo único dentro de la cuenta del inquilino). • Debe ser compatible con DNS. • Debe contener 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 contener puntos en las solicitudes de estilo alojado virtualmente. Los períodos causarán problemas con la verificación del certificado comodín del servidor. Para obtener más información, consulte la "Documentación de Amazon Web Services (AWS) sobre las reglas de nombres de bucket". Nota: No puedes cambiar el nombre del depósito después de crearlo.
Región	La región del cubo. Su administrador de StorageGRID administra las regiones disponibles. La región de un depósito puede afectar la política de protección de datos aplicada a los objetos. De forma predeterminada, todos los depósitos se crean en el <code>us-east-1</code> región. Nota: No puedes cambiar la región después de crear el depósito.

2. Seleccione **Continuar**.

Administrar configuraciones

Pasos

1. De manera opcional, habilite el control de versiones de objetos para el depósito.

Habilite el control de versiones de objetos si desea almacenar todas las versiones de cada objeto en este depósito. Luego puede recuperar versiones anteriores de un objeto según sea necesario. Debe habilitar el control de versiones de objetos si el depósito se utilizará para la replicación entre redes.

2. Si la configuración global de Bloqueo de objetos S3 está habilitada, habilite opcionalmente el Bloqueo de objetos S3 para que el depósito almacene objetos utilizando un modelo de escritura única, lectura múltiple (WORM).

Habilite el bloqueo de objetos S3 para un depósito solo si necesita conservar objetos durante un período de tiempo fijo, por ejemplo, para cumplir con ciertos requisitos reglamentarios. El bloqueo de objetos S3 es una configuración permanente que le ayuda a evitar que los objetos se eliminen o sobrescriban durante un período de tiempo fijo o de manera indefinida.



Una vez habilitada la configuración de bloqueo de objetos S3 para un depósito, no se puede deshabilitar. Cualquier persona con los permisos correctos puede agregar objetos a este depósito que no se pueden modificar. Es posible que no puedas eliminar estos objetos ni el depósito en sí.

Si habilita el Bloqueo de objetos S3 para un depósito, el control de versiones del depósito se habilita automáticamente.

3. Si seleccionó **Habilitar bloqueo de objetos S3**, habilite opcionalmente la **Retención predeterminada** para este depósito.



Su administrador de red debe darle permiso para "[Utilice funciones específicas de S3 Object Lock](#)".

Cuando la **Retención predeterminada** está habilitada, los objetos nuevos agregados al depósito estarán automáticamente protegidos contra eliminación o sobrescritura. La configuración **Retención predeterminada** no se aplica a los objetos que tienen sus propios períodos de retención.

- a. Si la **Retención predeterminada** está habilitada, especifique un **Modo de retención predeterminado** para el depósito.

Modo de retención predeterminado	Descripción
Gobernancia	• Usuarios con la <code>s3:BypassGovernanceRetention</code> El permiso puede utilizar el <code>x-amz-bypass-governance-retention: true</code> encabezado de solicitud para omitir la configuración de retención. • Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su fecha de conservación. • Estos usuarios pueden aumentar, disminuir o eliminar la fecha de conservación de un objeto.
Cumplimiento	• El objeto no se puede eliminar hasta que se alcance su fecha de conservación. • La fecha de conservación del objeto se puede aumentar, pero no se puede disminuir. • La fecha de retención del objeto no se puede eliminar hasta que se alcance esa fecha. Nota: El administrador de su red debe permitirle utilizar el modo de cumplimiento.

- b. Si la **Retención predeterminada** está habilitada, especifique el **Período de retención predeterminado** para el depósito.

El **Período de retención predeterminado** indica durante cuánto tiempo se deben conservar los objetos nuevos agregados a este depósito, a partir del momento en que se ingieren. Especifique un valor que sea menor o igual al período de retención máximo para el inquilino, según lo establecido por el administrador de la red.

Se establece un período de retención *máximo*, que puede tener un valor de entre 1 día y 100 años, cuando el administrador de la red crea el inquilino. Cuando se establece un período de retención *predeterminado*, no puede exceder el valor establecido para el período de retención máximo. Si es necesario, solicite al administrador de su red que aumente o disminuya el período máximo de retención.

4. Opcionalmente, seleccione **Habilitar límite de capacidad**.

El límite de capacidad es la capacidad máxima disponible para los objetos de este bucket. Este valor representa una cantidad lógica (tamaño del objeto), no una cantidad física (tamaño en disco).

Si no se establece ningún límite, la capacidad de este depósito es ilimitada. Consulte "[Uso del límite de capacidad](#)" Para más información.

5. Seleccione **Crear depósito**.

El depósito se crea y se agrega a la tabla en la página Depósitos.

6. Opcionalmente, seleccione **Ir a la página de detalles del depósito** para "[ver detalles del depósito](#)" y realizar una configuración adicional.

Ver detalles del depósito

Puede ver los depósitos en su cuenta de inquilino.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un "[navegador web compatible](#)".
- Pertenece a un grupo de usuarios que tiene la "[Permiso para acceso root, administrar todos los depósitos o ver todos los depósitos](#)". Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.

Pasos

1. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.

Aparece la página Cubos.

2. Revise la tabla de resumen para cada segmento.

Según sea necesario, puede ordenar la información por cualquier columna o puede avanzar o retroceder en la lista.



Los valores de recuento de objetos, espacio utilizado y uso que se muestran son estimaciones. Estas estimaciones se ven afectadas por el momento de la ingesta, la conectividad de la red y el estado del nodo. Si los depósitos tienen habilitada la gestión de versiones, las versiones de los objetos eliminados se incluyen en el recuento de objetos.

Nombre

El nombre único del depósito, que no se puede cambiar.

Funciones habilitadas

La lista de funciones que están habilitadas para el depósito.

Bloqueo de objetos S3

Si el bloqueo de objetos S3 está habilitado para el depósito.

Esta columna solo aparece si el bloqueo de objetos S3 está habilitado para la cuadrícula. Esta columna también muestra información sobre cualquier depósito compatible heredado.

Región

La región del cubo, que no se puede cambiar. Esta columna está oculta de forma predeterminada.

Recuento de objetos

La cantidad de objetos en este depósito. Si los depósitos tienen habilitada la gestión de versiones, las versiones de objetos no actuales se incluyen en este valor.

Cuando se agregan o eliminan objetos, es posible que este valor no se actualice inmediatamente.

Espacio utilizado

El tamaño lógico de todos los objetos en el depósito. El tamaño lógico no incluye el espacio real requerido para copias replicadas o codificadas por borrado o para metadatos de objetos.

Este valor puede tardar hasta 10 minutos en actualizarse.

Uso

El porcentaje utilizado del límite de capacidad del depósito, si se ha establecido uno.

El valor de uso se basa en estimaciones internas y podría superarse en algunos casos. Por ejemplo, StorageGRID verifica el límite de capacidad (si está configurado) cuando un inquilino comienza a cargar objetos y rechaza nuevas ingestas en este depósito si el inquilino ha excedido el límite de capacidad. Sin embargo, StorageGRID no tiene en cuenta el tamaño de la carga actual al determinar si se ha excedido el límite de capacidad. Si se eliminan objetos, es posible que se le impida temporalmente a un inquilino cargar nuevos objetos en este depósito hasta que se vuelva a calcular el uso del límite de capacidad. Los cálculos pueden tardar 10 minutos o más.

Este valor indica el tamaño lógico, no el tamaño físico necesario para almacenar los objetos y sus metadatos.

Capacidad

Si se establece, el límite de capacidad del depósito.

Fecha de creación

La fecha y hora en que se creó el depósito. Esta columna está oculta de forma predeterminada.

3. Para ver los detalles de un depósito específico, seleccione el nombre del depósito en la tabla.
 - a. Vea la información resumida en la parte superior de la página web para confirmar los detalles del depósito, como la región y la cantidad de objetos.
 - b. Ver la barra de uso del límite de capacidad. Si el uso es del 100% o cercano al 100%, considere aumentar el límite o eliminar algunos objetos.
 - c. Según sea necesario, seleccione **Eliminar objetos en el depósito** y **Eliminar depósito**.



Preste mucha atención a las precauciones que aparecen al seleccionar cada una de estas opciones. Para obtener más información, consulte:

- ["Eliminar todos los objetos en un depósito"](#)
- ["Eliminar un depósito"](#)(el cubo debe estar vacío)

d. Vea o cambie la configuración del depósito en cada una de las pestañas según sea necesario.

- **Consola S3:** Ver los objetos del depósito. Para obtener más información, consulte ["Usar la consola S3"](#) .
- **Opciones de depósito:** Ver o cambiar la configuración de las opciones. Algunas configuraciones, como el bloqueo de objetos S3, no se pueden cambiar una vez creado el depósito.
 - ["Gestionar la consistencia del depósito"](#)
 - ["Actualizaciones de la última hora de acceso"](#)
 - ["Límite de capacidad"](#)
 - ["Control de versiones de objetos"](#)
 - ["Bloqueo de objetos S3"](#)
 - ["Retención de depósito predeterminada"](#)
 - ["Administrar la replicación entre redes"](#)(si está permitido para el inquilino)
- **Servicios de plataforma:**["Administrar los servicios de la plataforma"](#) (si está permitido para el inquilino)
- **Acceso al bucket:** Ver o cambiar la configuración de las opciones. Debe tener permisos de acceso específicos.
 - Configurar["Intercambio de recursos entre orígenes \(CORS\)"](#) De esta forma, el depósito y los objetos dentro del depósito serán accesibles para las aplicaciones web en otros dominios.
 - ["Controlar el acceso de los usuarios"](#)para un bucket S3 y los objetos dentro de ese bucket.

Aplicar una etiqueta de política ILM a un depósito

Elija una etiqueta de política ILM para aplicar a un depósito en función de sus requisitos de almacenamiento de objetos.

La política ILM controla dónde se almacenan los datos del objeto y si se eliminan después de un cierto período de tiempo. El administrador de su red crea políticas ILM y las asigna a etiquetas de políticas ILM cuando utiliza múltiples políticas activas.



Evite reasignar con frecuencia la etiqueta de política de un depósito. De lo contrario, podrían surgir problemas de rendimiento.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un["navegador web compatible"](#) .
- Pertenece a un grupo de usuarios que tiene la["Permiso para acceso root, administrar todos los depósitos o ver todos los depósitos"](#) . Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.

Pasos

1. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.

Aparece la página Cubos. Según sea necesario, puede ordenar la información por cualquier columna o puede avanzar o retroceder en la lista.

2. Seleccione el nombre del depósito al que desea asignar una etiqueta de política ILM.

También puede cambiar la asignación de etiqueta de la política ILM para un depósito que ya tiene una etiqueta asignada.



Los valores de recuento de objetos y espacio utilizado que se muestran son estimaciones. Estas estimaciones se ven afectadas por el momento de la ingesta, la conectividad de la red y el estado del nodo. Si los depósitos tienen habilitada la gestión de versiones, las versiones de los objetos eliminados se incluyen en el recuento de objetos.

3. En la pestaña Opciones de depósito, expanda el acordeón de etiquetas de política ILM. Este acordeón solo aparece si el administrador de su red ha habilitado el uso de etiquetas de políticas personalizadas.
4. Lea la descripción de cada etiqueta de política para determinar qué etiqueta debe aplicarse al depósito.



Cambiar la etiqueta de política ILM de un depósito activará la reevaluación ILM de todos los objetos del depósito. Si la nueva política conserva los objetos durante un tiempo limitado, se eliminarán los objetos más antiguos.

5. Seleccione el botón de opción correspondiente a la etiqueta que desea asignar al depósito.
6. Seleccione **Guardar cambios**. Se establecerá una nueva etiqueta de depósito S3 en el depósito con la clave `NTAP-SG-ILM-BUCKET-TAG` y el valor del nombre de la etiqueta de política ILM.



Asegúrese de que sus aplicaciones S3 no anulen ni eliminen accidentalmente la nueva etiqueta de depósito. Si se omite esta etiqueta al aplicar un nuevo TagSet al depósito, los objetos del depósito volverán a evaluarse según la política ILM predeterminada.



Establezca y modifique las etiquetas de política de ILM utilizando únicamente el Administrador de inquilinos o la API del Administrador de inquilinos donde se valida la etiqueta de política de ILM. No modifique el `NTAP-SG-ILM-BUCKET-TAG` Etiqueta de política ILM que utiliza la API S3 PutBucketTagging o la API S3 DeleteBucketTagging.



Cambiar la etiqueta de política asignada a un depósito tiene un impacto temporal en el rendimiento mientras se reevalúan los objetos utilizando la nueva política ILM.

Administrar la política de depósitos

Puede controlar el acceso de los usuarios a un bucket S3 y a los objetos que contiene.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene la "Permiso de acceso root". Los permisos Ver todos los depósitos y Administrar todos los depósitos solo permiten la visualización.
- Ha verificado que la cantidad requerida de nodos de almacenamiento y sitios están disponibles. Si dos o más nodos de almacenamiento no están disponibles dentro de algún sitio, o si un sitio no está disponible,

es posible que los cambios en estas configuraciones no estén disponibles.

Pasos

1. Seleccione **Cubos** y luego seleccione el cubo que desea administrar.
2. En la página de detalles del depósito, seleccione **Acceso al depósito > Política del depósito**.
3. Debe realizar una de las siguientes acciones:
 - Introduzca una política de depósito seleccionando la casilla de verificación **Habilitar política**. Luego ingrese una cadena con formato JSON válida.

Cada política de bucket tiene un límite de tamaño de 20 480 bytes.
 - Modifique una política existente editando la cadena.
 - Deshabilite una política desmarcando la opción **Habilitar política**.

Para obtener información detallada sobre las políticas de bucket, incluida la sintaxis del lenguaje y ejemplos, consulte "[Ejemplos de políticas de depósito](#)".

Gestionar la consistencia del depósito

Los valores de consistencia se pueden usar para especificar la disponibilidad de los cambios de configuración del depósito, así como para proporcionar un equilibrio entre la disponibilidad de los objetos dentro de un depósito y la consistencia de esos objetos en diferentes nodos de almacenamiento y sitios. Puede cambiar los valores de consistencia para que sean diferentes de los valores predeterminados para que las aplicaciones cliente puedan satisfacer sus necesidades operativas.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un "[navegador web compatible](#)".
- Pertenece a un grupo de usuarios que tiene la "[Administrar todos los depósitos o permisos de acceso raíz](#)". Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.

Pautas de consistencia del cubo

La consistencia del depósito se utiliza para determinar la consistencia de las aplicaciones cliente que afectan a los objetos dentro de ese depósito S3. En general, debe utilizar la consistencia **Lectura después de nueva escritura** para sus depósitos.

Cambiar la consistencia del depósito

Si la consistencia de **Lectura después de nueva escritura** no cumple con los requisitos de la aplicación cliente, puede cambiar la consistencia configurando la consistencia del depósito o utilizando el `Consistency-Control` encabezamiento. El `Consistency-Control` El encabezado anula la consistencia del depósito.



Cuando se cambia la consistencia de un bucket, solo aquellos objetos que se ingieran después del cambio tienen la garantía de cumplir con la configuración revisada.

Pasos

1. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.

2. Seleccione el nombre del depósito de la tabla.

Aparece la página de detalles del depósito.

3. Desde la pestaña **Opciones de depósito**, seleccione el acordeón **.

4. Seleccione una consistencia para las operaciones realizadas en los objetos de este depósito.

- **Todos:** Proporciona el mayor nivel de consistencia. Todos los nodos reciben los datos inmediatamente o la solicitud fallará.
- **Strong-global:** garantiza la consistencia de lectura después de escritura para todas las solicitudes de clientes en todos los sitios.
- **Sitio fuerte:** garantiza la consistencia de lectura después de escritura para todas las solicitudes de clientes dentro de un sitio.
- **Lectura después de nueva escritura** (predeterminado): proporciona consistencia de lectura después de escritura para objetos nuevos y consistencia eventual para actualizaciones de objetos. Ofrece alta disponibilidad y garantías de protección de datos. Recomendado para la mayoría de los casos.
- **Disponible:** Proporciona consistencia eventual tanto para objetos nuevos como para actualizaciones de objetos. Para los buckets S3, úselo solo cuando sea necesario (por ejemplo, para un bucket que contiene valores de registro que rara vez se leen, o para operaciones HEAD o GET en claves que no existen). No compatible con depósitos S3 FabricPool .

5. Seleccione **Guardar cambios**.

¿Qué sucede cuando cambias la configuración del depósito?

Los depósitos tienen múltiples configuraciones que afectan el comportamiento de los depósitos y de los objetos dentro de ellos.

Las siguientes configuraciones de depósito utilizan una consistencia **fuerte** de manera predeterminada. Si dos o más nodos de almacenamiento no están disponibles dentro de algún sitio, o si un sitio no está disponible, es posible que los cambios en estas configuraciones no estén disponibles.

- "Eliminación de un depósito vacío en segundo plano"
- "Hora del último acceso"
- "Ciclo de vida del bucket"
- "Política de cubos"
- "Etiquetado de cubos"
- "Control de versiones de bucket"
- "Bloqueo de objetos S3"
- "Cifrado de bucket"



El valor de consistencia para el control de versiones del bucket, el bloqueo de objetos S3 y el cifrado del bucket no se puede establecer en un valor que no sea fuertemente consistente.

Las siguientes configuraciones de depósito no utilizan una consistencia fuerte y tienen una mayor disponibilidad para los cambios. Los cambios en esta configuración pueden tardar algún tiempo antes de surtir efecto.

- "Configuración de servicios de la plataforma: Integración de notificaciones, replicación o búsqueda"

- ["Configuración de CORS"](#)
- [Cambiar la consistencia del depósito](#)



Si la consistencia predeterminada utilizada al cambiar la configuración del depósito no cumple con los requisitos de la aplicación cliente, puede cambiar la consistencia mediante el uso de Consistency-Control encabezado para el ["API REST de S3"](#) o mediante el uso del reducedConsistency o force opciones en el ["API de gestión de inquilinos"](#).

Habilitar o deshabilitar las actualizaciones de la última hora de acceso

Cuando los administradores de red crean reglas de administración del ciclo de vida de la información (ILM) para un sistema StorageGRID, pueden especificar opcionalmente que se utilice la última hora de acceso de un objeto para determinar si se debe mover ese objeto a una ubicación de almacenamiento diferente. Si utiliza un inquilino S3, puede aprovechar dichas reglas habilitando actualizaciones de hora del último acceso para los objetos en un bucket S3.

Estas instrucciones solo se aplican a los sistemas StorageGRID que incluyen al menos una regla ILM que utiliza la opción **Hora del último acceso** como filtro avanzado o como hora de referencia. Puede ignorar estas instrucciones si su sistema StorageGRID no incluye dicha regla. Ver ["Utilice la hora del último acceso en las reglas de ILM"](#) Para más detalles.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene la ["Administrar todos los depósitos o permisos de acceso raíz"](#). Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.

Acerca de esta tarea

Hora del último acceso es una de las opciones disponibles para la instrucción de ubicación de **Hora de referencia** para una regla ILM. Establecer la hora de referencia para una regla en Hora del último acceso permite a los administradores de la red especificar que los objetos se coloquen en determinadas ubicaciones de almacenamiento en función de cuándo se recuperaron (leyeron o vieron) por última vez.

Por ejemplo, para garantizar que los objetos vistos recientemente permanezcan en un almacenamiento más rápido, un administrador de red puede crear una regla ILM que especifique lo siguiente:

- Los objetos que se hayan recuperado durante el último mes deben permanecer en los nodos de almacenamiento locales.
- Los objetos que no se hayan recuperado durante el último mes deberán trasladarse a una ubicación fuera del sitio.

De forma predeterminada, las actualizaciones de la hora del último acceso están deshabilitadas. Si su sistema StorageGRID incluye una regla ILM que utiliza la opción **Hora del último acceso** y desea que esta opción se aplique a los objetos en este bucket, debe habilitar las actualizaciones de la hora del último acceso para los buckets S3 especificados en esa regla.



Actualizar la hora del último acceso cuando se recupera un objeto puede reducir el rendimiento de StorageGRID, especialmente para objetos pequeños.

Se produce un impacto en el rendimiento con las actualizaciones del último tiempo de acceso porque

StorageGRID debe realizar estos pasos adicionales cada vez que se recuperan objetos:

- Actualizar los objetos con nuevas marcas de tiempo
- Agregue los objetos a la cola de ILM, para que puedan reevaluarse según las reglas y políticas de ILM actuales.

La tabla resume el comportamiento aplicado a todos los objetos en el depósito cuando el último tiempo de acceso está deshabilitado o habilitado.

Tipo de solicitud	Comportamiento si el último tiempo de acceso está deshabilitado (predeterminado)		Comportamiento si el último tiempo de acceso está habilitado	
	¿Última hora de acceso actualizada?	¿Objeto agregado a la cola de evaluación de ILM?	¿Última hora de acceso actualizada?	¿Objeto agregado 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
Solicitud de lista de objetos o versiones de objetos	No	No	No	No
Solicitud para copiar un objeto de un depósito a otro	• No, para la copia fuente • Sí, para la copia de destino	• No, para la copia fuente • Sí, para la copia de destino	• Sí, para la copia fuente • Sí, para la copia de destino	• Sí, para la copia fuente • Sí, para la copia de destino
Solicitud para completar una carga de varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Pasos

1. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.
2. Seleccione el nombre del depósito de la tabla.

Aparece la página de detalles del depósito.

3. Desde la pestaña **Opciones de depósito**, seleccione el acordeón **Actualizaciones de hora del último acceso**.

4. Habilitar o deshabilitar las actualizaciones del último tiempo de acceso.
5. Seleccione **Guardar cambios**.

Cambiar la versión de un objeto para un bucket

Si está utilizando un inquilino S3, puede cambiar el estado de la versión de los depósitos S3.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene la ["Administrar todos los depósitos o permisos de acceso raíz"](#). Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.
- Ha verificado que la cantidad requerida de nodos de almacenamiento y sitios están disponibles. Si dos o más nodos de almacenamiento no están disponibles dentro de algún sitio, o si un sitio no está disponible, es posible que los cambios en estas configuraciones no estén disponibles.

Acerca de esta tarea

Puede habilitar o suspender el control de versiones de objetos para un depósito. Después de habilitar el control de versiones para un depósito, este no podrá regresar a un estado sin versiones. Sin embargo, puedes suspender el control de versiones del depósito.

- Deshabilitado: El control de versiones nunca se ha habilitado
- Habilitado: el control de versiones está habilitado
- Suspendido: el control de versiones estaba habilitado previamente y está suspendido

Para obtener más información, consulte lo siguiente:

- ["Control de versiones de objetos"](#)
- ["Reglas y políticas de ILM para objetos versionados de S3 \(Ejemplo 4\)"](#)
- ["Cómo se eliminan los objetos"](#)

Pasos

1. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.
2. Seleccione el nombre del depósito de la tabla.

Aparece la página de detalles del depósito.

3. Desde la pestaña **Opciones de depósito**, seleccione el acordeón **Versiones de objeto**.
4. Seleccione un estado de control de versiones para los objetos en este depósito.

El control de versiones de objetos debe permanecer habilitado para un depósito utilizado para la replicación entre redes. Si está habilitado el bloqueo de objetos S3 o la conformidad con versiones anteriores, las opciones de **Control de versiones de objetos** estarán deshabilitadas.

Opción	Descripción
Habilitar control de versiones	Habilite el control de versiones de objetos si desea almacenar todas las versiones de cada objeto en este depósito. Luego puede recuperar versiones anteriores de un objeto según sea necesario. Los objetos que ya estaban en el depósito se versionarán cuando un usuario los modifique.
Suspender el control de versiones	Suspenda el control de versiones de objetos si ya no desea que se creen nuevas versiones de objetos. Aún puedes recuperar cualquier versión de objeto existente.

5. Seleccione **Guardar cambios**.

Utilice S3 Object Lock para retener objetos

Puede utilizar S3 Object Lock si los depósitos y objetos deben cumplir con los requisitos reglamentarios para la retención.



El administrador de su red debe darle permiso para utilizar funciones específicas de S3 Object Lock.

¿Qué es el bloqueo de objetos S3?

La función StorageGRID S3 Object Lock es una solución de protección de objetos que es equivalente a S3 Object Lock en Amazon Simple Storage Service (Amazon S3).

Cuando la configuración global de Bloqueo de objetos S3 está habilitada para un sistema StorageGRID, una cuenta de inquilino S3 puede crear depósitos con o sin el Bloqueo de objetos S3 habilitado. Si un bucket tiene habilitado el bloqueo de objetos S3, se requiere el control de versiones del bucket y se habilita automáticamente.

Un depósito sin bloqueo de objetos S3 solo puede tener objetos sin configuraciones de retención especificadas. Ningún objeto ingerido tendrá configuraciones de retención.

Un depósito con bloqueo de objetos S3 puede tener objetos con y sin configuraciones de retención especificadas por las aplicaciones cliente S3. Algunos objetos ingeridos tendrán configuraciones de retención.

Un depósito con bloqueo de objetos S3 y retención predeterminada configurada puede tener objetos cargados con configuraciones de retención especificadas y objetos nuevos sin configuraciones de retención. Los nuevos objetos utilizan la configuración predeterminada, porque la configuración de retención no se ha configurado a nivel de objeto.

De hecho, todos los objetos recién ingeridos tienen configuraciones de retención cuando se configura la retención predeterminada. Los objetos existentes sin configuraciones de retención de objetos no se verán afectados.

Modos de retención

La función de bloqueo de objetos de StorageGRID S3 admite dos modos de retención para aplicar diferentes niveles de protección a los objetos. Estos modos son equivalentes a los modos de retención de Amazon S3.

- En modo de cumplimiento:
 - El objeto no se puede eliminar hasta que se alcance su fecha de conservación.
 - La fecha de conservación del objeto se puede aumentar, pero no se puede disminuir.
 - La fecha de retención del objeto no se puede eliminar hasta que se alcance esa fecha.
- En modo de gobernanza:
 - Los usuarios con permiso especial pueden usar un encabezado de omisión en las solicitudes para modificar ciertas configuraciones de retención.
 - Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su fecha de conservación.
 - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de conservación de un objeto.

Configuración de retención para versiones de objetos

Si se crea un depósito con el bloqueo de objetos S3 habilitado, los usuarios pueden usar la aplicación cliente S3 para especificar opcionalmente las siguientes configuraciones de retención para cada objeto que se agregue al depósito:

- **Modo de retención:** Cumplimiento o gobernanza.
- **Conservar hasta fecha:** si la fecha de conservación de una versión de un objeto está en el futuro, el objeto se puede recuperar, pero no se puede eliminar.
- **Retención legal:** al aplicar una retención legal a una versión de un objeto, se bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesites colocar una retención legal en un objeto que esté relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, sino que permanece vigente hasta que se elimina explícitamente. Las retenciones legales son independientes de la fecha de conservación.



Si un objeto está bajo retención legal, nadie puede eliminarlo, independientemente de su modo de retención.

Para obtener detalles sobre la configuración de los objetos, consulte ["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#).

Configuración de retención predeterminada para depósitos

Si se crea un depósito con el bloqueo de objetos S3 habilitado, los usuarios pueden especificar opcionalmente las siguientes configuraciones predeterminadas para el depósito:

- **Modo de retención predeterminado:** Cumplimiento o gobernanza.
- **Período de retención predeterminado:** durante cuánto tiempo se deben conservar las nuevas versiones de objetos agregadas a este depósito, a partir del día en que se agregan.

La configuración de depósito predeterminada se aplica únicamente a los objetos nuevos que no tienen su propia configuración de retención. Los objetos de bucket existentes no se ven afectados cuando agrega o cambia estas configuraciones predeterminadas.

Ver ["Crear un bucket S3"](#) y ["Actualizar la retención predeterminada de bloqueo de objetos S3"](#).

Tareas de bloqueo de objetos S3

Las siguientes listas para administradores de red y usuarios inquilinos contienen las tareas de alto nivel para usar la función de bloqueo de objetos S3.

Administrador de red

- Habilite la configuración global de bloqueo de objetos S3 para todo el sistema StorageGRID .
- Asegúrese de que las políticas de gestión del ciclo de vida de la información (ILM) sean *compatibles*; es decir, que cumplan con los requisitos "[Requisitos de los buckets con bloqueo de objetos S3 habilitado](#)".
- Según sea necesario, permita que un inquilino utilice Cumplimiento como modo de retención. De lo contrario, solo se permite el modo Gobernanza.
- Según sea necesario, establezca un período máximo de retención para un inquilino.

Usuario inquilino

- Revise las consideraciones para depósitos y objetos con bloqueo de objetos S3.
- Según sea necesario, comuníquese con el administrador de la red para habilitar la configuración global de bloqueo de objetos S3 y establecer permisos.
- Cree depósitos con el bloqueo de objetos S3 habilitado.
- De manera opcional, configure los ajustes de retención predeterminados para un depósito:
 - Modo de retención predeterminado: Gobernanza o Cumplimiento, si lo permite el administrador de la red.
 - Período de retención predeterminado: debe ser menor o igual al período de retención máximo establecido por el administrador de la red.
- Utilice la aplicación cliente S3 para agregar objetos y, opcionalmente, configurar la retención específica de objetos:
 - Modo de retención. Gobernanza o Cumplimiento, si lo permite el administrador de la red.
 - Conservar hasta la fecha: debe ser menor o igual a lo permitido por el período máximo de retención establecido por el administrador de la red.

Requisitos para los buckets con el bloqueo de objetos S3 habilitado

- Si la configuración global de Bloqueo de objetos S3 está habilitada para el sistema StorageGRID , puede usar el Administrador de inquilinos, la API de administración de inquilinos o la API REST de S3 para crear depósitos con el Bloqueo de objetos S3 habilitado.
- Si planea utilizar S3 Object Lock, debe habilitar S3 Object Lock cuando cree el depósito. No se puede habilitar el bloqueo de objetos S3 para un depósito existente.
- Cuando S3 Object Lock está habilitado para un bucket, StorageGRID habilita automáticamente el control de versiones para ese bucket. No puedes deshabilitar el bloqueo de objetos S3 ni suspender el control de versiones del depósito.
- De manera opcional, puede especificar un modo de retención predeterminado y un período de retención para cada depósito mediante el Administrador de inquilinos, la API de administración de inquilinos o la API REST de S3. La configuración de retención predeterminada del depósito se aplica únicamente a los objetos nuevos agregados al depósito que no tienen su propia configuración de retención. Puede anular estas configuraciones predeterminadas especificando un modo de retención y una fecha de retención para cada versión del objeto cuando se carga.
- La configuración del ciclo de vida del bucket es compatible con los buckets que tienen el bloqueo de objetos S3 habilitado.

- La replicación de CloudMirror no es compatible con depósitos con el bloqueo de objetos S3 habilitado.

Requisitos para objetos en depósitos con bloqueo de objetos S3 habilitado

- Para proteger una versión de objeto, puede especificar la configuración de retención predeterminada para el depósito o puede especificar la configuración de retención para cada versión de objeto. Las configuraciones de retención a nivel de objeto se pueden especificar mediante la aplicación cliente S3 o la API REST S3.
- Las configuraciones de retención se aplican a versiones de objetos individuales. Una versión de objeto puede tener una configuración de conservación hasta la fecha y una configuración de conservación legal, una pero no la otra, o ninguna. Al especificar una configuración de retención hasta la fecha o de retención legal para un objeto, se protege únicamente la versión especificada en la solicitud. Puede crear nuevas versiones del objeto, mientras la versión anterior del objeto permanece bloqueada.

Ciclo de vida de objetos en buckets con S3 Object Lock habilitado

Cada objeto que se guarda en un bucket con el bloqueo de objetos S3 habilitado pasa por estas etapas:

1. Ingesta de objeto

Cuando se agrega una versión de objeto a un depósito que tiene habilitado el Bloqueo de objetos S3, las configuraciones de retención se aplican de la siguiente manera:

- Si se especifican configuraciones de retención para el objeto, se aplican las configuraciones a nivel de objeto. Se ignoran todas las configuraciones de depósito predeterminadas.
- Si no se especifican configuraciones de retención para el objeto, se aplican las configuraciones de depósito predeterminadas, si existen.
- Si no se especifican configuraciones de retención para el objeto o el depósito, el objeto no estará protegido por el bloqueo de objetos S3.

Si se aplican configuraciones de retención, tanto el objeto como cualquier metadato definido por el usuario de S3 estarán protegidos.

2. Retención y eliminación de objetos

StorageGRID almacena varias copias de cada objeto protegido durante el período de retención especificado. La cantidad exacta y el tipo de copias de objetos y las ubicaciones de almacenamiento están determinados por las reglas compatibles con las políticas ILM activas. Si un objeto protegido se puede eliminar antes de que se alcance su fecha de retención depende de su modo de retención.

- Si un objeto está bajo retención legal, nadie puede eliminarlo, independientemente de su modo de retención.

¿Puedo seguir administrando buckets compatibles heredados?

La función de bloqueo de objetos S3 reemplaza la función de cumplimiento que estaba disponible en versiones anteriores de StorageGRID. Si creó depósitos compatibles con una versión anterior de StorageGRID, puede continuar administrando la configuración de estos depósitos; sin embargo, ya no podrá crear nuevos depósitos compatibles. Para obtener instrucciones, consulte https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5 ["Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5"].

Actualizar la retención predeterminada de bloqueo de objetos S3

Si habilitó el bloqueo de objetos S3 cuando creó el depósito, puede editarlo para cambiar la configuración de retención predeterminada. Puede habilitar (o deshabilitar) la retención predeterminada y establecer un modo de retención y un período de retención predeterminados.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#) .
- Pertenece a un grupo de usuarios que tiene la ["Administrar todos los depósitos o permisos de acceso raíz"](#) . Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.
- El bloqueo de objetos S3 está habilitado globalmente para su sistema StorageGRID y usted lo habilitó cuando creó el depósito. Ver ["Utilice S3 Object Lock para retener objetos"](#) .

Pasos

1. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.
2. Seleccione el nombre del depósito de la tabla.

Aparece la página de detalles del depósito.

3. Desde la pestaña **Opciones de depósito**, seleccione el acordeón **Bloqueo de objeto S3**.
4. De manera opcional, habilite o deshabilite la **Retención predeterminada** para este depósito.

Los cambios en esta configuración no se aplican a los objetos que ya están en el depósito ni a ningún objeto que pueda tener sus propios períodos de retención.

5. Si la **Retención predeterminada** está habilitada, especifique un **Modo de retención predeterminado** para el depósito.

Modo de retención predeterminado	Descripción
Gobernancia	• Usuarios con la <code>s3:BypassGovernanceRetention</code> El permiso puede utilizar el <code>x-amz-bypass-governance-retention:true</code> encabezado de solicitud para omitir la configuración de retención. • Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su fecha de conservación. • Estos usuarios pueden aumentar, disminuir o eliminar la fecha de conservación de un objeto.

Modo de retención predeterminado	Descripción
Cumplimiento	• El objeto no se puede eliminar hasta que se alcance su fecha de conservación. • La fecha de conservación del objeto se puede aumentar, pero no se puede disminuir. • La fecha de retención del objeto no se puede eliminar hasta que se alcance esa fecha. Nota: El administrador de su red debe permitirle utilizar el modo de cumplimiento.

6. Si la **Retención predeterminada** está habilitada, especifique el **Período de retención predeterminado** para el depósito.

El **Período de retención predeterminado** indica durante cuánto tiempo se deben conservar los objetos nuevos agregados a este depósito, a partir del momento en que se ingieren. Especifique un valor que sea menor o igual al período de retención máximo para el inquilino, según lo establecido por el administrador de la red.

Se establece un período de retención *máximo*, que puede tener un valor de entre 1 día y 100 años, cuando el administrador de la red crea el inquilino. Cuando se establece un período de retención *predeterminado*, no puede exceder el valor establecido para el período de retención máximo. Si es necesario, solicite al administrador de su red que aumente o disminuya el período máximo de retención.

7. Seleccione **Guardar cambios**.

Configurar el uso compartido de recursos entre orígenes (CORS)

Puede configurar el uso compartido de recursos de origen cruzado (CORS) para un bucket S3 si desea que ese bucket y los objetos que contiene sean accesibles para las aplicaciones web en otros dominios.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un [navegador web compatible](#).
- Para las solicitudes de configuración GET CORS, usted pertenece a un grupo de usuarios que tiene la ["Administrar todos los depósitos o Ver todos los permisos de los depósitos"](#). Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.
- Para las solicitudes de configuración PUT CORS, usted pertenece a un grupo de usuarios que tiene la ["Administrar todos los permisos de los buckets"](#). Este permiso anula la configuración de permisos en las políticas de grupo o de depósito.
- El ["Permiso de acceso root"](#) Proporciona acceso a todas las solicitudes de configuración de CORS.

Acerca de esta tarea

El uso compartido de recursos entre orígenes (CORS) es un mecanismo de seguridad que permite que las aplicaciones web cliente de un dominio accedan a recursos de un dominio diferente. Por ejemplo, supongamos que utiliza un depósito S3 llamado `Images` para almacenar gráficos. Al configurar CORS para el `Images` Cubo, puede permitir que las imágenes en ese cubo se muestren en el sitio web `http://www.example.com`.

Habilitar CORS para un bucket

Pasos

1. Utilice un editor de texto para crear el XML requerido. Este ejemplo muestra el XML utilizado para habilitar CORS para un bucket S3. Específicamente:
 - Permite que cualquier dominio envíe solicitudes GET al depósito
 - Sólo permite el `http://www.example.com` dominio para enviar solicitudes GET, POST y DELETE
 - Se permiten todos los encabezados de solicitud

```
<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 sobre el XML de configuración de CORS, consulte ["Documentación de Amazon Web Services \(AWS\): Guía del usuario de Amazon Simple Storage Service"](#).

2. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.
3. Seleccione el nombre del depósito de la tabla.

Aparece la página de detalles del depósito.

4. Desde la pestaña **Acceso al bucket**, seleccione el acordeón **Intercambio de recursos de origen cruzado (CORS)**.
5. Seleccione la casilla de verificación **Habilitar CORS**.
6. Pegue el XML de configuración de CORS en el cuadro de texto.
7. Seleccione **Guardar cambios**.

Modificar la configuración de CORS

Pasos

1. Actualice el XML de configuración de CORS en el cuadro de texto o seleccione **Borrar** para comenzar de nuevo.
2. Seleccione **Guardar cambios**.

Deshabilitar la configuración CORS

Pasos

1. Desmarque la casilla de verificación **Habilitar CORS**.
2. Seleccione **Guardar cambios**.

Eliminar objetos en el depósito

Puede utilizar el Administrador de inquilinos para eliminar los objetos en uno o más depósitos.

Consideraciones y requisitos

Antes de realizar estos pasos, tenga en cuenta lo siguiente:

- Cuando elimina los objetos de un depósito, StorageGRID elimina de forma permanente todos los objetos y todas las versiones de objetos en cada depósito seleccionado de todos los nodos y sitios de su sistema StorageGRID . StorageGRID también elimina cualquier metadato de objeto relacionado. No podrás recuperar esta información.
- Eliminar todos los objetos de un depósito puede llevar minutos, días o incluso semanas, según la cantidad de objetos, copias de objetos y operaciones simultáneas.
- Si un cubo tiene "[Bloqueo de objetos S3 habilitado](#)" , podría permanecer en el estado **Eliminando objetos: solo lectura** durante *años*.



Un depósito que utiliza S3 Object Lock permanecerá en el estado **Eliminando objetos: solo lectura** hasta que se alcance la fecha de retención para todos los objetos y se eliminen todas las retenciones legales.

- Mientras se eliminan objetos, el estado del depósito es **Eliminando objetos: solo lectura**. En este estado no se pueden agregar nuevos objetos al depósito.
- Cuando se hayan eliminado todos los objetos, el depósito permanecerá en estado de solo lectura. Puede realizar una de las siguientes acciones:
 - Devuelva el depósito al modo de escritura y reutilícelo para nuevos objetos
 - Eliminar el depósito
 - Mantenga el depósito en modo de solo lectura para reservar su nombre para uso futuro
- Si un bucket tiene habilitada la versión de objetos, los marcadores de eliminación que se crearon en StorageGRID 11.8 o posterior se pueden quitar mediante las operaciones Eliminar objetos en el bucket.
- Si un bucket tiene habilitada la versión de objetos, la operación de eliminación de objetos no eliminará los marcadores de eliminación creados en StorageGRID 11.7 o anterior. Consulte información sobre cómo eliminar objetos en un depósito en "[Cómo se eliminan los objetos versionados de S3](#)" .
- Si utilizas "[replicación entre redes](#)" , tenga en cuenta lo siguiente:
 - Al utilizar esta opción no se elimina ningún objeto del depósito en la otra cuadrícula.
 - Si selecciona esta opción para el depósito de origen, se activará la alerta **Error de replicación entre cuadrículas** si agrega objetos al depósito de destino en la otra cuadrícula. Si no puede garantizar que nadie agregará objetos al contenedor en la otra cuadrícula, "[Deshabilitar la replicación entre redes](#)" para ese depósito antes de eliminar todos los objetos del depósito.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#) .
- Pertenece a un grupo de usuarios que tiene la ["Permiso de acceso root"](#) . Este permiso anula la configuración de permisos en las políticas de grupo o de depósito.

Pasos

1. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.

Aparece la página Buckets y muestra todos los buckets S3 existentes.

2. Utilice el menú **Acciones** o la página de detalles para un bucket específico.

Menú de acciones

- a. Seleccione la casilla de verificación para cada depósito del que desee eliminar objetos.
- b. Seleccione **Acciones > Eliminar objetos en el depósito**.

Página de detalles

- a. Seleccione un nombre de depósito para mostrar sus detalles.
- b. Seleccione **Eliminar objetos del depósito**.

3. Cuando aparezca el cuadro de diálogo de confirmación, revise los detalles, ingrese **Sí** y seleccione **Aceptar**.
4. Espere a que comience la operación de eliminación.

Después de unos minutos:

- Aparece un banner de estado amarillo en la página de detalles del depósito. La barra de progreso representa qué porcentaje de objetos se han eliminado.
- **(solo lectura)** aparece después del nombre del depósito en la página de detalles del depósito.
- **(Eliminar objetos: solo lectura)** aparece junto al nombre del depósito en la página Depósitos.

Buckets > my-bucket

my-bucket (read-only)

Region: us-east-1

Date created: 2022-12-14 10:09:50 MST

Object count: 3

View bucket contents in Experimental S3 Console

Delete bucket

 **All bucket objects are being deleted**

StorageGRID is deleting all copies of the objects in this bucket, which might take days or weeks. While objects are being deleted, the bucket is read only. To stop the operation, select **Stop deleting objects**. You cannot restore objects that have already been deleted.

0% (0 of 3 objects deleted)

Stop deleting objects

Success

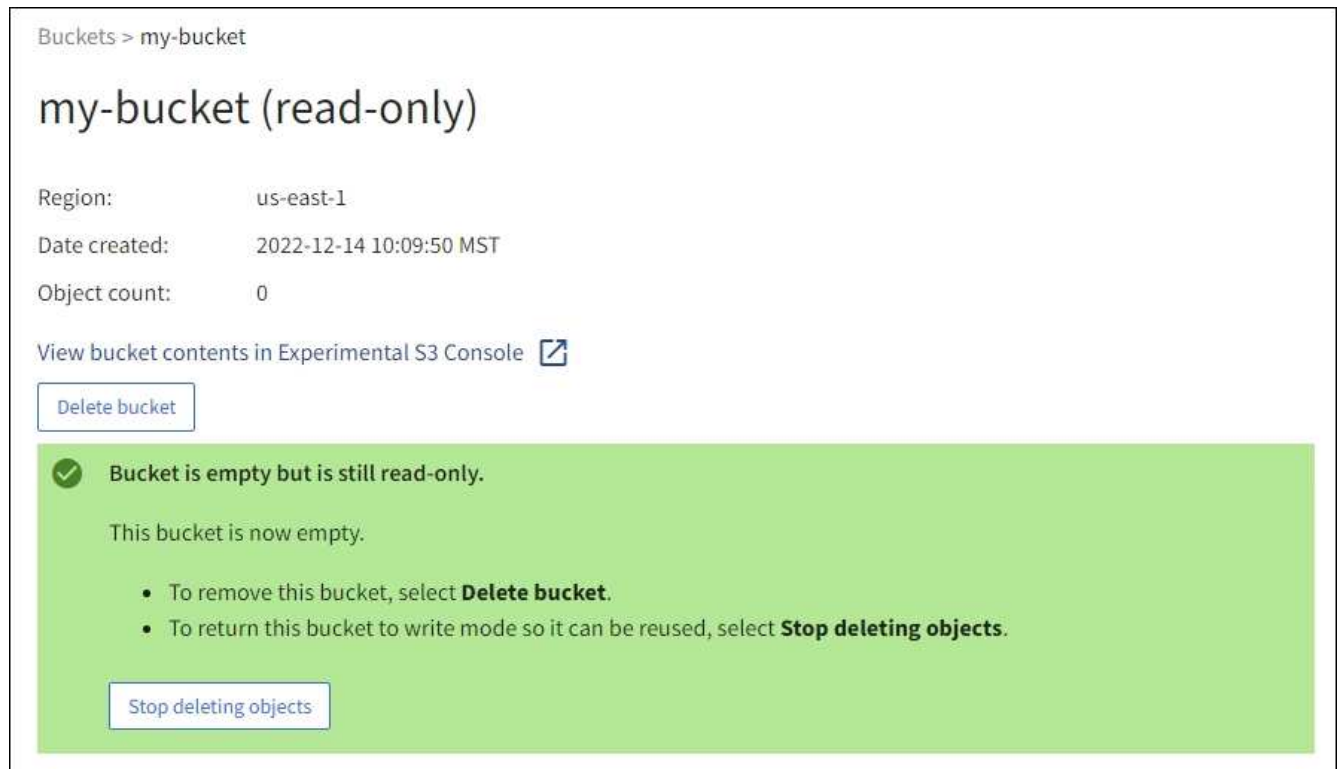
Starting to delete objects from one bucket.

5. Según sea necesario mientras la operación se esté ejecutando, seleccione **Detener la eliminación de objetos** para detener el proceso. Luego, opcionalmente, seleccione **Eliminar objetos en el depósito** para reanudar el proceso.

Cuando selecciona **Detener eliminación de objetos**, el depósito vuelve al modo de escritura; sin embargo, no puede acceder ni restaurar ningún objeto que se haya eliminado.

6. Espere a que se complete la operación.

Cuando el depósito está vacío, el banner de estado se actualiza, pero el depósito permanece como de solo lectura.



7. Debe realizar una de las siguientes acciones:

- Salga de la página para mantener el depósito en modo de solo lectura. Por ejemplo, puede mantener un depósito vacío en modo de solo lectura para reservar el nombre del depósito para uso futuro.
- Eliminar el depósito. Puede seleccionar **Eliminar depósito** para eliminar un solo depósito o regresar a la página Depósitos y seleccionar **Acciones > Eliminar depósitos** para eliminar más de un depósito.



Si no puede eliminar un depósito versionado después de eliminar todos los objetos, es posible que queden marcadores de eliminación. Para eliminar el depósito, debes quitar todos los marcadores de eliminación restantes.

- Devuelve el depósito al modo de escritura y, opcionalmente, reutilízalo para nuevos objetos. Puede seleccionar **Detener la eliminación de objetos** para un solo depósito o regresar a la página Depósitos y seleccionar **Acción > Detener la eliminación de objetos** para más de un depósito.

Eliminar el depósito S3

Puede utilizar el Administrador de inquilinos para eliminar uno o más depósitos S3 que estén vacíos.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene la ["Administrar todos los depósitos o permisos de acceso raíz"](#). Estos permisos anulan la configuración de permisos en las políticas de grupo o de depósito.
- Los depósitos que desea eliminar están vacíos. Si los depósitos que desea eliminar no están vacíos, ["eliminar objetos del depósito"](#).

Acerca de esta tarea

Estas instrucciones describen cómo eliminar un depósito S3 mediante el Administrador de inquilinos. También

puedes eliminar depósitos S3 usando el ["API de gestión de inquilinos"](#) o el ["API REST de S3"](#) .

No puedes eliminar un bucket S3 si contiene objetos, versiones de objetos no actuales o marcadores de eliminación. Para obtener información sobre cómo se eliminan los objetos versionados de S3, consulte ["Cómo se eliminan los objetos"](#) .

Pasos

1. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.

Aparece la página Buckets y muestra todos los buckets S3 existentes.

2. Utilice el menú **Acciones** o la página de detalles para un bucket específico.

Menú de acciones

- a. Seleccione la casilla de verificación para cada depósito que desee eliminar.
- b. Seleccione **Acciones > Eliminar depósitos**.

Página de detalles

- a. Seleccione un nombre de depósito para mostrar sus detalles.
- b. Seleccione **Eliminar depósito**.

3. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí**.

StorageGRID confirma que cada depósito está vacío y luego elimina cada uno de ellos. Esta operación puede tardar unos minutos.

Si un depósito no está vacío, aparece un mensaje de error. Usted debe ["eliminar todos los objetos y cualquier marcador de eliminación en el depósito"](#) antes de poder eliminar el depósito.

Usar la consola S3

Puede utilizar la Consola S3 para ver y administrar los objetos en un bucket S3.

La consola S3 le permite:

- Cargar, descargar, renombrar, copiar, mover y eliminar objetos
- Ver, revertir, descargar y eliminar versiones de objetos
- Buscar objetos por prefijo
- Administrar etiquetas de objetos
- Ver metadatos del objeto
- Ver, crear, renombrar, copiar, mover y eliminar carpetas

La consola S3 proporciona una experiencia de usuario mejorada para los casos más comunes. No está diseñado para reemplazar las operaciones CLI o API en todas las situaciones.



Si el uso de la consola S3 hace que las operaciones tarden demasiado tiempo (por ejemplo, minutos u horas), considere lo siguiente:

- Reducir el número de objetos seleccionados
- Usar métodos no gráficos (API o CLI) para acceder a sus datos

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#) .
- Si desea administrar objetos, pertenece a un grupo de usuarios que tenga permiso de acceso Root. Como alternativa, pertenece a un grupo de usuarios que tiene el permiso de la pestaña Usar consola S3 y el permiso Ver todos los depósitos o el permiso Administrar todos los depósitos. Ver ["Permisos de gestión de inquilinos"](#) .
- Se ha configurado una política de grupo o bucket S3 para el usuario. Ver ["Utilice políticas de acceso a grupos y buckets"](#) .
- Conoces el ID de la clave de acceso del usuario y la clave de acceso secreta. Opcionalmente, tienes un `.csv` archivo que contiene esta información. Ver el ["instrucciones para crear claves de acceso"](#) .

Pasos

1. Seleccione **ALMACENAMIENTO > Cubos > *nombre del cubo***.
2. Seleccione la pestaña Consola S3.
3. Pegue el ID de la clave de acceso y la clave de acceso secreta en los campos. De lo contrario, seleccione **Cargar claves de acceso** y seleccione su `.csv` archivo.
4. Seleccionar * Sign in*.
5. Aparece la tabla de objetos del bucket. Puede administrar objetos según sea necesario.

Información adicional

- **Buscar por prefijo:** La función de búsqueda por prefijo solo busca objetos que comiencen con una palabra específica relativa a la carpeta actual. La búsqueda no incluye objetos que contengan la palabra en otro lugar. Esta regla también se aplica a los objetos dentro de las carpetas. Por ejemplo, una búsqueda de `folder1/folder2/somefile-` devolvería objetos que están dentro del `folder1/folder2/` carpeta y comenzar con la palabra `somefile-` .
- **Arrastrar y soltar:** puedes arrastrar y soltar archivos desde el administrador de archivos de tu computadora a la Consola S3. Sin embargo, no es posible cargar carpetas.
- **Operaciones en carpetas:** cuando mueves, copias o renombas una carpeta, todos los objetos en la carpeta se actualizan uno a la vez, lo que puede llevar tiempo.
- **Eliminación permanente cuando el control de versiones del depósito está deshabilitado:** cuando sobrescribe o elimina un objeto en un depósito con el control de versiones deshabilitado, la operación es permanente. Ver ["Cambiar la versión de un objeto para un bucket"](#) .

Administrar los servicios de la plataforma S3

Servicios de la plataforma S3

Descripción general y consideraciones sobre los servicios de la plataforma

Antes de implementar los servicios de la plataforma, revise la descripción general y las consideraciones para el uso de estos servicios.

Para obtener información sobre S3, consulte ["Utilice la API REST de S3"](#).

Descripción general de los servicios de la plataforma

Los servicios de la plataforma StorageGRID pueden ayudarlo a implementar una estrategia de nube híbrida al permitirle enviar notificaciones de eventos y copias de objetos S3 y metadatos de objetos a destinos externos.

Dado que la ubicación de destino de los servicios de plataforma generalmente es externa a su implementación de StorageGRID, los servicios de plataforma le brindan la potencia y la flexibilidad que brinda el uso de recursos de almacenamiento externos, servicios de notificación y servicios de búsqueda o análisis para sus datos.

Se puede configurar cualquier combinación de servicios de plataforma para un único bucket S3. Por ejemplo, puede configurar tanto el ["Servicio CloudMirror"](#) y ["notificaciones"](#) en un bucket S3 de StorageGRID para que pueda reflejar objetos específicos en Amazon Simple Storage Service (S3) y, al mismo tiempo, enviar una notificación sobre cada uno de esos objetos a una aplicación de monitoreo de terceros para ayudarlo a realizar un seguimiento de sus gastos de AWS.



El uso de los servicios de la plataforma debe ser habilitado para cada cuenta de inquilino por un administrador de StorageGRID mediante Grid Manager o la API de administración de Grid.

Cómo se configuran los servicios de la plataforma

Los servicios de plataforma se comunican con puntos finales externos que usted configura mediante el ["Administrador de inquilinos"](#) o el ["API de gestión de inquilinos"](#). Cada punto final representa un destino externo, como un bucket S3 de StorageGRID, un bucket de Amazon Web Services, un tema de Amazon SNS o un clúster de Elasticsearch alojado localmente, en AWS o en otro lugar.

Después de crear un punto final externo, puede habilitar un servicio de plataforma para un depósito agregando una configuración XML al depósito. La configuración XML identifica los objetos sobre los que debe actuar el depósito, la acción que debe realizar el depósito y el punto final que debe utilizar el depósito para el servicio.

Debe agregar configuraciones XML independientes para cada servicio de plataforma que desee configurar. Por ejemplo:

- Si desea todos los objetos cuyas claves comiencen con `/images` Para replicarlo en un bucket de Amazon S3, debe agregar una configuración de replicación al bucket de origen.
- Si también desea enviar notificaciones cuando estos objetos se almacenan en el depósito, debe agregar una configuración de notificaciones.
- Si desea indexar los metadatos de estos objetos, debe agregar la configuración de notificación de metadatos que se utiliza para implementar la integración de búsqueda.

El formato del XML de configuración está regido por las API REST de S3 utilizadas para implementar los servicios de la plataforma StorageGRID :

Servicio de plataforma	API REST de S3	Referirse a
Replicación de CloudMirror	• Obtener réplica de cubo • Replicación de PutBucket	• "Replicación de CloudMirror" • "Operaciones en buckets"
Notificaciones	• Configuración de GetBucketNotification • Configuración de notificación de PutBucket	• "Notificaciones" • "Operaciones en buckets"
Integración de búsqueda	• Configuración de notificación de metadatos del depósito GET • Configuración de notificación de metadatos del depósito PUT	• "Integración de búsqueda" • "Operaciones personalizadas de StorageGRID"

Consideraciones para el uso de servicios de plataforma

Consideración	Detalles
Monitoreo de puntos finales de destino	Debes supervisar la disponibilidad de cada punto final de destino. Si se pierde la conectividad con el punto final de destino durante un período prolongado y existe una gran acumulación de solicitudes, las solicitudes de cliente adicionales (como las solicitudes PUT) a StorageGRID fallarán. Debes volver a intentar estas solicitudes fallidas cuando el punto final sea accesible.
Limitación del punto final de destino	El software StorageGRID puede limitar las solicitudes S3 entrantes para un bucket si la velocidad a la que se envían las solicitudes excede la velocidad a la que el punto final de destino puede recibirlas. La limitación solo se produce cuando hay una acumulación de solicitudes en espera de ser enviadas al punto final de destino. El único efecto visible es que las solicitudes S3 entrantes tardarán más en ejecutarse. Si comienza a detectar un rendimiento significativamente más lento, debe reducir la tasa de ingesta o utilizar un punto final con mayor capacidad. Si la acumulación de solicitudes continúa creciendo, las operaciones S3 del cliente (como las solicitudes PUT) eventualmente fallarán. Es más probable que las solicitudes de CloudMirror se vean afectadas por el rendimiento del punto final de destino porque estas solicitudes generalmente implican más transferencia de datos que las solicitudes de integración de búsqueda o notificación de eventos.

Consideración	Detalles
Garantías de pedidos	StorageGRID garantiza el orden de las operaciones en un objeto dentro de un sitio. Siempre que todas las operaciones contra un objeto se realicen dentro del mismo sitio, el estado final del objeto (para la replicación) siempre será igual al estado en StorageGRID. StorageGRID hace todo lo posible para ordenar las solicitudes cuando se realizan operaciones en los sitios de StorageGRID . Por ejemplo, si escribe un objeto inicialmente en el sitio A y luego sobrescribe el mismo objeto en el sitio B, no se garantiza que el objeto final replicado por CloudMirror en el depósito de destino sea el objeto más nuevo.
Eliminaciones de objetos impulsadas por ILM	Para que coincida con el comportamiento de eliminación de AWS CRR y Amazon Simple Notification Service, las solicitudes de notificación de eventos y CloudMirror no se envían cuando se elimina un objeto en el bucket de origen debido a las reglas ILM de StorageGRID . Por ejemplo, no se envían solicitudes de notificaciones de eventos ni de CloudMirror si una regla ILM elimina un objeto después de 14 días. Por el contrario, las solicitudes de integración de búsqueda se envían cuando se eliminan objetos debido a ILM.
Uso de puntos finales de Kafka	Para los puntos finales de Kafka, no se admite TLS mutuo. Como resultado, si tienes <code>ssl.client.auth</code> empezar a <code>required</code> en la configuración de su agente de Kafka, podría causar problemas de configuración del punto final de Kafka. La autenticación de los puntos finales de Kafka utiliza los siguientes tipos de autenticación. Estos tipos son diferentes de los que se utilizan para la autenticación de otros puntos finales, como Amazon SNS, y requieren credenciales de nombre de usuario y contraseña. • SASL/LLANO • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 Nota: Las configuraciones del proxy de almacenamiento configuradas no se aplican a los puntos finales de los servicios de la plataforma Kafka.

Consideraciones para utilizar el servicio de replicación CloudMirror

Consideración	Detalles
Estado de replicación	StorageGRID no es compatible con <code>x-amz-replication-status</code> encabezamiento.

Consideración	Detalles
Tamaño del objeto	El tamaño máximo de los objetos que el servicio de replicación CloudMirror puede replicar en un depósito de destino es de 5 TiB, que es el mismo que el tamaño máximo de objeto <i>compatible</i>. Nota: El tamaño máximo <i>recomendado</i> para una sola operación PutObject es 5 GiB (5.368.709.120 bytes). Si tiene objetos de más de 5 GiB, utilice la carga multiparte en su lugar.
Control de versiones de bucket e ID de versiones	Si el depósito S3 de origen en StorageGRID tiene habilitada la gestión de versiones, también debe habilitarla para el depósito de destino. Al utilizar versiones, tenga en cuenta que el orden de las versiones de los objetos en el depósito de destino es el máximo esfuerzo y no está garantizado por el servicio CloudMirror, debido a las limitaciones del protocolo S3. Nota: Los ID de versión del depósito de origen en StorageGRID no están relacionados con los ID de versión del depósito de destino.
Etiquetado de versiones de objetos	El servicio CloudMirror no replica ninguna solicitud PutObjectTagging o DeleteObjectTagging que proporcione un ID de versión, debido a limitaciones en el protocolo S3. Debido a que los ID de versión para el origen y el destino no están relacionados, no hay forma de garantizar que se replique una actualización de etiqueta a un ID de versión específico. Por el contrario, el servicio CloudMirror replica solicitudes PutObjectTagging o DeleteObjectTagging que no especifican un ID de versión. Estas solicitudes actualizan las etiquetas para la última clave (o la última versión si el depósito tiene versión). Las ingestas normales con etiquetas (no actualizaciones de etiquetas) también se replican.
Cargas multiparte y ETag valores	Al reflejar objetos que se cargaron mediante una carga multiparte, el servicio CloudMirror no conserva las partes. Como resultado, la ETag El valor del objeto reflejado será diferente al ETag valor del objeto original.
Objetos cifrados con SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente)	El servicio CloudMirror no admite objetos cifrados con SSE-C. Si intenta ingerir un objeto en el bucket de origen para la replicación de CloudMirror y la solicitud incluye los encabezados de solicitud SSE-C, la operación fallará.
Cubo con bloqueo de objetos S3 habilitado	La replicación no es compatible con los depósitos de origen o destino que tengan el bloqueo de objetos S3 habilitado.

Comprender el servicio de replicación CloudMirror

Puede habilitar la replicación de CloudMirror para un bucket S3 si desea que StorageGRID replique objetos específicos agregados al bucket en uno o más buckets de destino externos.

Por ejemplo, puede utilizar la replicación de CloudMirror para reflejar registros de clientes específicos en Amazon S3 y luego aprovechar los servicios de AWS para realizar análisis de sus datos.



La replicación de CloudMirror no es compatible si el depósito de origen tiene habilitado el bloqueo de objetos S3.

CloudMirror e ILM

La replicación de CloudMirror funciona independientemente de las políticas ILM activas de la red. El servicio CloudMirror replica los objetos a medida que se almacenan en el depósito de origen y los envía al depósito de destino lo antes posible. La entrega de objetos replicados se activa cuando la ingesta del objeto se realiza correctamente.

CloudMirror y replicación entre redes

La replicación de CloudMirror tiene similitudes y diferencias importantes con la función de replicación entre redes. Consulte ["Comparar la replicación entre redes y la replicación de CloudMirror"](#).

Cubos de CloudMirror y S3

La replicación de CloudMirror normalmente está configurada para utilizar un depósito S3 externo como destino. Sin embargo, también puede configurar la replicación para utilizar otra implementación de StorageGRID o cualquier servicio compatible con S3.

Cubos existentes

Cuando habilita la replicación de CloudMirror para un depósito existente, solo se replican los nuevos objetos agregados a ese depósito. Cualquier objeto existente en el depósito no se replica. Para forzar la replicación de objetos existentes, puede actualizar los metadatos del objeto existente realizando una copia del objeto.



Si utiliza la replicación de CloudMirror para copiar objetos a un destino de Amazon S3, tenga en cuenta que Amazon S3 limita el tamaño de los metadatos definidos por el usuario dentro de cada encabezado de solicitud PUT a 2 KB. Si un objeto tiene metadatos definidos por el usuario mayores a 2 KB, ese objeto no se replicará.

Cubos de destino múltiples

Para replicar objetos de un solo depósito en varios depósitos de destino, especifique el destino de cada regla en el XML de configuración de replicación. No es posible replicar un objeto en más de un bucket al mismo tiempo.

Cubos versionados o no versionados

Puede configurar la replicación de CloudMirror en depósitos versionados o no versionados. Los depósitos de destino pueden tener versiones o no. Puede utilizar cualquier combinación de depósitos versionados y no versionados. Por ejemplo, puede especificar un depósito versionado como destino para un depósito de origen no versionado, o viceversa. También puedes replicar entre depósitos sin versiones.

Eliminación, bucles de replicación y eventos

Comportamiento de eliminación

Es lo mismo que el comportamiento de eliminación del servicio Amazon S3, Replicación entre regiones (CRR). Eliminar un objeto en un depósito de origen nunca elimina un objeto replicado en el destino. Si tanto el depósito de origen como el de destino tienen versiones, se replica el marcador de eliminación. Si el depósito de destino no tiene versión, eliminar un objeto en el depósito de origen no replica el marcador de

eliminación en el depósito de destino ni elimina el objeto de destino.

Protección contra bucles de replicación

A medida que los objetos se replican en el depósito de destino, StorageGRID los marca como "réplicas". Un depósito StorageGRID de destino no volverá a replicar objetos marcados como réplicas, lo que lo protege de bucles de replicación accidentales. Esta marca de réplica es interna a StorageGRID y no le impide aprovechar AWS CRR cuando usa un bucket de Amazon S3 como destino.



El encabezado personalizado utilizado para marcar una réplica es `x-ntap-sg-replica`. Esta marca evita que se forme un espejo en cascada. StorageGRID admite un CloudMirror bidireccional entre dos redes.

Eventos en el bucket de destino

No se garantiza la singularidad ni el orden de los eventos en el depósito de destino. Es posible que se entregue más de una copia idéntica de un objeto de origen al destino como resultado de las operaciones realizadas para garantizar el éxito de la entrega. En casos excepcionales, cuando el mismo objeto se actualiza simultáneamente desde dos o más sitios StorageGRID diferentes, el orden de las operaciones en el depósito de destino podría no coincidir con el orden de los eventos en el depósito de origen.

Comprender las notificaciones de los buckets

Puede habilitar la notificación de eventos para un bucket S3 si desea que StorageGRID envíe notificaciones sobre eventos específicos a un clúster de Kafka de destino o a Amazon Simple Notification Service.

Por ejemplo, puede configurar alertas para que se envíen a los administradores sobre cada objeto agregado a un depósito, donde los objetos representan archivos de registro asociados con un evento crítico del sistema.

Las notificaciones de eventos se crean en el depósito de origen según lo especificado en la configuración de notificación y se envían al destino. Si un evento asociado con un objeto tiene éxito, se crea una notificación sobre ese evento y se pone en cola para su entrega.

No se garantiza la singularidad ni el orden de las notificaciones. Es posible que se envíe más de una notificación de un evento al destino como resultado de las operaciones realizadas para garantizar el éxito de la entrega. Y debido a que la entrega es asíncrona, no se garantiza que el orden temporal de las notificaciones en el destino coincida con el orden de los eventos en el depósito de origen, en particular para las operaciones que se originan en diferentes sitios de StorageGRID. Puedes utilizar el `sequencer` Introduzca la clave en el mensaje de evento para determinar el orden de los eventos para un objeto en particular, como se describe en la documentación de Amazon S3.

Las notificaciones de eventos de StorageGRID siguen la API de Amazon S3 con algunas limitaciones.

- Se admiten los siguientes tipos de eventos:
 - `s3:ObjetoCreado`:
 - `s3:ObjetoCreado:Poner`
 - `s3:ObjetoCreado:Publicación`
 - `s3:ObjetoCreado:Copiar`
 - `s3:Objeto creado:Carga multiparte completa`
 - `s3:Objeto eliminado`:
 - `s3:ObjetoEliminado:Eliminar`

- s3:Objeto eliminado:Eliminar marcador creado
- s3:Restaurar objeto:Publicar
- Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar, pero no incluyen algunas claves y utilizan valores específicos para otras, como se muestra en la tabla:

Nombre de la clave	Valor de StorageGRID
Fuente del evento	sgws:s3
Región de AWS	<i>no incluido</i>
x-amz-id-2	<i>no incluido</i>
arn	urn:sgws:s3:::bucket_name

Comprender el servicio de integración de búsqueda

Puede habilitar la integración de búsqueda para un bucket S3 si desea utilizar un servicio de búsqueda y análisis de datos externo para los metadatos de sus objetos.

El servicio de integración de búsqueda es un servicio StorageGRID personalizado que envía de forma automática y asincrónica metadatos de objetos S3 a un punto final de destino cada vez que se crea o elimina un objeto, o se actualizan sus metadatos o etiquetas. Luego, puede utilizar herramientas sofisticadas de búsqueda, análisis de datos, visualización o aprendizaje automático proporcionadas por el servicio de destino para buscar, analizar y obtener información de los datos de sus objetos.

Por ejemplo, puede configurar sus depósitos para enviar metadatos de objetos S3 a un servicio Elasticsearch remoto. Luego, puede usar Elasticsearch para realizar búsquedas en diferentes grupos y realizar análisis sofisticados de patrones presentes en los metadatos de sus objetos.

Si bien la integración de Elasticsearch se puede configurar en un bucket con S3 Object Lock habilitado, los metadatos de S3 Object Lock (incluidos Conservar hasta la fecha y el estado de Retención legal) de los objetos no se incluirán en los metadatos enviados a Elasticsearch.



Debido a que el servicio de integración de búsqueda hace que se envíen metadatos de objetos a un destino, su XML de configuración se denomina "XML de configuración de notificación *metadata*". Este XML de configuración es diferente del "XML de configuración de notificación" utilizado para habilitar las notificaciones de *eventos*.

Integración de búsquedas y buckets S3

Puede habilitar el servicio de integración de búsqueda para cualquier depósito con o sin versión. La integración de búsqueda se configura asociando el XML de configuración de notificación de metadatos con el depósito que especifica sobre qué objetos actuar y el destino de los metadatos del objeto.

Las notificaciones de metadatos se generan en forma de un documento JSON cuyo nombre incluye el nombre del depósito, el nombre del objeto y el ID de la versión, si corresponde. 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 del usuario, StorageGRID pasa fechas y números a Elasticsearch como cadenas o como notificaciones de eventos S3. Para configurar Elasticsearch para que interprete estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para el mapeo de campos dinámicos y para el mapeo de formatos de fecha. Debe habilitar las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Una vez indexado un documento, no es posible editar los tipos de campos del documento en el índice.

Notificaciones de búsqueda

Las notificaciones de metadatos 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 de la operación de la política ILM de la red.
- Se agregan, actualizan o eliminan metadatos o etiquetas de objetos. Al actualizar, siempre se envía el conjunto completo de metadatos y etiquetas, no solo los valores modificados.

Después de agregar XML de configuración de notificación de metadatos a un bucket, se envían notificaciones para cualquier objeto nuevo que cree y para cualquier objeto que modifique actualizando sus datos, metadatos de usuario o etiquetas. Sin embargo, no se envían notificaciones para ningún objeto que ya estuviera en el depósito. Para garantizar que los metadatos de todos los objetos del depósito se envíen al destino, debe realizar una de las siguientes acciones:

- Configure el servicio de integración de búsqueda inmediatamente después de crear el depósito y antes de agregar cualquier objeto.
- Realice una acción en todos los objetos que ya se encuentran en el depósito que activará el envío de un mensaje de notificación de metadatos al destino.

Servicio de integración de búsqueda y Elasticsearch

El servicio de integración de búsqueda StorageGRID admite un clúster Elasticsearch como destino. Al igual que con los demás servicios de la plataforma, el destino se especifica en el punto final cuyo URN se utiliza en el XML de configuración para el servicio. Utilice el "[Herramienta de matriz de interoperabilidad de NetApp](#)" para determinar las versiones compatibles de Elasticsearch.

Administrar puntos finales de servicios de la plataforma

Configurar puntos finales de servicios de la plataforma

Antes de poder configurar un servicio de plataforma para un bucket, debe configurar al menos un punto final para que sea el destino del servicio de plataforma.

El acceso a los servicios de la plataforma lo habilita un administrador de StorageGRID por inquilino. Para crear o usar un punto final de servicios de plataforma, debe ser un usuario inquilino con permiso de acceso Administrar puntos finales o Raíz, en una red cuya red haya sido configurada para permitir que los nodos de almacenamiento accedan a recursos de puntos finales externos. Para un solo inquilino, puede configurar un máximo de 500 puntos finales de servicios de plataforma. Comuníquese con su administrador de StorageGRID para obtener más información.

¿Qué es un punto final de servicios de plataforma?

Un punto final de servicios de plataforma especifica la información que StorageGRID necesita para acceder al destino externo.

Por ejemplo, si desea replicar objetos de un bucket de StorageGRID a un bucket de Amazon S3, debe crear un punto final de servicios de plataforma que incluya la información y las credenciales que StorageGRID necesita para acceder al bucket de destino en Amazon.

Cada tipo de servicio de plataforma requiere su propio punto final, por lo que debe configurar al menos un punto final para cada servicio de plataforma que planea utilizar. Después de definir un punto final de servicios de plataforma, utilice el URN del punto final como destino en el XML de configuración utilizado para habilitar el servicio.

Puede utilizar el mismo punto final como destino para más de un depósito de origen. Por ejemplo, puede configurar varios depósitos de origen para enviar metadatos de objetos al mismo punto final de integración de búsqueda para poder realizar búsquedas en varios depósitos. También puede configurar un bucket de origen para usar más de un punto final como destino, lo que le permite hacer cosas como enviar notificaciones sobre la creación de objetos a un tema de Amazon Simple Notification Service (Amazon SNS) y notificaciones sobre la eliminación de objetos a un segundo tema de Amazon SNS.

Puntos finales para la replicación de CloudMirror

StorageGRID admite puntos finales de replicación que representan depósitos S3. Estos depósitos pueden estar alojados en Amazon Web Services, en el mismo StorageGRID o en una implementación remota del mismo, o en otro servicio.

Puntos finales para notificaciones

StorageGRID admite puntos finales de Amazon SNS y Kafka. No se admiten los puntos finales de Simple Queue Service (SQS) ni de AWS Lambda.

Para los puntos finales de Kafka, no se admite TLS mutuo. Como resultado, si tienes `ssl.client.auth` empezar a `required` en la configuración de su agente de Kafka, podría causar problemas de configuración del punto final de Kafka.

Puntos finales para el servicio de integración de búsqueda

StorageGRID admite puntos finales de integración de búsqueda que representan clústeres de Elasticsearch. Estos clústeres de Elasticsearch pueden estar en un centro de datos local o alojados en una nube de AWS o en otro lugar.

El punto final de integración de búsqueda hace referencia a un índice y tipo de Elasticsearch específicos. Debe crear el índice en Elasticsearch antes de crear el punto final en StorageGRID, de lo contrario la creación del punto final fallará. No es necesario crear el tipo antes de crear el punto final. StorageGRID creará el tipo si es necesario cuando envíe metadatos del objeto al punto final.

Información relacionada

["Administrar StorageGRID"](#)

Especificar URN para el punto final de los servicios de la plataforma

Cuando crea un punto final de servicios de plataforma, debe especificar un nombre de recurso único (URN). Utilizará la URN para hacer referencia al punto final cuando cree

un XML de configuración para el servicio de la plataforma. La URN de cada punto final debe ser única.

StorageGRID valida los puntos finales de los servicios de la plataforma a medida que los crea. Antes de crear un punto final de servicios de plataforma, confirme que el recurso especificado en el punto final exista y que se pueda acceder a él.

Elementos URN

El URN para un punto final de servicios de plataforma debe comenzar con `arn:aws` o `urn:mysite`, de la siguiente manera:

- 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 está alojado localmente, utilice `urn:mysite`

Por ejemplo, si está especificando el URN para un punto final de CloudMirror alojado en StorageGRID, el URN podría comenzar con `urn:sgws`.

El siguiente elemento de la URN especifica el tipo de servicio de plataforma, de la siguiente manera:

Servicio	Tipo
Replicación de CloudMirror	s3
Notificaciones	sns`o `kafka
Integración de búsqueda	es

Por ejemplo, para continuar especificando el URN para un punto final de CloudMirror alojado en StorageGRID, agregaría s3 Llegar `urn:sgws:s3`.

El elemento final de la URN identifica el recurso de destino específico en la URI de destino.

Servicio	Recurso específico
Replicación de CloudMirror	bucket-name
Notificaciones	sns-topic-name`o `kafka-topic-name
Integración de búsqueda	domain-name/index-name/type-name Nota: Si el clúster Elasticsearch no está configurado para crear índices automáticamente, debe crear el índice manualmente antes de crear el punto final.

URN para servicios alojados en AWS y GCP

Para las entidades de AWS y GCP, el URN completo es un ARN de AWS 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 punto final de integración de búsqueda de AWS, el `domain-name` debe incluir la cadena literal `domain/` , como se muestra aquí.

URN para servicios alojados localmente

Al utilizar servicios alojados localmente en lugar de servicios en la nube, puede especificar el URN de cualquier forma que cree un URN válido y único, siempre que el URN incluya los elementos requeridos 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 la URN sea única. Por ejemplo:

- Replicación de CloudMirror:

```
urn:mystore:s3:optional:optional:bucket-name
```

Para un punto final de CloudMirror alojado en StorageGRID, puede especificar un URN válido que comience con `urn:sgws:`

```
urn:sgws:s3:optional:optional:bucket-name
```

- Notificaciones:

Especifique un punto final de Amazon Simple Notification Service:

```
urn:mystore:sns:optional:optional:sns-topic-name
```

Especifique un punto final de Kafka:

```
urn:mysite:kafka:optional:optional:kafka-topic-name
```

- Integración de búsqueda:

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```



Para los puntos finales de integración de búsqueda alojados localmente, el `domain-name` El elemento puede ser cualquier cadena siempre que la URN del punto final sea única.

Crear punto final de servicios de plataforma

Debe crear al menos un punto final del tipo correcto antes de poder habilitar un servicio de plataforma.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Un administrador de StorageGRID habilitó los servicios de plataforma para su cuenta de inquilino.
- Pertenece a un grupo de usuarios que tiene la ["Administrar puntos finales o permisos de acceso raíz"](#).
- Se han creado los recursos a los que hace referencia el punto final de servicios de la plataforma:
 - Replicación de CloudMirror: depósito S3
 - Notificación de eventos: Amazon Simple Notification Service (Amazon SNS) o tema de Kafka
 - Notificación de búsqueda: índice de Elasticsearch, si el clúster de destino no está configurado para crear índices automáticamente.
- Tienes la información sobre el recurso de destino:
 - Host y puerto para el Identificador uniforme de recursos (URI)



Si planea utilizar un depósito alojado en un sistema StorageGRID como punto final para la replicación de CloudMirror, comuníquese con el administrador de la red para determinar los valores que debe ingresar.

- Nombre único de recurso (URN)

["Especificar URN para el punto final de los servicios de la plataforma"](#)

- Credenciales de autenticación (si es necesario):

Puntos finales de integración de búsqueda

Para los puntos finales de integración de búsqueda, puede utilizar las siguientes credenciales:

- Clave de acceso: ID de clave de acceso y clave de acceso secreta
- HTTP básico: Nombre de usuario y contraseña

Puntos finales de replicación de CloudMirror

Para los puntos finales de replicación de CloudMirror, puede utilizar las siguientes credenciales:

- Clave de acceso: ID de clave de acceso y clave de acceso secreta
- CAP (Portal de acceso C2S): URL de credenciales temporales, certificados de servidor y cliente, claves de cliente y una frase de contraseña de clave privada de cliente opcional.

Puntos finales de Amazon SNS

Para los puntos finales de Amazon SNS, puede utilizar las siguientes credenciales:

- Clave de acceso: ID de clave de acceso y clave de acceso secreta

Puntos finales de Kafka

Para los puntos finales de Kafka, puede utilizar las siguientes credenciales:

- SASL/PLAIN: Nombre de usuario y contraseña
- SASL/SCRAM-SHA-256: Nombre de usuario y contraseña
- SASL/SCRAM-SHA-512: Nombre de usuario y contraseña

- Certificado de seguridad (si se utiliza un certificado CA personalizado)

- Si las funciones de seguridad de Elasticsearch están habilitadas, tiene el privilegio de clúster de monitorización para realizar pruebas de conectividad y el privilegio de escritura de índice o los privilegios de índice y eliminación de índice para las actualizaciones de documentos.

Pasos

1. Seleccione **ALMACENAMIENTO (S3) > Puntos finales de servicios de plataforma**. Aparece la página de puntos finales de servicios de la plataforma.
2. Seleccione **Crear punto final**.
3. Ingrese un nombre para mostrar para describir brevemente el punto final y su propósito.

El tipo de servicio de plataforma que admite el punto final se muestra junto al nombre del punto final cuando aparece en la página Puntos finales, por lo que no es necesario incluir esa información en el nombre.

4. En el campo **URI**, especifique el Identificador único de recurso (URI) del punto final.

Utilice uno de los siguientes formatos:

```
https://host:port
http://host:port
```

Si no especifica un puerto, se utilizan los siguientes puertos predeterminados:

- Puerto 443 para URI HTTPS y puerto 80 para URI HTTP (la mayoría de los puntos finales)
- Puerto 9092 para HTTPS y URI HTTP (solo puntos finales de Kafka)

Por ejemplo, el URI de un depósito 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 punto final del balanceador 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 falla.

De manera similar, el URI de un bucket alojado en AWS podría ser:

```
https://s3-aws-region.amazonaws.com
```



Si el punto final se utiliza para el servicio de replicación CloudMirror, no incluya el nombre del depósito en la URI. Incluye el nombre del depósito en el campo **URN**.

5. Introduzca el nombre de recurso único (URN) para el punto final.



No se puede cambiar el URN de un punto final una vez creado el punto final.

6. Seleccione **Continuar**.

7. Seleccione un valor para **Tipo de autenticación**.

Puntos finales de integración de búsqueda

Ingresa o cargue las credenciales para un punto final de integración de búsqueda.

Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Cartas credenciales
Anónimo	Proporciona acceso anónimo al destino. Sólo funciona para puntos finales que tienen la seguridad deshabilitada.	Sin autenticación.
Tecla de acceso	Utiliza credenciales de estilo AWS para autenticar las 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 • Password

Puntos finales de replicación de CloudMirror

Ingresa o cargue las credenciales para un punto final de replicación de CloudMirror.

Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Cartas credenciales
Anónimo	Proporciona acceso anónimo al destino. Sólo funciona para puntos finales que tienen la seguridad deshabilitada.	Sin autenticación.
Tecla de acceso	Utiliza credenciales de estilo AWS para autenticar las conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta

Tipo de autenticación	Descripción	Cartas credenciales
CAP (Portal de acceso C2S)	Utiliza certificados y claves para autenticar las conexiones al destino.	• URL de credenciales temporales • Certificado de CA del servidor (carga de archivo PEM) • Certificado de cliente (carga de archivo PEM) • Clave privada del cliente (carga de archivo PEM, formato cifrado OpenSSL o formato de clave privada sin cifrar) • Frase de contraseña de la clave privada del cliente (opcional)

Puntos finales de Amazon SNS

Ingrese o cargue las credenciales para un punto final de Amazon SNS.

Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Cartas credenciales
Anónimo	Proporciona acceso anónimo al destino. Sólo funciona para puntos finales que tienen la seguridad deshabilitada.	Sin autenticación.
Tecla de acceso	Utiliza credenciales de estilo AWS para autenticar las conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta

Puntos finales de Kafka

Ingrese o cargue las credenciales para un punto final de Kafka.

Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Cartas credenciales
Anónimo	Proporciona acceso anónimo al destino. Sólo funciona para puntos finales que tienen la seguridad deshabilitada.	Sin autenticación.
SASL/LLANO	Utiliza un nombre de usuario y una contraseña con texto sin formato para autenticar las conexiones al destino.	• Nombre de usuario • Password

Tipo de autenticación	Descripción	Cartas credenciales
SASL/SCRAM-SHA-256	Utiliza un nombre de usuario y una contraseña mediante un protocolo de desafío-respuesta y hash SHA-256 para autenticar las conexiones al destino.	• Nombre de usuario • Password
SASL/SCRAM-SHA-512	Utiliza un nombre de usuario y una contraseña mediante un protocolo de desafío-respuesta y hash SHA-512 para autenticar las conexiones al destino.	• Nombre de usuario • Password

Seleccione **Usar autenticación mediante delegación** si el nombre de usuario y la contraseña se derivan de un token de delegación obtenido de un clúster de Kafka.

8. Seleccione **Continuar**.

9. Seleccione un botón de opción para **Verificar servidor** para elegir cómo se verifica la conexión TLS al punto final.

Tipo de verificación del certificado	Descripción
Utilice un certificado CA personalizado	Utilice un certificado de seguridad personalizado. Si selecciona esta configuración, copie y pegue el certificado de seguridad personalizado en el cuadro de texto Certificado CA .
Utilice el certificado CA del sistema operativo	Utilice el certificado CA de Grid predeterminado instalado en el sistema operativo para proteger las conexiones.
No verificar el certificado	El certificado utilizado para la conexión TLS no está verificado. Esta opción no es segura.

10. Seleccione **Probar y crear punto final**.

- Aparece un mensaje de éxito si se puede acceder al punto final utilizando las credenciales especificadas. La conexión al punto final se valida desde un nodo en cada sitio.
- Aparece un mensaje de error si falla la validación del punto final. Si necesita modificar el punto final para corregir el error, seleccione **Regresar a los detalles del punto final** y actualice la información. Luego, seleccione **Probar y crear punto final**.



La creación de puntos finales falla si los servicios de la plataforma no están habilitados para su cuenta de inquilino. Comuníquese con su administrador de StorageGRID .

Después de haber configurado un punto final, puede usar su URN para configurar un servicio de plataforma.

Información relacionada

- "Especificar URN para el punto final de los servicios de la plataforma"
- "Configurar la replicación de CloudMirror"
- "Configurar notificaciones de eventos"
- "Configurar el servicio de integración de búsqueda"

Conexión de prueba para el punto final de servicios de la plataforma

Si la conexión a un servicio de la plataforma ha cambiado, puede probar la conexión del punto final para validar que el recurso de destino existe y que se puede acceder a él utilizando las credenciales que especificó.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene la ["Administrar puntos finales o permisos de acceso raíz"](#).

Acerca de esta tarea

StorageGRID no valida que las credenciales tengan los permisos correctos.

Pasos

1. Seleccione **ALMACENAMIENTO (S3) > Puntos finales de servicios de plataforma**.

Aparece la página Puntos finales de servicios de la plataforma y muestra la lista de puntos finales de servicios de la plataforma que ya se han configurado.

2. Seleccione el punto final cuya conexión desea probar.

Aparece la página de detalles del punto final.

3. Seleccione **Probar conexión**.

- Aparece un mensaje de éxito si se puede acceder al punto final utilizando las credenciales especificadas. La conexión al punto final se valida desde un nodo en cada sitio.
- Aparece un mensaje de error si falla la validación del punto final. Si necesita modificar el punto final para corregir el error, seleccione **Configuración** y actualice la información. Luego, seleccione **Probar y guardar cambios**.

Editar el punto final de los servicios de la plataforma

Puede editar la configuración de un punto final de servicios de la plataforma para cambiar su nombre, URI u otros detalles. Por ejemplo, es posible que necesite actualizar credenciales vencidas o cambiar la URI para que apunte a un índice de Elasticsearch de respaldo para conmutación por error. No se puede cambiar el URN de un punto final de servicios de plataforma.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene la ["Administrar puntos finales o permisos de acceso raíz"](#).

Pasos

1. Seleccione **ALMACENAMIENTO (S3) > Puntos finales de servicios de plataforma.**

Aparece la página Puntos finales de servicios de la plataforma y muestra la lista de puntos finales de servicios de la plataforma que ya se han configurado.

2. Seleccione el punto final que desea editar.

Aparece la página de detalles del punto final.

3. Seleccione **Configuración.**

4. Según sea necesario, cambie la configuración del punto final.



No se puede cambiar el URN de un punto final una vez creado el punto final.

a. Para cambiar el nombre para mostrar del punto final, seleccione el ícono de edición .

b. Según sea necesario, cambie la 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 una nueva ID de clave de acceso y una clave de acceso secreta. Si necesita cancelar sus cambios, seleccione **Revertir edición de clave S3**.
- Para la autenticación CAP (Portal de acceso C2S), 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 clave según sea necesario.



La clave privada del cliente debe estar en formato cifrado OpenSSL o en formato de clave privada sin cifrar.

d. Según sea necesario, cambie el método para verificar el servidor.

5. Seleccione **Probar y guardar cambios.**

- Aparece un mensaje de éxito si se puede acceder al punto final utilizando las credenciales especificadas. La conexión al punto final se verifica desde un nodo en cada sitio.
- Aparece un mensaje de error si falla la validación del punto final. Modifique el punto final para corregir el error y luego seleccione **Probar y guardar cambios.**

Eliminar el punto final de los servicios de la plataforma

Puede eliminar un punto final si ya no desea utilizar el servicio de plataforma asociado.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene la ["Administrar puntos finales o permisos de acceso raíz"](#).

Pasos

1. Seleccione **ALMACENAMIENTO (S3) > Puntos finales de servicios de plataforma.**

Aparece la página Puntos finales de servicios de la plataforma y muestra la lista de puntos finales de servicios de la plataforma que ya se han configurado.

2. Seleccione la casilla de verificación para cada punto final que desee eliminar.



Si elimina un punto final de servicios de plataforma que está en uso, el servicio de plataforma asociado se deshabilitará para cualquier depósito que use el punto final. Cualquier solicitud que aún no se haya completado será descartada. Se seguirán generando nuevas solicitudes hasta que usted cambie la configuración de su depósito para que ya no haga referencia al URN eliminado. StorageGRID informará estas solicitudes como errores irrecuperables.

3. Seleccione **Acciones > Eliminar punto final**.

Aparece un mensaje de confirmación.

4. Seleccione **Eliminar punto final**.

Solucionar errores de puntos finales de servicios de la plataforma

Si se produce un error cuando StorageGRID intenta comunicarse con un punto final de servicios de la plataforma, se muestra un mensaje en el panel. En la página de puntos finales de servicios de la plataforma, la columna **Último error** indica cuánto tiempo hace que ocurrió el error. No se muestra ningún error si los permisos asociados con las credenciales de un punto final son incorrectos.

Determinar si se ha producido un error

Si se produjo algún error en los puntos finales de los servicios de la plataforma en los últimos 7 días, el panel del Administrador de inquilinos muestra un mensaje de alerta. Puede ir a la página de puntos finales de servicios de la plataforma para ver más detalles sobre el error.



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.

El mismo error que aparece en el panel también aparece en la parte superior de la página de puntos finales de los servicios de la plataforma. Para ver un mensaje de error más detallado:

Pasos

1. De la lista de puntos finales, seleccione el punto final que tiene el error.
2. En la página de detalles del punto final, seleccione **Conexión**. Esta pestaña muestra solo el error más reciente de un punto final e indica cuánto tiempo hace que ocurrió el error. Errores que incluyen el icono X rojo  ocurrió dentro de los últimos 7 días.

Comprobar si el error sigue vigente

Es posible que algunos errores sigan apareciendo en la columna **Último error** incluso después de que se hayan resuelto. Para ver si hay un error actual o para forzar la eliminación de un error resuelto de la tabla:

Pasos

1. Seleccione el punto final.

Aparece la página de detalles del punto final.
2. Seleccione **Conexión > Probar conexión**.

Al seleccionar **Probar conexión**, StorageGRID valida que el punto final de servicios de la plataforma existe y que se puede acceder a él con las credenciales actuales. La conexión al punto final se valida desde un nodo en cada sitio.

Resolver errores de puntos finales

Puede utilizar el mensaje **Último error** en la página de detalles del punto final para ayudar a determinar qué está causando el error. Algunos errores podrían requerir que edite el punto final para resolver el problema. Por ejemplo, puede ocurrir un error de CloudMirroring si StorageGRID no puede acceder al bucket S3 de destino porque no tiene los permisos de acceso correctos o la clave de acceso ha expirado. El mensaje es "Es necesario actualizar las credenciales del punto final o el acceso al destino" y los detalles son "Acceso denegado" o "InvalidAccessKeyId".

Si necesita editar el punto final para resolver un error, seleccionar **Probar y guardar cambios** hace que StorageGRID valide el punto final actualizado y confirme que se puede acceder a él con las credenciales actuales. La conexión al punto final se valida desde un nodo en cada sitio.

Pasos

1. Seleccione el punto final.
2. En la página de detalles del punto final, seleccione **Configuración**.
3. Edite la configuración del punto final según sea necesario.
4. Seleccione **Conexión > Probar conexión**.

Credenciales de punto final con permisos insuficientes

Cuando StorageGRID valida un punto final de servicios de plataforma, confirma que las credenciales del punto final se pueden usar para contactar al recurso de destino y realiza una verificación de permisos básica. Sin embargo, StorageGRID no valida todos los permisos necesarios para ciertas operaciones de servicios de la plataforma. Por este motivo, si recibe un error al intentar utilizar un servicio de la plataforma (como "403 Prohibido"), verifique los permisos asociados con las credenciales del punto final.

Información relacionada

- [Administrar StorageGRID > Solucionar problemas de servicios de la plataforma](#)
- ["Crear punto final de servicios de plataforma"](#)
- ["Conexión de prueba para el punto final de servicios de la plataforma"](#)
- ["Editar el punto final de los servicios de la plataforma"](#)

Configurar la replicación de CloudMirror

Para habilitar la replicación de CloudMirror para un depósito, debe crear y aplicar un XML de configuración de replicación de depósito válido.

Antes de empezar

- Un administrador de StorageGRID habilitó los servicios de plataforma para su cuenta de inquilino.
- Ya ha creado un depósito para que actúe como fuente de replicación.
- El punto final que desea utilizar como destino para la replicación de CloudMirror ya existe y tiene su URN.
- Pertenece a un grupo de usuarios que tiene la ["Administrar todos los depósitos o permisos de acceso raíz"](#). Estos permisos anulan las configuraciones de permisos en las políticas de grupo o de depósito cuando se configura el depósito mediante el Administrador de inquilinos.

Acerca de esta tarea

La replicación de CloudMirror copia objetos de un depósito de origen a un depósito de destino que se especifica en un punto final.

Para obtener información general sobre la replicación de buckets y cómo configurarla, consulte ["Documentación de Amazon Simple Storage Service \(S3\): Replicación de objetos"](#) . Para obtener información sobre cómo StorageGRID implementa GetBucketReplication, DeleteBucketReplication y PutBucketReplication, consulte la ["Operaciones en buckets"](#) .



La replicación de CloudMirror tiene similitudes y diferencias importantes con la función de replicación entre redes. Para obtener más información, consulte ["Comparar la replicación entre redes y la replicación de CloudMirror"](#) .

Tenga en cuenta los siguientes requisitos y características al configurar la replicación de CloudMirror:

- Cuando crea y aplica un XML de configuración de replicación de bucket válido, debe utilizar el URN de un punto final de bucket S3 para cada destino.
- La replicación no es compatible con los depósitos de origen o destino que tengan el bloqueo de objetos S3 habilitado.
- Si habilita la replicación de CloudMirror en un depósito que contiene objetos, los objetos nuevos agregados al depósito se replican, pero los objetos existentes en el depósito no se replican. Debe actualizar los objetos existentes para activar la replicación.
- Si especifica una clase de almacenamiento en el XML de configuración de replicación, StorageGRID utiliza esa clase al realizar operaciones contra el punto final S3 de destino. El punto final de destino también debe admitir la clase de almacenamiento especificada. Asegúrese de seguir todas las recomendaciones proporcionadas por el proveedor del sistema de destino.

Pasos

1. Habilite la replicación para su depósito de origen:

- Utilice un editor de texto para crear el XML de configuración de replicación necesario para habilitar la replicación, como se especifica en la API de replicación S3.
- Al configurar el XML:
 - Tenga en cuenta que StorageGRID solo admite la versión 1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso de `Filter` elemento para reglas y sigue las convenciones V1 para la eliminación de versiones de objetos. Consulte la documentación de Amazon sobre la configuración de replicación para obtener más detalles.
 - Utilice la URN de un punto final del bucket S3 como destino.
 - Opcionalmente agregue el `<StorageClass>` elemento y especifique uno de los siguientes:
 - `STANDARD`: La clase de almacenamiento predeterminada. Si no especifica una clase de almacenamiento cuando carga un objeto, el `STANDARD` Se utiliza la clase de almacenamiento.
 - `STANDARD_IA`: (Estándar - acceso poco frecuente). Utilice esta clase de almacenamiento para datos a los que se accede con menos frecuencia, pero que aún requieren 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 la `STANDARD` clase de almacenamiento.
 - Si especifica un `Role` En el XML de configuración se ignorará. StorageGRID no utiliza este valor.

```
<ReplicationConfiguration>
  <Role></Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>2020</Prefix>
    <Destination>
      <Bucket>urn:sgws:s3:::2017-records</Bucket>
      <StorageClass>STANDARD</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

2. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Depósitos**.
3. Seleccione el nombre del depósito de origen.

Aparece la página de detalles del depósito.

4. Seleccione **Servicios de plataforma > Replicación**.
5. Seleccione la casilla de verificación **Habilitar replicación**.
6. Pegue el XML de configuración de replicación en el cuadro de texto y seleccione **Guardar cambios**.



Los servicios de la plataforma deben ser habilitados para cada cuenta de inquilino por un administrador de StorageGRID mediante Grid Manager o Grid Management API. Comuníquese con su administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Verifique que la replicación esté configurada correctamente:
 - a. Agregue un objeto al depósito de origen que cumpla con los requisitos de replicación según lo especificado en la configuración de replicación.

En el ejemplo mostrado anteriormente, se replican los objetos que coinciden con el prefijo "2020".

- b. Confirme que el objeto se haya replicado en el depósito de destino.

Para objetos pequeños, la replicación ocurre rápidamente.

Información relacionada

["Crear punto final de servicios de plataforma"](#)

Configurar notificaciones de eventos

Puede habilitar las notificaciones para un depósito creando un XML de configuración de notificaciones y utilizando el Administrador de inquilinos para aplicar el XML a un depósito.

Antes de empezar

- Un administrador de StorageGRID habilitó los servicios de plataforma para su cuenta de inquilino.

- Ya has creado un depósito que actuará como fuente de notificaciones.
- El punto final que desea utilizar como destino para las notificaciones de eventos ya existe y tiene su URN.
- Pertenece a un grupo de usuarios que tiene la ["Administrar todos los depósitos o permisos de acceso raíz"](#) . Estos permisos anulan las configuraciones de permisos en las políticas de grupo o de depósito cuando se configura el depósito mediante el Administrador de inquilinos.

Acerca de esta tarea

Puede configurar las notificaciones de eventos asociando el XML de configuración de notificaciones con un depósito de origen. El XML de configuración de notificaciones sigue las convenciones S3 para configurar notificaciones de bucket, con el tema de destino de Kafka o Amazon SNS especificado como el URN de un punto final.

Para obtener información general sobre las notificaciones de eventos y cómo configurarlas, consulte la ["Documentación de Amazon"](#) . Para obtener información sobre cómo StorageGRID implementa la API de configuración de notificaciones de bucket S3, consulte ["Instrucciones para implementar aplicaciones cliente S3"](#) .

Tenga en cuenta los siguientes requisitos y características al configurar las notificaciones de eventos para un bucket:

- Cuando crea y aplica un XML de configuración de notificación válido, debe utilizar el URN de un punto final de notificaciones de eventos para cada destino.
- Si bien la notificación de eventos se puede configurar en un bucket con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos S3 (incluidos la fecha de retención y el estado de retención legal) de los objetos no se incluirán en los mensajes de notificación.
- Después de configurar las notificaciones de eventos, cada vez que ocurre un evento específico para un objeto en el bucket de origen, se genera una notificación y se envía al tema de Amazon SNS o Kafka utilizado como punto final de destino.
- Si habilita las notificaciones de eventos para un depósito que contiene objetos, las notificaciones se envían solo para las acciones que se realizan después de guardar la configuración de notificación.

Pasos

1. Habilitar notificaciones para su depósito de origen:
 - Utilice un editor de texto para crear el XML de configuración de notificación necesario para habilitar las notificaciones de eventos, como se especifica en la API de notificación S3.
 - Al configurar el XML, utilice la URN de un punto final 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) > Cubos**.

3. Seleccione el nombre del depósito de origen.

Aparece la página de detalles del depósito.

4. Seleccione **Servicios de plataforma > Notificaciones de eventos**.

5. Seleccione la casilla de verificación **Habilitar notificaciones de eventos**.

6. Pegue el XML de configuración de notificación en el cuadro de texto y seleccione **Guardar cambios**.



Los servicios de la plataforma deben ser habilitados para cada cuenta de inquilino por un administrador de StorageGRID mediante Grid Manager o Grid Management API. Comuníquese con su administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Verifique que las notificaciones de eventos estén configuradas correctamente:

- a. Realizar una acción en un objeto en el depósito de origen que cumpla con los requisitos para activar una notificación según lo 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 enviado una notificación al tema de destino de Amazon SNS o Kafka.

Por ejemplo, si el tema de destino está alojado en Amazon SNS, puede configurar el servicio para que le envíe un correo electrónico cuando se entregue la notificación.

```

{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "arn": "arn:sgws:s3:::test1"
        },
        "object": {
          "key": "images/cat.jpg",
          "size": 0,
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",
          "sequencer": "14D90402421461C7"
        }
      }
    }
  ]
}

```

+

Si la notificación se recibe en el tema de destino, ha configurado correctamente su depósito de origen para las notificaciones de StorageGRID .

Información relacionada

["Comprender las notificaciones de los buckets"](#)

["Utilice la API REST de S3"](#)

Configurar el servicio de integración de búsqueda

Puede habilitar la integración de búsqueda para un depósito creando un XML de integración de búsqueda y utilizando el Administrador de inquilinos para aplicar el XML al depósito.

Antes de empezar

- Un administrador de StorageGRID habilitó los servicios de plataforma para su cuenta de inquilino.
- Ya ha creado un bucket S3 cuyo contenido desea indexar.
- El punto final que desea utilizar como destino para el servicio de integración de búsqueda ya existe y tiene su URN.
- Pertenece a un grupo de usuarios que tiene la ["Administrar todos los depósitos o permisos de acceso raíz"](#). Estos permisos anulan las configuraciones de permisos en las políticas de grupo o de depósito cuando se configura el depósito mediante el Administrador de inquilinos.

Acerca de esta tarea

Después de configurar el servicio de integración de búsqueda para un depósito de origen, la creación de un objeto o la actualización de los metadatos o las etiquetas de un objeto activa el envío de metadatos del objeto al punto final de destino.

Si habilita el servicio de integración de búsqueda para un depósito que ya contiene objetos, las notificaciones de metadatos no se envían automáticamente para los objetos existentes. Actualice estos objetos existentes para garantizar que sus metadatos se agreguen al índice de búsqueda de destino.

Pasos

1. Habilitar la integración de búsqueda para un depósito:

- Utilice un editor de texto para crear el XML de notificación de metadatos necesario para habilitar la integración de búsqueda.
- Al configurar el XML, utilice la URN de un punto final de integración de búsqueda como destino.

Los objetos se pueden filtrar según el prefijo del nombre del objeto. Por ejemplo, podría enviar metadatos para objetos con el prefijo `images` a un destino y metadatos para 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.

Según sea necesario, consulte la [Ejemplos para la configuración de metadatos XML](#).

```

<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>/Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Elementos en el XML de configuración de notificación de metadatos:

Nombre	Descripción	Requerido
Configuración de notificación de metadatos	Etiqueta contenedora para reglas utilizadas para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o más elementos de regla.	Sí
Regla	Etiqueta contenedora para una regla que identifica los objetos cuyos metadatos deben agregarse a un índice específico. Se rechazan las reglas con prefijos superpuestos. Incluido en el elemento MetadataNotificationConfiguration.	Sí
IDENTIFICACIÓN	Identificador único de la regla. Incluido en el elemento Regla.	No
Estado	El estado puede ser 'Habilitado' o 'Deshabilitado'. No se realiza ninguna acción para las reglas que están deshabilitadas. 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 que coincida con 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	Requerido
Urna	URN del destino donde se envían los metadatos del objeto. Debe ser la URN de un punto final de StorageGRID con las siguientes propiedades: • `es` Debe ser el tercer elemento. • La URN debe terminar con el índice y tipo donde se almacenan los metadatos, en el formato <code>domain-name/myindex/mytype</code>. Los puntos finales se configuran mediante el Administrador de inquilinos o la API de administración de inquilinos. Toman la siguiente forma: • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> El punto final debe configurarse antes de enviar el XML de configuración; de lo contrario, la configuración fallará con un error 404. URN está incluido en el elemento Destino.	Sí

- En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3) > Cubos**.
 - Seleccione el nombre del depósito de origen.
- Aparece la página de detalles del depósito.
- Seleccione **Servicios de plataforma > Integración de búsqueda**
 - Seleccione la casilla de verificación **Habilitar integración de búsqueda**.
 - Pegue la configuración de notificación de metadatos en el cuadro de texto y seleccione **Guardar cambios**.



Los servicios de plataforma deben ser habilitados para cada cuenta de inquilino por un administrador de StorageGRID mediante Grid Manager o la API de administración. Comuníquese con su administrador de StorageGRID si se produce un error al guardar el XML de configuración.

- Verifique que el servicio de integración de búsqueda esté configurado correctamente:
 - Agregue un objeto al depósito de origen que cumpla con los requisitos para activar una notificación de metadatos según lo especificado en el XML de configuración.

En el ejemplo mostrado anteriormente, todos los objetos agregados al depósito activan una notificación de metadatos.

 - Confirme que se agregó un documento JSON que contiene los metadatos y las etiquetas del objeto al índice de búsqueda especificado en el punto final.

Después de terminar

Según sea necesario, puede deshabilitar la integración de búsqueda para un depósito utilizando cualquiera de los siguientes métodos:

- Seleccione **ALMACENAMIENTO (S3) > Cubos** y desmarque la casilla **Habilitar integración de búsqueda**.
- Si está utilizando la API S3 directamente, utilice una solicitud de notificación de metadatos de DELETE Bucket. Consulte las instrucciones para implementar aplicaciones cliente S3.

Ejemplo: Configuración de notificación de metadatos que se aplica a todos los objetos

En este ejemplo, los metadatos 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>
```

Ejemplo: Configuración de notificación 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 del objeto para 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-1:33333333: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>

```

Formato de notificación de metadatos

Cuando habilita el servicio de integración de búsqueda para un depósito, se genera un documento JSON y se envía al punto final de destino cada vez que se agregan, actualizan o eliminan metadatos o etiquetas de objeto.

Este ejemplo muestra un ejemplo del JSON que podría generarse cuando un objeto con la clave SGWS/Tagging.txt se crea en un depósito llamado test . El test El bucket no tiene versión, por lo que 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"
  }
}
```

Campos incluidos en el documento JSON

El nombre del documento incluye el nombre del depósito, el nombre del objeto y el ID de la versión, si está presente.

Información de depósito y objeto

bucket: Nombre del bucket

key: Nombre de la clave del objeto

versionID: Versión del objeto, para objetos en depósitos versionados

region: Región del cubo, por ejemplo us-east-1

Metadatos del sistema

size: Tamaño del objeto (en bytes) tal como lo ve un cliente HTTP

md5: Hash de objeto

Metadatos del usuario

metadata: Todos los metadatos del usuario para el objeto, como pares clave-valor

key: value

Etiquetas

tags: Todas las etiquetas de objeto definidas para el objeto, como pares clave-valor

key: value

Cómo ver resultados en Elasticsearch

Para las etiquetas y los metadatos del usuario, StorageGRID pasa fechas y números a Elasticsearch como

cadena o como notificaciones de eventos S3. Para configurar Elasticsearch para que interprete estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para el mapeo de campos dinámicos y para el mapeo de formatos de fecha. Habilite las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Una vez indexado un documento, no es posible editar los tipos de campos del documento en el índice.

Utilice la API REST de S3

Versiones y actualizaciones compatibles con la API REST de S3

StorageGRID admite la API del Servicio de almacenamiento simple (S3), que se implementa como un conjunto de servicios web de transferencia de estado representacional (REST).

La compatibilidad con la API REST de S3 le permite conectar aplicaciones orientadas a servicios desarrolladas para servicios web de S3 con almacenamiento de objetos local que utiliza el sistema StorageGRID . Se requieren cambios mínimos en el uso actual de las llamadas API REST de S3 de una aplicación cliente.

Versiones compatibles

StorageGRID admite las siguientes versiones específicas de S3 y HTTP.

Artículo	Versión
Especificación de la API de S3	"Documentación de Amazon Web Services (AWS): Referencia de la API de Amazon Simple Storage Service"
HTTP	1,1 Para obtener más información sobre HTTP, consulte HTTP/1.1 (RFC 7230-35). "IETF RFC 2616: Protocolo de transferencia de hipertexto (HTTP/1.1)" Nota: StorageGRID no admite la canalización HTTP/1.1.

Actualizaciones de la compatibilidad con la API REST de S3

Liberar	Comentarios
11,9	• Se agregó soporte para valores de suma de comprobación SHA-256 precalculados para las siguientes solicitudes y encabezados admitidos. Puede utilizar esta función para verificar la integridad de los objetos cargados: ◦ Carga completa de varias partes: <code>x-amz-checksum-sha256</code> ◦ Crear carga múltiple: <code>x-amz-checksum-algorithm</code> ◦ Obtener objeto: <code>x-amz-checksum-mode</code> ◦ Objeto principal: <code>x-amz-checksum-mode</code> ◦ Lista de partes ◦ PonerObjeto: <code>x-amz-checksum-sha256</code> ◦ Subir parte: <code>x-amz-checksum-sha256</code> • Se agregó la capacidad para que el administrador de la red controle la retención a nivel de inquilino y las configuraciones de cumplimiento. Estas configuraciones afectan la configuración de bloqueo de objetos S3. ◦ Modo de retención predeterminado del depósito y modo de retención de objetos: Gobernanza o Cumplimiento, si lo permite el administrador de la red. ◦ Período de retención predeterminado del depósito y objeto Conservar hasta fecha: debe ser menor o igual a lo permitido por el período de retención máximo establecido por el administrador de la red. • Soporte mejorado para <code>aws-chunked</code> codificación y transmisión de contenido <code>x-amz-content-sha256</code> valores. Limitaciones: ◦ Si está presente, <code>chunk-signature</code> es opcional y no validado ◦ Si está presente, <code>x-amz-trailer</code> el contenido se ignora
11,8	Se actualizaron los nombres de las operaciones de S3 para que coincidan con los nombres utilizados en el "Documentación de Amazon Web Services (AWS): Referencia de la API de Amazon Simple Storage Service" .
11,7	• Agregado "Referencia rápida: solicitudes de API de S3 compatibles" . • Se agregó soporte para usar el modo GOBERNANCIA con S3 Object Lock. • Se agregó soporte para StorageGRID específico <code>x-ntap-sg-cgr-replication-status</code> encabezado de respuesta para solicitudes de objeto GET y objeto HEAD. Este encabezado proporciona el estado de replicación de un objeto para la replicación entre redes. • Las solicitudes <code>SelectObjectContent</code> ahora admiten objetos Parquet.

Liberar	Comentarios
11,6	• Se agregó soporte para el uso de <code>partNumber</code> parámetro de solicitud en solicitudes de objeto GET y objeto HEAD. • Se agregó soporte para un modo de retención predeterminado y un período de retención predeterminado a nivel de depósito para S3 Object Lock. • Se agregó soporte para el <code>s3:object-lock-remaining-retention-days</code> Clave de condición de política para establecer el rango de períodos de retención permitidos para sus objetos. • Se cambió el tamaño máximo <i>recomendado</i> para una sola operación de objeto PUT a 5 GiB (5.368.709.120 bytes). Si tiene objetos de más de 5 GiB, utilice la carga multiparte en su lugar.
11,5	• Se agregó soporte para administrar el cifrado de bucket. • Se agregó soporte para S3 Object Lock y solicitudes de cumplimiento heredadas obsoletas. • Se agregó soporte para usar DELETE Multiple Objects en depósitos versionados. • El <code>Content-MD5</code> El encabezado de solicitud ahora se admite correctamente.
11,4	• Se agregó soporte para etiquetado de depósito DELETE, etiquetado de depósito GET y etiquetado de depósito PUT. No se admiten etiquetas de asignación de costos. • Para los depósitos creados en StorageGRID 11.4, ya no es necesario restringir los nombres de claves de objeto para cumplir con las mejores prácticas de rendimiento. • Se agregó soporte para notificaciones de depósito en el <code>s3:ObjectRestore:Post</code> tipo de evento. • Ahora se aplican los límites de tamaño de AWS para partes multiparte. Cada parte de una carga multiparte debe tener entre 5 MiB y 5 GiB. La última parte puede ser menor a 5 MiB. • Se agregó soporte para TLS 1.3
11,3	• Se agregó soporte para el cifrado del lado del servidor de datos de objetos con claves proporcionadas por el cliente (SSE-C). • Se agregó soporte para operaciones de ciclo de vida de bucket DELETE, GET y PUT (solo acción de vencimiento) y para <code>x-amz-expiration</code> encabezado de respuesta. • Se actualizaron Objeto PUT, Objeto PUT - Copiar y Carga multiparte para describir el impacto de las reglas ILM que utilizan la ubicación sincrónica en la ingesta. • Los cifrados TLS 1.1 ya no son compatibles.

Liberar	Comentarios
11,2	Se agregó soporte para la restauración de objetos POST para su uso con grupos de almacenamiento en la nube. Se agregó soporte para usar la sintaxis de AWS para ARN, claves de condición de política y variables de política en políticas de grupo y de depósito. Las políticas de grupo y de depósito existentes que utilizan la sintaxis StorageGRID seguirán siendo compatibles. Nota: Los usos de ARN/URN en otras configuraciones JSON/XML, incluidas aquellas utilizadas en funciones personalizadas de StorageGRID , no han cambiado.
11,1	Se agregó soporte para compartir recursos de origen cruzado (CORS), HTTP para conexiones de cliente S3 a nodos de la red y configuraciones de cumplimiento en los buckets.
11,0	Se agregó soporte para configurar servicios de plataforma (replicación de CloudMirror, notificaciones e integración de búsqueda de Elasticsearch) para depósitos. También se agregó soporte para restricciones de ubicación de etiquetado de objetos para depósitos y la consistencia disponible.
10,4	Se agregó soporte para cambios de escaneo ILM en versiones, actualizaciones de la página Nombres de dominio de puntos finales, condiciones y variables en políticas, ejemplos de políticas y el permiso PutOverwriteObject.
10,3	Se agregó soporte para control de versiones.
10,2	Se agregó soporte para políticas de acceso a grupos y buckets, y para copia multiparte (Cargar parte - Copiar).
10,1	Se agregó soporte para carga de varias partes, solicitudes de estilo alojado virtual y autenticación v4.
10,0	Soporte inicial de la API REST S3 por parte del sistema StorageGRID . La versión actualmente compatible de la <i>Referencia de API de servicio de almacenamiento simple</i> es 2006-03-01.

Referencia rápida: solicitudes de API de S3 compatibles

Esta página resume cómo StorageGRID admite las API de Amazon Simple Storage Service (S3).

Esta página incluye solo las operaciones S3 compatibles con StorageGRID.



Para ver la documentación de AWS para cada operación, seleccione el enlace en el encabezado.

Parámetros de consulta URI comunes y encabezados de solicitud

A menos que se indique lo contrario, se admiten los siguientes parámetros de consulta URI comunes:

- `versionId`(según sea necesario para las operaciones de objetos)

A menos que se indique lo contrario, se admiten los siguientes encabezados de solicitud comunes:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Información relacionada

- ["Detalles de implementación de la API REST de S3"](#)
- ["Referencia de la API de Amazon Simple Storage Service: encabezados de solicitud comunes"](#)

"AbortarMultipartUpload"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud, más este parámetro de consulta URI adicional:

- `uploadId`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones para cargas multiparte"](#)

"Carga completa de varias partes"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud, más este parámetro de consulta URI adicional:

- `uploadId`
- `x-amz-checksum-sha256`

Etiquetas XML del cuerpo de la solicitud

StorageGRID admite estas etiquetas XML del cuerpo de solicitud:

- `ChecksumSHA256`
- `CompleteMultipartUpload`

- ETag
- Part
- PartNumber

Documentación de StorageGRID

"Carga completa de varias partes"

"Copiar objeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) Para esta solicitud, más estos encabezados adicionales:

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-metadata-directive
- x-amz-object-lock-legal-hold
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-storage-class
- x-amz-tagging
- x-amz-tagging-directive
- x-amz-meta-`<metadata-name>`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Copiar objeto"

"Crear cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) Para esta solicitud, más estos encabezados adicionales:

- x-amz-bucket-object-lock-enabled

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Crear carga de varias partes"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) Para esta solicitud, más estos encabezados adicionales:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-algorithm
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Crear carga de varias partes"](#)

"Eliminar cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Documentación de StorageGRID

["Operaciones en buckets"](#)

"EliminarBucketCors"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Eliminar cifrado del cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Eliminar ciclo de vida del cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

- ["Operaciones en buckets"](#)
- ["Crear la configuración del ciclo de vida de S3"](#)

"Política de eliminación de cubos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"EliminarReplicaciónDeBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Eliminar etiquetado de cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Eliminar objeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) Para esta solicitud, más este encabezado de solicitud adicional:

- `x-amz-bypass-governance-retention`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones sobre objetos"](#)

"Eliminar objetos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) Para esta solicitud, más este encabezado de solicitud adicional:

- `x-amz-bypass-governance-retention`

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

["Operaciones sobre objetos"](#)

"Eliminar etiquetado de objetos"

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones sobre objetos"](#)

"ObtenerBucketAcl"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"ObtenerBucketCors"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Obtener cifrado de cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Obtener configuración del ciclo de vida del cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

- ["Operaciones en buckets"](#)
- ["Crear la configuración del ciclo de vida de S3"](#)

"Obtener la ubicación del cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Configuración de GetBucketNotification"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Obtener política de cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Obtener réplica de cubo"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Obtener etiquetado de cubos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Obtener versiones de Bucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Obtener objeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud, más estos parámetros de consulta URI adicionales:

- x-amz-checksum-mode
- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding
- response-content-language
- response-content-type
- response-expires

Y estos encabezados de solicitud adicionales:

- Range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Obtener objeto"](#)

"ObtenerObjetoAcl"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones sobre objetos"](#)

"Obtener retención legal de objeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#)

"Obtener configuración de bloqueo de objeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#)

"Obtener retención de objetos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#)

"Obtener etiquetado de objetos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones sobre objetos"](#)

"Cubo de cabeza"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Objeto principal"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) Para esta solicitud, más estos encabezados adicionales:

- x-amz-checksum-mode
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Objeto principal"](#)

"Lista de cubos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

[Operaciones en el servicio](#) > [ListBuckets](#)

"Lista de cargas de varias partes"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) Para esta solicitud, más estos parámetros adicionales:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Lista de cargas de varias partes"](#)

"Lista de objetos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) Para esta solicitud, más estos parámetros adicionales:

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"ListObjectsV2"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) Para esta solicitud, más estos parámetros adicionales:

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Lista de versiones de objetos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) Para esta solicitud, más estos parámetros adicionales:

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Lista de partes"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) Para esta solicitud, más estos parámetros adicionales:

- max-parts

- part-number-marker
- uploadId

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Lista de cargas de varias partes"](#)

"PonerBucketCors"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Cifrado de PutBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Etiquetas XML del cuerpo de la solicitud

StorageGRID admite estas etiquetas XML del cuerpo de solicitud:

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Configuración del ciclo de vida de PutBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Etiquetas XML del cuerpo de la solicitud

StorageGRID admite estas etiquetas XML del cuerpo de solicitud:

- And
- Days
- Expiration

- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

Documentación de StorageGRID

- ["Operaciones en buckets"](#)
- ["Crear la configuración del ciclo de vida de S3"](#)

"Configuración de notificación de PutBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Etiquetas XML del cuerpo de la solicitud

StorageGRID admite estas etiquetas XML del cuerpo de solicitud:

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Política de depósito de basura"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Para obtener detalles sobre los campos de cuerpo JSON admitidos, consulte ["Utilice políticas de acceso a grupos y buckets"](#).

"Replicación de PutBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Etiquetas XML del cuerpo de la solicitud

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Etiquetado de PutBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

["Operaciones en buckets"](#)

"Versiones de PutBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Parámetros del cuerpo de la solicitud

StorageGRID admite estos parámetros del cuerpo de la solicitud:

- VersioningConfiguration
- Status

Documentación de StorageGRID

"Operaciones en buckets"

"PonerObjeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) Para esta solicitud, más estos encabezados adicionales:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-sha256
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-<metadata-name>

Cuerpo de la solicitud

- Datos binarios del objeto

Documentación de StorageGRID

"PonerObjeto"

"PonerObjetoLegalRetención"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#)

"Configuración de bloqueo de objeto de colocación"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#)

"PonerRetenciónDeObjeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) Para esta solicitud, más este encabezado adicional:

- x-amz-bypass-governance-retention

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#)

"Etiquetado de objetos puestos"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

StorageGRID admite todos los parámetros del cuerpo de la solicitud definidos por la API REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

["Operaciones sobre objetos"](#)

"Restaurar objeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Para obtener detalles sobre los campos corporales admitidos, consulte ["Restaurar objeto"](#) .

"Seleccionar contenido del objeto"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Para obtener detalles sobre los campos de cuerpo admitidos, consulte lo siguiente:

- ["Utilice S3 Select"](#)
- ["Seleccionar contenido del objeto"](#)

"Subir parte"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud, más estos parámetros de consulta URI adicionales:

- `partNumber`
- `uploadId`

Y estos encabezados de solicitud adicionales:

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Cuerpo de la solicitud

- Datos binarios de la pieza

Documentación de StorageGRID

["Subir parte"](#)

["Subir copia parcial"](#)

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud, más estos parámetros de consulta URI adicionales:

- `partNumber`
- `uploadId`

Y estos encabezados de solicitud adicionales:

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`

- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Subir copia parcial"](#)

Probar la configuración de la API REST de S3

Puede utilizar la interfaz de línea de comandos de Amazon Web Services (AWS CLI) para probar su conexión al sistema y verificar que puede leer y escribir objetos.

Antes de empezar

- Ha descargado e instalado la AWS CLI desde ["aws.amazon.com/cli"](https://aws.amazon.com/cli/) .
- Opcionalmente, tienes ["creó un punto final de balanceador de carga"](#) . De lo contrario, conoce la dirección IP del nodo de almacenamiento al que desea conectarse y el número de puerto a utilizar. Ver ["Direcciones IP y puertos para conexiones de cliente"](#) .
- Tienes ["creó una cuenta de inquilino S3"](#) .
- Has iniciado sesión en el inquilino y ["creó una clave de acceso"](#) .

Para obtener más detalles sobre estos pasos, consulte ["Configurar conexiones de cliente"](#) .

Pasos

1. Configure los ajustes de AWS CLI para usar la cuenta que creó en el sistema StorageGRID :
 - a. Entrar al modo de configuración: `aws configure`
 - b. Introduzca el ID de la clave de acceso para la cuenta que ha creado.
 - c. Introduzca la clave de acceso secreta para la cuenta que ha creado.
 - d. Introduzca la región predeterminada a utilizar. Por ejemplo, `us-east-1` .
 - e. Ingrese el formato de salida predeterminado a utilizar o presione **Enter** para seleccionar JSON.
2. Crear un depósito.

Este ejemplo supone que configuró un punto final del balanceador de carga para usar la dirección IP 10.96.101.17 y el puerto 10443.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

Si el depósito se crea correctamente, se devuelve la ubicación del depósito, como se ve en el siguiente ejemplo:

```
"Location": "/testbucket"
```

3. Subir un objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

Si el objeto se carga correctamente, se devuelve un Etag, que es un hash de los datos del objeto.

4. Enumere el contenido del depósito para verificar que se cargó el objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. Eliminar el objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Eliminar el depósito.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Cómo StorageGRID implementa la API REST de S3

Solicitudes de clientes conflictivas

Las solicitudes de clientes conflictivas, como dos clientes que escriben en la misma clave, se resuelven según el criterio del "último que gana".

El momento de la evaluación de "últimas victorias" se basa en cuándo el sistema StorageGRID completa una solicitud determinada y no en cuándo los clientes S3 comienzan una operación.

Valores de consistencia

La consistencia proporciona un equilibrio entre la disponibilidad de los objetos y la consistencia de esos objetos en diferentes nodos de almacenamiento y sitios. Puede cambiar la consistencia según lo requiera su aplicación.

De forma predeterminada, StorageGRID garantiza la consistencia de lectura tras escritura para los objetos recién creados. Cualquier operación GET posterior a una operación PUT completada con éxito podrá leer los datos recién escritos. Las sobrescrituras de objetos existentes, las actualizaciones de metadatos y las eliminaciones son eventualmente consistentes. Las sobrescrituras generalmente tardan segundos o minutos en propagarse, pero pueden demorar hasta 15 días.

Si desea realizar operaciones de objetos con una consistencia diferente, puede:

- Especificar una consistencia para [cada cubo](#) .
- Especificar una consistencia para [cada operación de API](#) .
- Cambie la consistencia predeterminada de toda la cuadrícula realizando una de las siguientes tareas:
 - En el Administrador de cuadrícula, vaya a **CONFIGURACIÓN > Sistema > Configuración de almacenamiento > Consistencia predeterminada**.
 - .



Un cambio en la consistencia de toda la cuadrícula se aplica solo a los depósitos creados después de que se modificó la configuración. Para determinar los detalles de un cambio, consulte el registro de auditoría ubicado en `/var/local/log` (buscar **consistencyLevel**).

Valores de consistencia

La consistencia afecta cómo se distribuyen los metadatos que StorageGRID utiliza para rastrear objetos entre los nodos y, por lo tanto, la disponibilidad de los objetos para las solicitudes de los clientes.

Puede establecer la consistencia de un depósito o una operación de API en uno de los siguientes valores:

- **Todos**: Todos los nodos reciben los datos inmediatamente o la solicitud fallará.
- **Strong-global**: garantiza la consistencia de lectura después de escritura para todas las solicitudes de clientes en todos los sitios.
- **Sitio fuerte**: garantiza la consistencia de lectura después de escritura para todas las solicitudes de clientes dentro de un sitio.
- **Lectura después de nueva escritura**: (predeterminado) proporciona consistencia de lectura después de escritura para objetos nuevos y consistencia eventual para actualizaciones de objetos. Ofrece alta disponibilidad y garantías de protección de datos. Recomendado para la mayoría de los casos.
- **Disponible**: Proporciona consistencia eventual tanto para objetos nuevos como para actualizaciones de objetos. Para los buckets S3, úselo solo cuando sea necesario (por ejemplo, para un bucket que contiene valores de registro que rara vez se leen, o para operaciones HEAD o GET en claves que no existen). No compatible con depósitos S3 FabricPool .

Utilice la consistencia "Lectura después de nueva escritura" y "Disponible"

Cuando una operación HEAD o GET utiliza la consistencia "Lectura después de nueva escritura", StorageGRID realiza la búsqueda en varios pasos, de la siguiente manera:

- Primero busca el objeto utilizando una consistencia baja.
- Si esa búsqueda falla, se repite la búsqueda en el siguiente valor de consistencia hasta que alcanza una consistencia equivalente al comportamiento de strong-global.

Si una operación HEAD o GET utiliza la consistencia "Lectura después de nueva escritura" pero el objeto no existe, la búsqueda del objeto siempre alcanzará una consistencia equivalente al comportamiento para una globalización fuerte. Debido a que esta consistencia requiere que varias copias de los metadatos del objeto estén disponibles en cada sitio, puede recibir una gran cantidad de errores internos del servidor 500 si dos o más nodos de almacenamiento en el mismo sitio no están disponibles.

A menos que necesite garantías de consistencia similares a Amazon S3, puede evitar estos errores para las operaciones HEAD y GET configurando la consistencia en "Disponible". Cuando una operación HEAD o GET utiliza la consistencia "Disponible", StorageGRID solo proporciona consistencia eventual. No vuelve a intentar una operación fallida con una consistencia creciente, por lo que no requiere que haya varias copias disponibles de los metadatos del objeto.

Especificar la consistencia para la operación de la API

Para establecer la consistencia de una operación de API individual, los valores de consistencia deben ser compatibles con la operación y debe especificar la consistencia en el encabezado de la solicitud. Este ejemplo establece la consistencia en "Strong-site" para una operación GetObject.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



Debe utilizar la misma consistencia para las operaciones PutObject y GetObject.

Especificar la consistencia para el depósito

Para establecer la consistencia del bucket, puede utilizar StorageGRID ["Consistencia del depósito PUT"](#) pedido. O puedes ["cambiar la consistencia de un cubo"](#) del administrador de inquilinos.

Al configurar la consistencia de un depósito, tenga en cuenta lo siguiente:

- La configuración de la consistencia de un depósito determina qué consistencia se utiliza para las operaciones S3 realizadas en los objetos del depósito o en la configuración del depósito. No afecta las operaciones en el bucket en sí.
- La consistencia de una operación de API individual anula la consistencia del depósito.
- En general, los buckets deben usar la consistencia predeterminada: "Lectura después de nueva 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 la consistencia para cada solicitud de API. Establezca la consistencia a nivel de depósito sólo como último recurso.

Cómo interactúan los controles de consistencia y las reglas ILM para afectar la protección de datos

Tanto su elección de consistencia como su regla ILM afectan cómo se protegen los objetos. Estas configuraciones pueden interactuar.

Por ejemplo, la consistencia utilizada cuando se almacena un objeto afecta la ubicación inicial de los metadatos del objeto, mientras que el comportamiento de ingesta seleccionado para la regla ILM afecta la ubicación inicial de las copias del objeto. Debido a que StorageGRID requiere acceso tanto a los metadatos de un objeto como a sus datos para cumplir con las solicitudes de los clientes, seleccionar niveles de protección coincidentes para la consistencia y el comportamiento de ingesta puede brindar una mejor protección de datos inicial y respuestas del sistema más predecibles.

La siguiente "opciones de ingesta" Están disponibles para las reglas ILM:

Compromiso dual

StorageGRID realiza inmediatamente copias provisionales del objeto y devuelve el éxito al cliente. Cuando sea posible se realizarán las copias especificadas en la regla ILM.

Estricto

Se deben realizar todas las copias especificadas en la regla ILM antes de devolver el éxito al cliente.

Equilibrado

StorageGRID intenta hacer todas las copias especificadas en la regla ILM durante la ingesta; si esto no es posible, se hacen copias provisionales y se devuelve el resultado exitoso al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

Ejemplo de cómo la consistencia y la regla ILM pueden interactuar

Supongamos que tiene una cuadrícula de dos sitios con la siguiente regla ILM y la siguiente consistencia:

- **Regla ILM:** Crea dos copias de objetos, una en el sitio local y otra en un sitio remoto. Utilice el comportamiento de ingesta estricto.
- **Consistencia:** Fuerte-global (los metadatos del objeto se distribuyen inmediatamente a todos los sitios).

Cuando un cliente almacena un objeto en la red, StorageGRID realiza copias de los objetos y distribuye metadatos a ambos sitios antes de devolver el éxito al cliente.

El objeto está completamente protegido contra pérdida en el momento del mensaje de ingesta exitosa. Por ejemplo, si el sitio local se pierde poco después de la ingesta, aún existen copias de los datos del objeto y de los metadatos del objeto en el sitio remoto. El objeto es completamente recuperable.

Si, en cambio, utilizara la misma regla ILM y la consistencia del sitio fuerte, el cliente podría recibir un mensaje de éxito después de que los datos del objeto se repliquen 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 del objeto no coincide con el nivel de protección de los datos del objeto. Si el sitio local se pierde poco después de la ingesta, se pierden los metadatos del objeto. No se puede recuperar el objeto.

La interrelación entre la consistencia y las reglas ILM puede ser compleja. Comuníquese con NetApp si necesita ayuda.

Control de versiones de objetos

Puede establecer el estado de control de versiones de un depósito si desea conservar varias versiones de cada objeto. Habilitar el control de versiones de un bucket puede ayudar a proteger contra la eliminación accidental de objetos y le permite recuperar y restaurar versiones anteriores de un objeto.

El sistema StorageGRID implementa control de versiones con soporte para la mayoría de las funciones y con

algunas limitaciones. StorageGRID admite hasta 10 000 versiones de cada objeto.

El control de versiones de objetos se puede combinar con la gestión del ciclo de vida de la información (ILM) de StorageGRID o con la configuración del ciclo de vida del bucket S3. Debe habilitar explícitamente el control de versiones para cada depósito. Cuando se habilita el control de versiones para un depósito, a cada objeto agregado al depósito se le asigna un ID de versión, que es generado por el sistema StorageGRID .

No se admite el uso de MFA (autenticación multifactor).



El control de versiones solo se puede habilitar en depósitos creados con StorageGRID versión 10.3 o posterior.

ILM y control de versiones

Las políticas ILM se aplican a cada versión de un objeto. Un proceso de escaneo ILM escanea continuamente todos los objetos y los reevalúa en función de la política ILM actual. Cualquier cambio que realice en las políticas de ILM se aplicará a todos los objetos ingeridos previamente. Esto incluye versiones ingeridas previamente si el control de versiones está habilitado. El escaneo ILM aplica nuevos cambios ILM a objetos ingeridos previamente.

Para los objetos S3 en depósitos habilitados para control de versiones, la compatibilidad con control de versiones le permite crear reglas ILM que usan "Hora no actual" como Hora de referencia (seleccione **Sí** para la pregunta "¿Aplicar esta regla solo a versiones de objetos anteriores?" en ["Paso 1 del asistente para crear una regla de ILM"](#)). Cuando se actualiza un objeto, sus versiones anteriores dejan de ser actuales. El uso de un filtro de "Tiempo no actual" le permite crear políticas que reducen el impacto del almacenamiento de versiones anteriores de los objetos.



Cuando se carga una nueva versión de un objeto mediante una operación de carga multiparte, el tiempo no actual de la versión original del objeto refleja cuándo se creó la carga multiparte para la nueva versión, no cuándo se completó la carga multiparte. En casos limitados, la hora no actual de la versión original puede ser horas o días anterior a la hora de la versión actual.

Información relacionada

- ["Cómo se eliminan los objetos versionados de S3"](#)
- ["Reglas y políticas de ILM para objetos versionados de S3 \(Ejemplo 4\)"](#) .

Utilice la API REST de S3 para configurar el bloqueo de objetos de S3

Si la configuración global de Bloqueo de objetos S3 está habilitada para su sistema StorageGRID , puede crear depósitos con el Bloqueo de objetos S3 habilitado. Puede especificar la retención predeterminada para cada depósito o configuraciones de retención para cada versión de objeto.

Cómo habilitar el bloqueo de objetos S3 para un bucket

Si la configuración global de Bloqueo de objetos S3 está habilitada para su sistema StorageGRID , puede habilitar opcionalmente el Bloqueo de objetos S3 cuando cree cada depósito.

El bloqueo de objetos S3 es una configuración permanente que solo se puede habilitar cuando se crea un depósito. No es posible agregar ni deshabilitar el bloqueo de objetos S3 después de crear un depósito.

Para habilitar el bloqueo de objetos S3 para un depósito, utilice cualquiera de estos métodos:

- Cree el depósito mediante el Administrador de inquilinos. Ver ["Crear un depósito S3"](#) .
- Cree el depósito mediante una solicitud CreateBucket con el `x-amz-bucket-object-lock-enabled` encabezado de solicitud. Ver ["Operaciones en buckets"](#) .

El bloqueo de objetos S3 requiere control de versiones del depósito, que se habilita automáticamente cuando se crea el depósito. No se puede suspender el control de versiones del depósito. Ver ["Control de versiones de objetos"](#) .

Configuración de retención predeterminada para un depósito

Cuando el bloqueo de objetos S3 está habilitado para un depósito, puede habilitar opcionalmente la retención predeterminada para el depósito y especificar un modo de retención predeterminado y un período de retención predeterminado.

Modo de retención predeterminado

- En modo CUMPLIMIENTO:
 - El objeto no se puede eliminar hasta que se alcance su fecha de conservación.
 - La fecha de conservación del objeto se puede aumentar, pero no se puede disminuir.
 - La fecha de retención del objeto no se puede eliminar hasta que se alcance esa fecha.
- En modo GOBERNANZA:
 - Usuarios con la `s3:BypassGovernanceRetention` El permiso puede utilizar el `x-amz-bypass-governance-retention: true` encabezado de solicitud para omitir la configuración de retención.
 - Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su fecha de conservación.
 - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de conservación de un objeto.

Período de retención predeterminado

Cada depósito puede tener un período de retención predeterminado especificado en años o días.

Cómo configurar la retención predeterminada para un depósito

Para establecer la retención predeterminada para un depósito, utilice cualquiera de estos métodos:

- Administre la configuración del depósito desde el Administrador de inquilinos. Ver ["Crear un bucket S3"](#) y ["Actualizar la retención predeterminada de bloqueo de objetos S3"](#) .
- Emita una solicitud PutObjectLockConfiguration para el depósito para especificar el modo predeterminado y el número predeterminado de días o años.

Configuración de bloqueo de objeto de colocación

La solicitud PutObjectLockConfiguration le permite establecer y modificar el modo de retención predeterminado y el período de retención predeterminado para un depósito que tiene habilitado el bloqueo de objetos S3. También puede eliminar las configuraciones de retención predeterminadas configuradas previamente.

Cuando se incorporan nuevas versiones de objetos al depósito, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` y `x-amz-object-lock-retain-until-date` no están especificados El período de retención predeterminado se utiliza para calcular la fecha de retención hasta si `x-`

amz-object-lock-retain-until-date No está especificado.

Si el período de retención predeterminado se modifica después de la ingesta de una versión de objeto, la fecha de retención de la versión del objeto permanece igual y no se vuelve a calcular utilizando el nuevo período de retención predeterminado.

Debes tener el `s3:PutBucketObjectLockConfiguration` permiso, o ser la cuenta root, para completar esta operación.

El Content-MD5 El encabezado de la solicitud debe especificarse en la solicitud PUT.

Ejemplo de solicitud

Este ejemplo habilita el bloqueo de objetos S3 para un depósito y establece el modo de retención predeterminado en CUMPLIMIENTO y el período de retención predeterminado en 6 años.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

Cómo determinar la retención predeterminada para un bucket

Para determinar si S3 Object Lock está habilitado para un bucket y ver el modo de retención predeterminado y el período de retención, utilice cualquiera de estos métodos:

- Ver el depósito en el Administrador de inquilinos. Ver ["Ver depósitos S3"](#) .
- Emite una solicitud GetObjectLockConfiguration.

Obtener configuración de bloqueo de objeto

La solicitud GetObjectLockConfiguration le permite determinar si S3 Object Lock está habilitado para un depósito y, si está habilitado, ver si hay un modo de retención predeterminado y un período de retención configurados para el depósito.

Cuando se incorporan nuevas versiones de objetos al depósito, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` No está especificado. El período de retención predeterminado se utiliza para calcular la fecha de retención hasta si `x-amz-object-lock-retain-until-date` No está especificado.

Debes tener el `s3:GetBucketObjectLockConfiguration` permiso, o ser la cuenta root, para completar esta operación.

Ejemplo de solicitud

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Ejemplo de respuesta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpX1knabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

Cómo especificar la configuración de retención para un objeto

Un depósito con el bloqueo de objetos S3 habilitado puede contener una combinación de objetos con y sin configuraciones de retención de bloqueo de objetos S3.

Las configuraciones de retención a nivel de objeto se especifican mediante la API REST de S3. La configuración de retención de un objeto anula cualquier configuración de retención predeterminada para el depósito.

Puede especificar las siguientes configuraciones para cada objeto:

- **Modo de retención:** CUMPLIMIENTO o GOBERNANZA.
- **Retain-until-date:** una fecha que especifica durante cuánto tiempo StorageGRID debe conservar la versión del objeto.
 - En el modo CUMPLIMIENTO, si la fecha de retención hasta está en el futuro, el objeto se puede recuperar, pero no se puede modificar ni eliminar. La fecha de conservación hasta se puede aumentar, pero esta fecha no se puede disminuir ni eliminar.
 - En el modo GOBERNANZA, los usuarios con permiso especial pueden omitir la configuración de conservar hasta la fecha. Pueden eliminar una versión de un objeto antes de que transcurra su período de retención. También pueden aumentar, disminuir o incluso eliminar la fecha de conservación.
- **Retención legal:** al aplicar una retención legal a una versión de un objeto, se bloquea inmediatamente ese objeto. Por ejemplo, es posible que necesites colocar una retención legal en un objeto que esté relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de vencimiento, sino que permanece vigente hasta que se elimina explícitamente.

La configuración de retención legal de un objeto es independiente del modo de retención y de la fecha de retención. Si una versión de un objeto está bajo retención legal, nadie puede eliminar esa versión.

Para especificar la configuración de bloqueo de objetos S3 al agregar una versión de objeto a un depósito, emita un ["PonerObjeto"](#), ["Copiar objeto"](#), o ["Crear carga de varias partes"](#) pedido.

Puedes utilizar lo siguiente:

- `x-amz-object-lock-mode`, que puede ser CUMPLIMIENTO o GOBERNANZA (sensible a mayúsculas y minúsculas).



Si lo 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 de conservación hasta la fecha debe tener el formato `2020-08-10T21:46:00Z`. Se permiten fracciones de segundo, pero solo se conservan 3 dígitos decimales (precisión de milisegundos). No se permiten otros formatos ISO 8601.
 - La fecha de conservación debe ser en el futuro.
- `x-amz-object-lock-legal-hold`

Si la retención legal está activada (distingue entre mayúsculas y minúsculas), el objeto se coloca bajo una retención legal. Si la retención legal está desactivada, no se aplica ninguna retención legal. Cualquier otro valor generará un error 400 Solicitud incorrecta (argumento inválido).

Si utiliza alguno de estos encabezados de solicitud, tenga en cuenta estas restricciones:

- El `Content-MD5` El encabezado de solicitud es obligatorio si lo hay `x-amz-object-lock-*` El encabezado de solicitud está presente en la solicitud `PutObject`. `Content-MD5` no es necesario para

CopyObject o CreateMultipartUpload.

- Si el depósito no tiene habilitado el bloqueo de objetos S3 y un `x-amz-object-lock-*` Si el encabezado de solicitud está presente, se devuelve un error 400 Solicitud incorrecta (InvalidRequest).
- La solicitud PutObject admite el uso de `x-amz-storage-class: REDUCED_REDUNDANCY` para que coincida con el comportamiento de AWS. Sin embargo, cuando se ingiere un objeto en un bucket con el bloqueo de objetos S3 habilitado, StorageGRID siempre realizará una ingesta de confirmación dual.
- Una respuesta de versión GET o HeadObject posterior 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 la información correcta `s3:Get*` permisos.

Puedes utilizar el `s3:object-lock-remaining-retention-days` Clave de condición de política para limitar los períodos de retención mínimos y máximos permitidos para sus objetos.

Cómo actualizar la configuración de retención de un objeto

Si necesita actualizar la configuración de retención o retención legal para una versión de objeto existente, puede realizar las siguientes operaciones de subrecurso de objeto:

- PutObjectLegalHold

Si el nuevo valor de retención legal está activado, el objeto se coloca bajo una retención legal. Si el valor de retención legal está DESACTIVADO, se levanta la retención legal.

- PutObjectRetention
 - El valor del modo puede ser CUMPLIMIENTO o GOBERNANZA (distingue entre mayúsculas y minúsculas).
 - El valor de conservación hasta la fecha debe tener el formato `2020-08-10T21:46:00Z`. Se permiten fracciones de segundo, pero solo se conservan 3 dígitos decimales (precisión de milisegundos). No se permiten otros formatos ISO 8601.
 - Si una versión de objeto tiene una fecha de conservación existente, solo puedes aumentarla. El nuevo valor debe estar en el futuro.

Cómo utilizar el modo GOBERNANZA

Los usuarios que tengan la `s3:BypassGovernanceRetention` El permiso puede omitir la configuración de retención activa de un objeto que utiliza el modo GOBERNANZA. Cualquier operación DELETE o PutObjectRetention debe incluir el `x-amz-bypass-governance-retention:true` encabezado de solicitud. Estos usuarios pueden realizar estas operaciones adicionales:

- Realice las operaciones DeleteObject o DeleteObjects para eliminar una versión de un objeto antes de que transcurra su período de retención.

Los objetos que están bajo retención legal no se pueden eliminar. La retención legal debe estar DESACTIVADA.

- Realice operaciones PutObjectRetention que cambien el modo de la versión de un objeto de GOBERNANZA a CUMPLIMIENTO antes de que transcurra el período de retención del objeto.

Nunca se permite cambiar el modo de CUMPLIMIENTO a GOBERNANZA.

- Realice operaciones PutObjectRetention para aumentar, disminuir o eliminar el período de retención de una versión de objeto.

Información relacionada

- ["Administrar objetos con S3 Object Lock"](#)
- ["Utilice S3 Object Lock para retener objetos"](#)
- ["Guía del usuario de Amazon Simple Storage Service: Bloqueo de objetos"](#)

Crear la configuración del ciclo de vida de S3

Puede crear una configuración de ciclo de vida S3 para controlar cuándo se eliminan objetos específicos del sistema StorageGRID .

El ejemplo simple de esta sección ilustra cómo una configuración del ciclo de vida de S3 puede controlar cuándo se eliminan (caducan) determinados objetos de depósitos S3 específicos. El ejemplo de esta sección es sólo para fines ilustrativos. Para obtener detalles completos sobre la creación de configuraciones del ciclo de vida de S3, consulte ["Guía del usuario de Amazon Simple Storage Service: Gestión del ciclo de vida de los objetos"](#) . Tenga en cuenta que StorageGRID solo admite acciones de vencimiento; 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 depósitos S3 específicos. Cada regla especifica qué objetos se ven afectados y cuándo expirarán esos objetos (en una fecha específica o después de una cierta cantidad de días).

StorageGRID admite hasta 1000 reglas de ciclo de vida en una configuración de ciclo de vida. Cada regla puede incluir los siguientes elementos XML:

- Vencimiento: elimina un objeto cuando se alcanza una fecha específica o cuando se alcanza una cantidad específica de días, a partir del momento en que se ingirió el objeto.
- NoncurrentVersionExpiration: elimina un objeto cuando se alcanza una cantidad específica de días, a partir del momento en que el objeto dejó de ser actual.
- Filtro (Prefijo, Etiqueta)
- Estado
- IDENTIFICACIÓN

Cada objeto sigue la configuración de retención de un ciclo de vida de un bucket S3 o de una política ILM. Cuando se configura un ciclo de vida de un depósito S3, las acciones de vencimiento del ciclo de vida anulan la política de ILM para los objetos que coinciden con el filtro del ciclo de vida del depósito. Los objetos que no coinciden con el filtro del ciclo de vida del depósito utilizan la configuración de retención de la política de ILM. Si un objeto coincide con un filtro de ciclo de vida de depósito y no se especifican explícitamente acciones de vencimiento, no se utilizan las configuraciones de retención de la política ILM y se implica que las versiones del objeto se conservan para siempre. Ver ["Prioridades de ejemplo para el ciclo de vida del depósito S3 y la política de ILM"](#) .

Como resultado, es posible que se elimine un objeto de la cuadrícula aunque las instrucciones de ubicación de una regla ILM todavía se apliquen al objeto. O bien, un objeto podría conservarse en la cuadrícula incluso después de que hayan transcurrido las instrucciones de ubicación de ILM para el objeto. Para obtener más información, consulte ["Cómo funciona ILM a lo largo de la vida de un objeto"](#) .



La configuración del ciclo de vida del bucket se puede usar con buckets que tienen habilitado el bloqueo de objetos S3, pero la configuración del ciclo de vida del bucket no es compatible con buckets compatibles heredados.

StorageGRID admite el uso de las siguientes operaciones de depósito para administrar las configuraciones del ciclo de vida:

- Eliminar ciclo de vida del cubo
- Obtener configuración del ciclo de vida del cubo
- Configuración del ciclo de vida de PutBucket

Crear configuración de ciclo de vida

Como primer paso para crear una configuración de ciclo de vida, crea un archivo JSON que incluye una o más reglas. Por ejemplo, este archivo JSON incluye tres reglas, como sigue:

1. La regla 1 se aplica únicamente a los objetos que coinciden con el prefijo `category1` / y que tienen una `key2` valor de `tag2` . El `Expiration` El parámetro especifica que los objetos que coincidan con el filtro caducarán a la medianoche del 22 de agosto de 2020.
2. La regla 2 se aplica únicamente a los objetos que coinciden con el prefijo `category2` /. El `Expiration` El parámetro especifica que los objetos que coinciden con el filtro caducarán 100 días después de su ingesta.



Las reglas que especifican un número de días son relativas al momento en que se ingirió el objeto. Si la fecha actual excede la fecha de ingesta más la cantidad de días, es posible que se eliminen algunos objetos del depósito tan pronto como se aplique la configuración del ciclo de vida.

3. La regla 3 se aplica únicamente a los objetos que coinciden con el prefijo `category3` /. El `Expiration` El parámetro especifica que cualquier versión no actual de los objetos coincidentes expirará 50 días después de que dejen de estar actuales.

```

{
  "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 depósito

Después de haber creado el archivo de configuración del ciclo de vida, debe aplicarlo a un depósito emitiendo una solicitud `PutBucketLifecycleConfiguration`.

Esta solicitud aplica la configuración del ciclo de vida en el archivo de ejemplo a los objetos en un depósito llamado `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Para validar que una configuración de ciclo de vida se aplicó correctamente al depósito, emita una solicitud `GetBucketLifecycleConfiguration`. Por ejemplo:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

Una respuesta exitosa enumera la configuración del ciclo de vida que acaba de aplicar.

Validar que la expiración del ciclo de vida del bucket se aplique al objeto

Puede determinar si una regla de expiración en la configuración del ciclo de vida se aplica a un objeto específico al emitir una solicitud `PutObject`, `HeadObject` o `GetObject`. Si se aplica una regla, la respuesta incluye una `Expiration` parámetro que indica cuándo expira el objeto y qué regla de expiración coincidió.



Debido a que el ciclo de vida del bucket anula ILM, `expiry-date` Se muestra la fecha real en la que se eliminará el objeto. Para obtener más información, consulte ["Cómo se determina la retención de objetos"](#).

Por ejemplo, esta solicitud `PutObject` se emitió el 22 de junio de 2020 y coloca un objeto en el `testbucket` balde.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La respuesta de éxito indica que el objeto caducará en 100 días (1 de octubre de 2020) y que coincidió con la Regla 2 de la configuración del ciclo de vida.

```
{
  "Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-id=\"rule2\"",
  "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Por ejemplo, esta solicitud HeadObject se utilizó para obtener metadatos para el mismo objeto en el depósito testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La respuesta de éxito incluye los metadatos del objeto e indica que el objeto caducará en 100 días y que coincidió con la Regla 2.

```
{
  "AcceptRanges": "bytes",
  "Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-id=\"rule2\"",
  "LastModified": "2020-06-23T09:07:48+00:00",
  "ContentLength": 921,
  "ETag": "\"9762f8a803bc34f5340579d4446076f7\"",
  "ContentType": "binary/octet-stream",
  "Metadata": {}
}
```



Para los depósitos con control de versiones habilitado, el `x-amz-expiration` El encabezado de respuesta se aplica solo a las versiones actuales de los objetos.

Recomendaciones para implementar la API REST de S3

Debe seguir estas recomendaciones al implementar la API REST S3 para su uso con StorageGRID.

Recomendaciones para HEADs a objetos inexistentes

Si su aplicación verifica rutinariamente si existe un objeto en una ruta en la que no espera que el objeto exista realmente, debe usar la opción "Disponible". ["consistencia"](#) . Por ejemplo, debe utilizar la consistencia "Disponible" si su aplicación encabeza una ubicación antes de PUT en ella.

De lo contrario, si la operación HEAD no encuentra el objeto, es posible que reciba una gran cantidad de errores internos del servidor 500 si dos o más nodos de almacenamiento en el mismo sitio no están disponibles o si no se puede acceder a un sitio remoto.

Puede establecer la consistencia "Disponible" para cada depósito utilizando el ["Consistencia del depósito PUT"](#) solicitud, o puede especificar la consistencia en el encabezado de la solicitud para una operación de API individual.

Recomendaciones para claves de objeto

Siga estas recomendaciones para los nombres de claves de objeto, según el momento en que se creó el depósito por primera vez.

Cubos creados en StorageGRID 11.4 o anterior

- No utilice valores aleatorios como los primeros cuatro caracteres de las claves de objeto. Esto contrasta con la recomendación anterior de AWS para prefijos clave. En su lugar, utilice prefijos no aleatorios ni únicos, como `image`.
- Si sigue la recomendación anterior de AWS de utilizar caracteres aleatorios y únicos en los prefijos de clave, anteponga a las claves de objeto un nombre de directorio. Es decir, utiliza este formato:

```
mybucket/mydir/f8e3-image3132.jpg
```

En lugar de este formato:

```
mybucket/f8e3-image3132.jpg
```

Cubos creados en StorageGRID 11.4 o posterior

No es necesario restringir los nombres de claves de objeto para cumplir con las mejores prácticas de rendimiento. En la mayoría de los casos, puede utilizar valores aleatorios para los primeros cuatro caracteres de los nombres de claves de objeto.



Una excepción a esto es una carga de trabajo S3 que elimina continuamente todos los objetos después de un corto período de tiempo. Para minimizar el impacto en el rendimiento de este caso de uso, varíe una parte inicial del nombre de la clave cada varios miles de objetos con algo como la fecha. Por ejemplo, supongamos que un cliente S3 normalmente escribe 2000 objetos por segundo y la política de ciclo de vida del ILM o del bucket elimina todos los objetos después de tres días. Para minimizar el impacto en el rendimiento, puedes nombrar las claves utilizando un patrón como este: `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

Recomendaciones para "lecturas de rango"

Si el "[Opción global para comprimir objetos almacenados](#)" Si está habilitado, las aplicaciones cliente S3 deben evitar realizar operaciones `GetObject` que especifiquen un rango de bytes que se devolverán. Estas operaciones de "lectura de rango" son ineficientes porque StorageGRID debe descomprimir efectivamente los objetos para acceder a los bytes solicitados. Las operaciones `GetObject` que solicitan un rango pequeño de bytes de un objeto muy grande son especialmente ineficientes; por ejemplo, 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 expirar.



Si necesita comprimir objetos y su aplicación cliente debe utilizar lecturas de rango, aumente el tiempo de espera de lectura de la aplicación.

Compatibilidad con la API REST de Amazon S3

Detalles de implementación de la API REST de S3

El sistema StorageGRID implementa la API de servicio de almacenamiento simple (versión de API 2006-03-01) con soporte para la mayoría de las operaciones y con algunas limitaciones. Debe comprender los detalles de implementación cuando integra aplicaciones cliente de API REST S3.

El sistema StorageGRID admite solicitudes de estilo alojado virtual y solicitudes de estilo de ruta.

Manejo de fechas

La implementación de StorageGRID de la API REST S3 solo admite formatos de fecha HTTP válidos.

El sistema StorageGRID solo admite formatos de fecha HTTP válidos para cualquier encabezado que acepte valores de fecha. La parte horaria de la fecha se puede especificar en formato de Hora Media de Greenwich (GMT) o en formato de Hora Universal Coordinada (UTC) sin diferencia de zona horaria (se debe especificar +0000). Si incluye el `x-amz-date` encabezado en su solicitud, anula cualquier valor especificado en el encabezado de solicitud de Fecha. Al utilizar AWS Signature Version 4, el `x-amz-date` El encabezado debe estar presente en la solicitud firmada porque el encabezado de fecha no es compatible.

Encabezados de solicitud comunes

El sistema StorageGRID admite los encabezados de solicitud comunes definidos por ["Referencia de la API de Amazon Simple Storage Service: encabezados de solicitud comunes"](#), con una excepción.

Encabezado de solicitud	Implementación
Autorización	Soporte completo para AWS Signature Version 2 Compatibilidad con AWS Signature versión 4, con las siguientes excepciones: • Cuando proporciona el valor de suma de comprobación de carga útil real en <code>x-amz-content-sha256</code>, el valor se acepta sin validación, como si el valor <code>UNSIGNED-PAYLOAD</code> se había previsto para el encabezado. Cuando usted proporciona un <code>x-amz-content-sha256</code> valor de encabezado que implica <code>aws-chunked</code> transmisión (por ejemplo, <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>), las firmas del fragmento no se verifican con los datos del fragmento.
token de seguridad x-amz	No implementado. Devoluciones <code>XNotImplemented</code> .

Encabezados de respuesta comunes

El sistema StorageGRID admite todos los encabezados de respuesta comunes definidos por la *Referencia de API del servicio de almacenamiento simple*, con una excepción.

Encabezado de respuesta	Implementación
x-amz-id-2	No utilizado

Autenticar solicitudes

El sistema StorageGRID admite el acceso autenticado y anónimo a objetos mediante la API S3.

La API S3 admite las versiones 2 y 4 de Signature para autenticar solicitudes de API S3.

Las solicitudes autenticadas deben firmarse utilizando 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 de autorización HTTP

El HTTP Authorization El encabezado lo utilizan todas las operaciones de API de S3, excepto las solicitudes anónimas cuando lo permite la política del bucket. El Authorization El encabezado contiene toda la información de firma necesaria para autenticar una solicitud.

Utilizar parámetros de consulta

Puede utilizar parámetros de consulta para agregar información de autenticación a una URL. Esto se conoce como prefirmar la URL, que puede utilizarse 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.

Operación	Implementación
Lista de cubos (anteriormente llamado Servicio GET)	Implementado con todo el comportamiento de la API REST de Amazon S3. Sujeto a cambios sin previo aviso.
Uso de almacenamiento GET	El StorageGRID " Uso de almacenamiento GET " La solicitud le indica la cantidad total de almacenamiento en uso por una cuenta y para cada depósito asociado con la cuenta. Esta es 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 / solicitudes al puerto S3 en un nodo de almacenamiento, sin proporcionar credenciales de autenticación S3, para determinar si el nodo de almacenamiento está disponible. Puede utilizar esta solicitud para realizar monitoreo o para permitir que los balanceadores de carga externos identifiquen cuando un nodo de almacenamiento está inactivo.

Operaciones en buckets

El sistema StorageGRID admite un máximo de 5000 depósitos para cada cuenta de inquilino de S3.

Cada cuadrícula puede tener un máximo de 100.000 contenedores.

Para soportar 5000 buckets, cada nodo de almacenamiento en la red debe tener un mínimo de 64 GB de RAM.

Las restricciones de nombre de depósito siguen las restricciones de la región estándar de AWS EE. UU., pero debe restringirlas aún más a las convenciones de nombres de DNS para admitir solicitudes de estilo alojado

virtualmente S3.

Para obtener más información, consulte lo siguiente:

- ["Guía del usuario de Amazon Simple Storage Service: cuotas, restricciones y limitaciones de buckets"](#)
- ["Configurar nombres de dominio de puntos finales S3"](#)

Las operaciones ListObjects (GET Bucket) y ListObjectVersions (GET Bucket object versions) admiten StorageGRID ["valores de consistencia"](#) .

Puede verificar si las actualizaciones de la última hora de acceso están habilitadas o deshabilitadas para depósitos individuales. Ver ["GET Hora del último acceso al bucket"](#) .

La siguiente tabla describe cómo StorageGRID implementa las operaciones del bucket de API REST de S3. Para realizar cualquiera de estas operaciones se deberán proporcionar las credenciales de acceso necesarias a la cuenta.

Operación	Implementación
Crear cubo	Crea un nuevo depósito. Al crear el depósito, usted se convierte en el propietario del mismo. • Los nombres de los depósitos deben cumplir con las siguientes reglas: ◦ Debe ser único en cada sistema StorageGRID (no solo único dentro de la cuenta del inquilino). ◦ Debe ser compatible con DNS. ◦ Debe contener 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 parecer una dirección IP con formato de texto. ◦ No se deben utilizar puntos en solicitudes de estilo alojado virtualmente. Los períodos causarán problemas con la verificación del certificado comodín del servidor. • De forma predeterminada, los depósitos se crean en el <code>us-east-1</code> región; sin embargo, puede utilizar el <code>LocationConstraint</code> Elemento de solicitud en el cuerpo de la solicitud para especificar una región diferente. Al utilizar el <code>LocationConstraint</code> elemento, debe especificar el nombre exacto de una región que se haya definido utilizando el Administrador de cuadrícula o la API de administración de cuadrícula. Comuníquese con su administrador del sistema si no sabe el nombre de la región que debe utilizar. Nota: Se producirá un error si su solicitud <code>CreateBucket</code> utiliza una región que no se ha definido en StorageGRID. • Puedes incluir el <code>x-amz-bucket-object-lock-enabled</code> encabezado de solicitud para crear un bucket con el bloqueo de objetos S3 habilitado. Ver "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" . Debe habilitar el bloqueo de objetos S3 al crear el depósito. No es posible agregar ni deshabilitar el bloqueo de objetos S3 después de crear un depósito. El bloqueo de objetos S3 requiere control de versiones del depósito, que se habilita automáticamente cuando se crea el depósito.
Eliminar cubo	Elimina el depósito.
EliminarBucketCors	Elimina la configuración CORS para el bucket.
Eliminar cifrado del cubo	Elimina el cifrado predeterminado del depósito. Los objetos cifrados existentes permanecen cifrados, pero cualquier objeto nuevo que se agregue al depósito no se cifra.
Eliminar ciclo de vida del cubo	Elimina la configuración del ciclo de vida del depósito. Ver "Crear la configuración del ciclo de vida de S3" .

Operación	Implementación
Política de eliminación de cubos	Elimina la política asociada al depósito.
EliminarReplicaciónDeBucket	Elimina la configuración de replicación asociada al depósito.
Eliminar etiquetado de cubo	Utiliza el <code>tagging</code> subrecurso para eliminar todas las etiquetas de un depósito. Precaución: Si se establece una etiqueta de política ILM no predeterminada para este depósito, habrá un <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta de cubo con un valor asignado a ella. No emita una solicitud <code>DeleteBucketTagging</code> si hay una <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta de cubo. En su lugar, emita una solicitud <code>PutBucketTagging</code> solo con el <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta y su valor asignado para eliminar todas las demás etiquetas del depósito. No modifique ni elimine el <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta de cubo
ObtenerBucketAcl	Devuelve una respuesta positiva y el ID, el nombre para mostrar y el permiso del propietario del depósito, lo que indica que el propietario tiene acceso completo al depósito.
ObtenerBucketCors	Devuelve el <code>cors</code> configuración para el bucket.
Obtener cifrado de cubo	Devuelve la configuración de cifrado predeterminada para el depósito.
Obtener configuración del ciclo de vida del cubo (anteriormente llamado ciclo de vida del bucket GET)	Devuelve la configuración del ciclo de vida del depósito. Ver " Crear la configuración del ciclo de vida de S3 ".
Obtener la ubicación del cubo	Devuelve la región que se configuró utilizando el <code>LocationConstraint</code> elemento en la solicitud <code>CreateBucket</code> . Si la región del cubo es <code>us-east-1</code> , se devuelve una cadena vacía para la región.
Configuración de GetBucketNotification (anteriormente llamada notificación GET Bucket)	Devuelve la configuración de notificación adjunta al depósito.
Obtener política de cubo	Devuelve la política asociada al depósito.
Obtener réplica de cubo	Devuelve la configuración de replicación asociada al depósito.

Operación	Implementación
Obtener etiquetado de cubos	Utiliza el <code>tagging</code> subrecurso para devolver todas las etiquetas de un depósito. Precaución: Si se establece una etiqueta de política ILM no predeterminada para este depósito, habrá un <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta de cubo con un valor asignado a ella. No modifique ni elimine esta etiqueta.
Obtener versiones de Bucket	Esta implementación utiliza el <code>versioning</code> subrecurso para devolver el estado de control de versiones de un bucket. • <i>blank</i>: El control de versiones nunca se ha habilitado (el depósito está "Sin versión") • Habilitado: el control de versiones está habilitado • Suspendido: el control de versiones estaba habilitado previamente y está suspendido
Obtener configuración de bloqueo de objeto	Devuelve el modo de retención predeterminado del depósito y el período de retención predeterminado, si está configurado. Ver "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" .
Cubo de cabeza	Determina si existe un depósito y tienes permiso para acceder a él. Esta operación devuelve: • <code>x-ntap-sg-bucket-id</code>: El UUID del depósito en formato UUID. • <code>x-ntap-sg-trace-id</code>: El ID de seguimiento único de la solicitud asociada.
ListObjects y ListObjectsV2 (anteriormente llamado GET Bucket)	Devuelve algunos o todos (hasta 1000) los objetos de un depósito. La clase de almacenamiento para objetos puede tener cualquiera de dos valores, incluso si el objeto se ingirió con el <code>REDUCED_REDUNDANCY</code> opción de clase de almacenamiento: • <code>STANDARD</code>, lo que indica que el objeto está almacenado en un grupo de almacenamiento que consta de nodos de almacenamiento. • <code>GLACIER</code>, lo que indica que el objeto se ha movido al depósito externo especificado por el grupo de almacenamiento en la nube. Si el depósito contiene una gran cantidad de claves eliminadas que tienen el mismo prefijo, la respuesta podría incluir algunas <code>CommonPrefixes</code> que no contienen claves.
Lista de versiones de objetos (anteriormente denominadas versiones del objeto GET Bucket)	Con acceso de LECTURA en un bucket, utilizando esta operación con el <code>versions</code> El subrecurso enumera los metadatos de todas las versiones de los objetos en el depósito.

Operación	Implementación
PonerBucketCors	Establece la configuración CORS para un depósito para que éste pueda atender solicitudes de origen cruzado. El uso compartido de recursos entre orígenes (CORS) es un mecanismo de seguridad que permite que las aplicaciones web cliente de un dominio accedan a recursos de un dominio diferente. Por ejemplo, supongamos que utiliza un depósito S3 llamado <code>images</code> para almacenar gráficos. Al establecer la configuración CORS para el <code>images</code> Cubo, puede permitir que las imágenes en ese cubo se muestren en el sitio web <code>http://www.example.com</code>.
Cifrado de PutBucket	Establece el estado de cifrado predeterminado de un depósito existente. Cuando el cifrado a nivel de bucket está habilitado, cualquier objeto nuevo que se añada al bucket se cifra. StorageGRID admite el cifrado del lado del servidor con claves administradas StorageGRID. Al especificar la regla de configuración de cifrado del lado del servidor, configure el <code>SSEAlgorithm</code> parámetro a <code>AES256</code>, y no utilices el <code>KMSMasterKeyID</code> parámetro. La configuración de cifrado predeterminada del depósito se ignora si la solicitud de carga de objetos ya especifica el cifrado (es decir, si la solicitud incluye el encabezado <code>x-amz-server-side-encryption-*</code> encabezado de solicitud).
Configuración del ciclo de vida de PutBucket (anteriormente llamado ciclo de vida del bucket PUT)	Crea una nueva configuración de ciclo de vida para el depósito o reemplaza una configuración de ciclo de vida existente. StorageGRID admite hasta 1000 reglas de ciclo de vida en una configuración de ciclo de vida. Cada regla puede incluir los siguientes elementos XML: • Vencimiento (Días, Fecha, <code>ExpiredObjectDeleteMarker</code>) • Caducidad de la versión no actual (versiones no actuales más recientes, días no actuales) • Filtro (Prefijo, Etiqueta) • Estado • IDENTIFICACIÓN StorageGRID no admite estas acciones: • Cancelar carga multiparte incompleta • Transición Ver "Crear la configuración del ciclo de vida de S3". Para comprender cómo la acción de Vencimiento en el ciclo de vida de un bucket interactúa con las instrucciones de ubicación de ILM, consulte "Cómo funciona ILM a lo largo de la vida de un objeto". Nota: La configuración del ciclo de vida del bucket se puede usar con buckets que tienen habilitado el bloqueo de objetos S3, pero la configuración del ciclo de vida del bucket no es compatible con buckets compatibles heredados.

Operación	Implementación
Configuración de notificación de PutBucket (anteriormente denominada notificación PUT Bucket)	Configura las notificaciones para el depósito utilizando el XML de configuración de notificaciones incluido en el cuerpo de la solicitud. Debe tener en cuenta los siguientes detalles de implementación: - StorageGRID admite Amazon Simple Notification Service (Amazon SNS) o temas de Kafka como destinos. No se admiten los puntos finales de Simple Queue Service (SQS) ni de Amazon Lambda. - El destino de las notificaciones debe especificarse como la URN de un punto final de StorageGRID . Los puntos finales se pueden crear utilizando el Administrador de inquilinos o la API de administración de inquilinos. El punto final debe existir para que la configuración de la notificación sea exitosa. Si el punto final no existe, un 400 Bad Request Se devuelve un error con el código <code>InvalidArgument</code> . - No se puede configurar una notificación para los siguientes tipos de eventos. Estos tipos de eventos no son compatibles. <code>s3:ReducedRedundancyLostObject</code> <code>s3:ObjectRestore:Completed</code> - Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar excepto que no incluyen algunas claves y utilizan valores específicos para otras, como se muestra en la siguiente lista: Fuente del evento <code>sgws:s3</code> awsRegión no incluido x-amz-id-2 no incluido arn <code>urn:sgws:s3:::bucket_name</code>
Política de depósito de basura	Establece la política asociada al depósito. Ver " Utilice políticas de acceso a grupos y buckets " .

Operación	Implementación
Replicación de PutBucket	Configura "Replicación de StorageGRID CloudMirror" para el depósito que utiliza el XML de configuración de replicación proporcionado en el cuerpo de la solicitud. Para la replicación de CloudMirror, debe tener en cuenta los siguientes detalles de implementación: • StorageGRID solo admite la versión 1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso de <code>Filter</code> elemento para reglas y sigue las convenciones V1 para la eliminación de versiones de objetos. Para más detalles, véase "Guía del usuario de Amazon Simple Storage Service: Configuración de replicación" . • La replicación de buckets se puede configurar en buckets versionados o no versionados. • Puede especificar un depósito de destino diferente en cada regla del XML de configuración de replicación. Un depósito de origen puede replicarse en más de un depósito de destino. • Los depósitos de destino deben especificarse como el URN de los puntos finales de StorageGRID , tal como se especifica en el Administrador de inquilinos o en la API de administración de inquilinos. Ver "Configurar la replicación de CloudMirror" . El punto final debe existir para que la configuración de la replicación sea exitosa. Si el punto final no existe, la solicitud falla como 400 Bad Request. El mensaje de error dice: <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</code> • No es necesario especificar un <code>Role</code> 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 la <code>STANDARD</code> clase de almacenamiento por defecto. • Si elimina un objeto del depósito de origen o elimina el depósito de origen en sí, el comportamiento de replicación entre regiones es el siguiente: ◦ Si elimina el objeto o el depósito antes de que se haya replicado, el objeto o depósito no se replica y no se le notifica. ◦ Si elimina el objeto o el depósito después de haberlo replicado, StorageGRID sigue el comportamiento de eliminación estándar de Amazon S3 para la versión 1 de la replicación entre regiones.

Operación	Implementación
Etiquetado de PutBucket	Utiliza el <code>tagging</code> subrecurso para agregar o actualizar un conjunto de etiquetas para un depósito. Al agregar etiquetas de depósito, tenga en cuenta las siguientes limitaciones: • Tanto StorageGRID como Amazon S3 admiten hasta 50 etiquetas para cada bucket. • Las etiquetas asociadas a un bucket deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener una longitud de hasta 128 caracteres Unicode. • Los valores de las etiquetas pueden tener una longitud de hasta 256 caracteres Unicode. • La clave y los valores distinguen entre mayúsculas y minúsculas. Precaución: Si se establece una etiqueta de política ILM no predeterminada para este depósito, habrá un <code>NTAP-SG-ILM-BUCKET-TAG</code> etiqueta de cubo con un valor asignado a ella. Asegúrese de que el <code>NTAP-SG-ILM-BUCKET-TAG</code> La etiqueta de bucket se incluye con el valor asignado en todas las solicitudes <code>PutBucketTagging</code>. No modifique ni elimine esta etiqueta. Nota: Esta operación sobrescribirá cualquier etiqueta actual que el depósito ya tenga. Si se omite alguna etiqueta existente del conjunto, dicha etiqueta se eliminará del depósito.
Versiones de PutBucket	Utiliza el <code>versioning</code> subrecurso para establecer el estado de control de versiones de un bucket existente. Puede establecer el estado de la versión con uno de los siguientes valores: • Habilitado: habilita el control de versiones de los objetos en el depósito. Todos los objetos agregados al depósito reciben un ID de versión único. • Suspendido: deshabilita el control de versiones de los objetos en el depósito. Todos los objetos agregados al depósito reciben el ID de la versión <code>null</code>.
Configuración de bloqueo de objeto de colocación	Configura o elimina el modo de retención predeterminado del depósito y el período de retención predeterminado. Si se modifica el período de retención predeterminado, la fecha de retención de las versiones de objetos existentes permanece igual y no se vuelve a calcular utilizando el nuevo período de retención predeterminado. Ver "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" para obtener información detallada.

Operaciones sobre objetos

Operaciones sobre objetos

Esta sección describe cómo el sistema StorageGRID implementa operaciones de API REST S3 para objetos.

Las siguientes condiciones se aplican a todas las operaciones de objetos:

- StorageGRID "valores de consistencia" son compatibles con todas las operaciones sobre objetos, con excepción de las siguientes:
 - ObtenerObjetoAcl
 - OPTIONS /
 - PonerObjetoLegalRetención
 - PonerRetenciónDeObjeto
 - Seleccionar contenido del objeto
- Las solicitudes de clientes conflictivas, como dos clientes que escriben en la misma clave, se resuelven según el criterio del "último que gana". El momento de la evaluación de "últimas victorias" se basa en cuándo el sistema StorageGRID completa una solicitud determinada y no en cuándo los clientes S3 comienzan una operación.
- Todos los objetos en un depósito StorageGRID son propiedad del propietario del depósito, incluidos los objetos creados por un usuario anónimo o por otra cuenta.
- No se puede acceder a los objetos de datos ingresados al sistema StorageGRID a través de Swift a través de S3.

La siguiente tabla describe cómo StorageGRID implementa las operaciones de objetos de la API REST de S3.

Operación	Implementación
Eliminar objeto	Autenticación multifactor (MFA) y el encabezado de respuesta <code>x-amz-mfa</code> no son compatibles Al procesar una solicitud <code>DeleteObject</code>, StorageGRID intenta eliminar inmediatamente todas las copias del objeto de todas las ubicaciones almacenadas. Si tiene éxito, StorageGRID devuelve una respuesta al cliente inmediatamente. Si no se pueden eliminar todas las copias en 30 segundos (por ejemplo, porque una ubicación no está disponible temporalmente), StorageGRID pone en cola las copias para su eliminación y luego indica el éxito al cliente. Control de versiones Para eliminar una versión específica, el solicitante debe ser el propietario del depósito y utilizar el <code>versionId</code> subrecurso. El uso de este subrecurso elimina permanentemente la versión. Si el <code>versionId</code> corresponde a un marcador de eliminación, el encabezado de respuesta <code>x-amz-delete-marker</code> se devuelve establecido en <code>true</code>. • Si se elimina un objeto sin el <code>versionId</code> subrecurso en un bucket con control de versiones habilitado, esto genera un marcador de eliminación. El <code>versionId</code> para el marcador de eliminación se devuelve utilizando el <code>x-amz-version-id</code> encabezado de respuesta y el <code>x-amz-delete-marker</code>. El encabezado de respuesta se devuelve configurado en <code>true</code>. • Si se elimina un objeto sin el <code>versionId</code> subrecurso en un bucket con control de versiones suspendido, esto da como resultado una eliminación permanente de una versión 'nula' ya existente o un marcador de eliminación 'nulo' y la generación de un nuevo marcador de eliminación 'nulo'. El <code>x-amz-delete-marker</code>. El encabezado de respuesta se devuelve configurado en <code>true</code>. Nota: En ciertos casos, pueden existir múltiples marcadores de eliminación para un objeto. Ver "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" para aprender cómo eliminar versiones de objetos en el modo GOBERNANZA.
Eliminar objetos (anteriormente llamado ELIMINAR Múltiples Objetos)	Autenticación multifactor (MFA) y el encabezado de respuesta <code>x-amz-mfa</code> no son compatibles Se pueden eliminar varios objetos en el mismo mensaje de solicitud. Ver "Utilice la API REST de S3 para configurar el bloqueo de objetos de S3" para aprender cómo eliminar versiones de objetos en el modo GOBERNANZA.

Operación	Implementación
Eliminar etiquetado de objetos	Utiliza el <code>tagging</code> subrecurso para eliminar todas las etiquetas de un objeto. Control de versiones Si el <code>versionId</code> Si 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 depósito versionado. Si la versión actual del objeto es un marcador de eliminación, se devuelve un estado "Método no permitido" con el <code>x-amz-delete-marker</code> encabezado de respuesta establecido en <code>true</code>.
Obtener objeto	"Obtener objeto"
ObtenerObjetoAcl	Si se proporcionan las credenciales de acceso necesarias para la cuenta, la operación devuelve una respuesta positiva y el ID, el nombre para mostrar y el permiso del propietario del objeto, lo que indica que el propietario tiene acceso completo al objeto.
Obtener retención legal de objeto	"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"
Obtener retención de objetos	"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"
Obtener etiquetado de objetos	Utiliza el <code>tagging</code> subrecurso para devolver todas las etiquetas de un objeto. Control de versiones Si el <code>versionId</code> Si 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 depósito versionado. Si la versión actual del objeto es un marcador de eliminación, se devuelve un estado "Método no permitido" con el <code>x-amz-delete-marker</code> encabezado de respuesta establecido en <code>true</code>.
Objeto principal	"Objeto principal"
Restaurar objeto	"Restaurar objeto"
PonerObjeto	"PonerObjeto"
Copiar objeto (anteriormente llamado Objeto PUT - Copiar)	"Copiar objeto"
PonerObjetoLegalRetención	"Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"

Operación	Implementación
PonerRetenciónDeObjeto	" Utilice la API REST de S3 para configurar el bloqueo de objetos de S3 "
Etiquetado de objetos puestos	Utiliza el <code>tagging</code> subrecurso para agregar un conjunto de etiquetas a un objeto existente. Límites de etiquetas de objetos Puede agregar etiquetas a objetos nuevos cuando los cargue o puede agregarlas a objetos existentes. Tanto StorageGRID como Amazon S3 admiten hasta 10 etiquetas para cada objeto. Las etiquetas asociadas a un objeto deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener una longitud de hasta 128 caracteres Unicode y los valores de etiqueta pueden tener una longitud de hasta 256 caracteres Unicode. La clave y los valores distinguen entre mayúsculas y minúsculas. Actualizaciones de etiquetas y comportamiento de ingesta Cuando utiliza <code>PutObjectTagging</code> para actualizar las etiquetas de un objeto, StorageGRID no vuelve a ingerir el objeto. Esto significa que no se utiliza la opción de Comportamiento de ingesta especificada en la regla ILM correspondiente. Cualquier cambio en la ubicación de objetos que se active mediante la actualización se realiza cuando ILM se vuelve a evaluar mediante procesos de fondo normales de ILM. Esto significa que si la regla ILM usa la opción Estricta para el comportamiento de ingesta, no se realiza ninguna acción si no se pueden realizar las ubicaciones de objetos requeridas (por ejemplo, porque una nueva ubicación requerida no está disponible). El objeto actualizado conserva su ubicación actual hasta que sea posible la ubicación requerida. Resolución de conflictos Las solicitudes de clientes conflictivas, como dos clientes que escriben en la misma clave, se resuelven según el criterio del "último que gana". El momento de la evaluación de "últimas victorias" se basa en cuándo el sistema StorageGRID completa una solicitud determinada y no en cuándo los clientes S3 comienzan una operación. Control de versiones Si el <code>versionId</code> Si el parámetro de consulta no se especifica en la solicitud, la operación agrega etiquetas a la versión más reciente del objeto en un depósito versionado. Si la versión actual del objeto es un marcador de eliminación, se devuelve un estado "Método no permitido" con el <code>x-amz-delete-marker</code> encabezado de respuesta establecido en <code>true</code>.
Seleccionar contenido del objeto	" Seleccionar contenido del objeto "

Utilice S3 Select

StorageGRID admite las siguientes cláusulas Select de Amazon S3, tipos de datos y operadores para ["Comando SelectObjectContent"](#) .



Cualquier artículo que no esté en la lista no será compatible.

Para la sintaxis, véase ["Seleccionar contenido del objeto"](#) . Para obtener más información sobre S3 Select, consulte la ["Documentación de AWS para S3 Select"](#) .

Solo las cuentas de inquilino que tienen S3 Select habilitado pueden emitir consultas SelectObjectContent. Ver el ["Consideraciones y requisitos para el uso de S3 Select"](#) .

Cláusulas

- Lista SELECT
- cláusula FROM
- cláusula WHERE
- Cláusula LIMIT

Tipos de datos

- bool
- entero
- cadena
- flotar
- decimal, numérico
- marca de tiempo

Operadores

Operadores lógicos

- Y
- NO
- O

Operadores de comparación

- <
- >
- <=
- >=
- =
- =
- <>

- !=
- ENTRE
- EN

Operadores de coincidencia de patrones

- COMO
- _
- %

Operadores unitarios

- ES NULO
- NO ES NULO

Operadores matemáticos

- +
- -
- *
- /
- %

StorageGRID sigue la precedencia del operador Amazon S3 Select.

Funciones agregadas

- AVG()
- CONTAR(*)
- MÁX()
- MÍNIMO()
- SUMA()

Funciones condicionales

- CASO
- JUNTARSE
- NULLIF

Funciones de conversión

- CAST (para tipos de datos admitidos)

Funciones de fecha

- FECHA_AÑADIR
- FECHA_DIFF

- EXTRACTO
- A_CADENA
- HASTA_LA_MARCA_DE_TIEMPO
- UTCNOW

Funciones de cadena

- LONGITUD_CHARACTER, LONGITUD_CHARACTER
- MÁS BAJO
- SUBCADENA
- RECORTAR
- SUPERIOR

Utilice cifrado del lado del servidor

El cifrado del lado del servidor le permite proteger los datos de sus objetos en reposo. StorageGRID cifra los datos a medida que escribe el objeto y los descifra cuando accede al objeto.

Si desea utilizar el cifrado del lado del servidor, puede elegir cualquiera de dos opciones mutuamente excluyentes, según cómo se administren las claves de cifrado:

- **SSE (cifrado del lado del servidor con claves administradas por StorageGRID)**: cuando emite una solicitud 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 emite una solicitud S3 para almacenar un objeto, proporciona su propia clave de cifrado. Cuando recupera un objeto, proporciona la misma clave de cifrado como parte de su solicitud. Si las dos claves de cifrado coinciden, el objeto se descifra y se devuelven los datos del objeto.

Si bien StorageGRID administra todas las operaciones de cifrado y descifrado de objetos, usted debe administrar las claves de cifrado que proporciona.



Las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente.



Si un objeto está cifrado con SSE o SSE-C, se ignoran todas las configuraciones de cifrado a nivel de bucket o de cuadrícula.

Utilice SSE

Para cifrar un objeto con una clave única administrada por StorageGRID, utilice el siguiente encabezado de solicitud:

```
x-amz-server-side-encryption
```

El encabezado de solicitud SSE es compatible con las siguientes operaciones de objeto:

- "PonerObjeto"
- "Copiar objeto"
- "Crear carga de varias partes"

Utilice SSE-C

Para cifrar un objeto con una clave única que usted administra, utiliza tres encabezados de solicitud:

Encabezado de solicitud	Descripción
x-amz-server-side-encryption-customer-algorithm	Especifique el algoritmo de cifrado. El valor del 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 ser de 256 bits y estar codificado en base64.
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 transmitió sin errores. El valor del resumen MD5 debe estar codificado en base64 de 128 bits.

Los encabezados de solicitud SSE-C son compatibles con las siguientes operaciones de objetos:

- "Obtener objeto"
- "Objeto principal"
- "PonerObjeto"
- "Copiar objeto"
- "Crear carga de varias partes"
- "Subir parte"
- "Subir copia parcial"

Consideraciones para el uso del cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C)

Antes de utilizar SSE-C, tenga en cuenta las siguientes consideraciones:

- Debes utilizar https.



StorageGRID rechaza cualquier solicitud realizada a través de HTTP al usar SSE-C. Por razones de seguridad, considere que cualquier clave que envíe accidentalmente a través de HTTP está comprometida. Deseche la llave y gírela según corresponda.

- La ETag en la respuesta no es el MD5 de los datos del objeto.
- Debe administrar la asignación de claves de cifrado a los objetos. StorageGRID no almacena claves de cifrado. Usted es responsable de rastrear la clave de cifrado que proporciona para cada objeto.

- Si su depósito tiene habilitada la gestión de versiones, cada versión del objeto debe tener su propia clave de cifrado. Usted es responsable de realizar el seguimiento de la clave de cifrado utilizada para cada versión del objeto.
- Dado que administra las claves de cifrado en el lado del cliente, también debe administrar cualquier protección adicional, como la rotación de claves, en el lado del cliente.



Las claves de cifrado que usted proporciona nunca se almacenan. Si pierde una clave de cifrado, perderá el objeto correspondiente.

- Si la replicación entre redes o la replicación de CloudMirror están configuradas para el bucket, no podrá ingerir objetos SSE-C. La operación de ingesta fallará.

Información relacionada

["Guía del usuario de Amazon S3: Uso del cifrado del lado del servidor con claves proporcionadas por el cliente \(SSE-C\)"](#)

Copiar objeto

Puede utilizar la solicitud S3 CopyObject para crear una copia de un objeto que ya esté almacenado en S3. Una operación CopyObject es lo mismo que realizar GetObject seguido de PutObject.

Resolver conflictos

Las solicitudes de clientes conflictivas, como dos clientes que escriben en la misma clave, se resuelven según el criterio del "último que gana". El momento de la evaluación de "últimas victorias" se basa en cuándo el sistema StorageGRID completa una solicitud determinada y no en cuándo los clientes S3 comienzan una operación.

Tamaño del objeto

El tamaño máximo *recomendado* para una sola operación PutObject es 5 GiB (5.368.709.120 bytes). Si tiene objetos de más de 5 GiB, utilice ["carga multiparte"](#) en cambio.

El tamaño máximo *admitido* para una sola operación PutObject es 5 TiB (5.497.558.138.880 bytes).



Si actualizó desde StorageGRID 11.6 o una versión anterior, se activará la alerta de tamaño de objeto PUT de S3 demasiado grande si intenta cargar un objeto que supere los 5 GiB. Si tiene una nueva instalación de StorageGRID 11.7 o 11.8, la alerta no se activará en este caso. Sin embargo, para alinearse con el estándar AWS S3, las futuras versiones de StorageGRID no admitirán cargas de objetos de más de 5 GiB.

Caracteres UTF-8 en metadatos de usuario

Si una solicitud incluye valores UTF-8 (sin escapar) 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 caracteres UTF-8 escapados incluidos en el nombre de clave o el valor de los metadatos definidos por el usuario. Los caracteres UTF-8 escapados se tratan como caracteres ASCII:

- Las solicitudes tienen éxito si los metadatos definidos por el usuario incluyen caracteres UTF-8 escapados.

- StorageGRID no devuelve el `x-amz-missing-meta` encabezado si el valor interpretado del nombre o valor de la 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 le permite copiar el objeto y los metadatos asociados.

Puedes especificar `REPLACE` para sobrescribir los metadatos existentes al copiar el objeto o para 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.

Puedes especificar `REPLACE` para sobrescribir las etiquetas existentes al copiar el objeto o para 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, se utilizan las configuraciones de retención predeterminadas del depósito para calcular el modo de versión del objeto y la fecha de retención. Ver ["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#).

- Encabezados de solicitud SSE:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption-customer-key`

- `x-amz-server-side-encryption-customer-algorithm`

Ver [Encabezados de solicitud para el cifrado del lado del servidor](#)

Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`

Cuando copia un objeto, si el objeto de origen tiene una suma de comprobación, StorageGRID no copia ese valor de suma de comprobación al nuevo objeto. Este comportamiento se aplica independientemente de si intenta utilizarlo o no. `x-amz-checksum-algorithm` en la solicitud de objeto.

- `x-amz-website-redirect-location`

Opciones de clase de almacenamiento

El `x-amz-storage-class` Se admite el encabezado de solicitud y afecta la cantidad de copias de objetos que crea StorageGRID si la regla ILM correspondiente usa la confirmación dual o equilibrada. ["opción de ingesta"](#).

- `STANDARD`

(Predeterminado) Especifica una operación de ingesta de confirmación dual cuando la regla ILM usa la opción Confirmación dual o cuando la opción Equilibrada recurre a la creación de copias provisionales.

- `REDUCED_REDUNDANCY`

Especifica una operación de ingesta de confirmación única cuando la regla ILM usa la opción de confirmación dual o cuando la opción Equilibrada recurre a la creación de copias provisionales.



Si está ingiriendo un objeto en un depósito con el bloqueo de objetos S3 habilitado, `REDUCED_REDUNDANCY` La opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, el `REDUCED_REDUNDANCY` La opción devuelve un error. StorageGRID siempre realizará una ingesta de confirmación dual para garantizar que se cumplan los requisitos de cumplimiento.

Uso de `x-amz-copy-source` en `CopyObject`

Si el depósito de origen y la clave se especifican en el `x-amz-copy-source` encabezado, son diferentes del depósito de destino y la clave, se escribe una copia de los datos del objeto de origen en el destino.

Si el origen y el destino coinciden, y el `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 ingerir el objeto. Esto tiene dos consecuencias importantes:

- No se puede utilizar CopyObject para cifrar un objeto existente en un lugar, ni para cambiar el cifrado de un objeto existente en un lugar. Si usted suministra el `x-amz-server-side-encryption` encabezado o el `x-amz-server-side-encryption-customer-algorithm` encabezado, StorageGRID rechaza la solicitud y devuelve `XNotImplemented`.
- No se utiliza la opción de Comportamiento de ingestión especificada en la regla ILM correspondiente. Cualquier cambio en la ubicación de objetos que se active mediante la actualización se realiza cuando ILM se vuelve a evaluar mediante procesos de fondo normales de ILM.

Esto significa que si la regla ILM usa la opción Estricta para el comportamiento de ingesta, no se realiza ninguna acción si no se pueden realizar las ubicaciones de objetos requeridas (por ejemplo, porque una nueva ubicación requerida no está disponible). El objeto actualizado conserva su ubicación actual hasta que sea posible la ubicación requerida.

Encabezados de solicitud para el cifrado del lado del servidor

Si usted ["utilizar cifrado del lado 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 está cifrado mediante una clave proporcionada por el cliente (SSE-C), debe incluir los siguientes tres encabezados en la solicitud CopyObject, para que el objeto pueda descifrarse y luego copiarse:
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Especificar AES256 .
 - `x-amz-copy-source-server-side-encryption-customer-key`:Especifique la clave de cifrado que proporcionó cuando creó el objeto de origen.
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`:Especifique el resumen MD5 que proporcionó cuando creó el objeto de origen.
- Si desea cifrar el objeto de destino (la copia) con una clave única que usted proporciona y administra, incluya los siguientes tres encabezados:
 - `x-amz-server-side-encryption-customer-algorithm`: Especificar AES256 .
 - `x-amz-server-side-encryption-customer-key`:Especifique una nueva clave de cifrado para el objeto de destino.
 - `x-amz-server-side-encryption-customer-key-MD5`:Especifique el resumen MD5 de la nueva clave de cifrado.



Las claves de cifrado que 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 los objetos, revise las consideraciones para ["utilizando cifrado del lado del servidor"](#) .

- Si desea cifrar el objeto de destino (la copia) con una clave única administrada por StorageGRID (SSE), incluya este encabezado en la solicitud CopyObject:
 - `x-amz-server-side-encryption`



El server-side-encryption El valor del objeto no se puede actualizar. En lugar de eso, haga una copia con un nuevo server-side-encryption valor usando `x-amz-metadata-directive: REPLACE`.

Control de versiones

Si el depósito de origen tiene versiones, puede utilizar el `x-amz-copy-source` encabezado para copiar la última versión de un objeto. Para copiar una versión específica de un objeto, debe especificar explícitamente la versión a copiar utilizando el `versionId` subrecurso. Si el depósito de destino está versionado, la versión generada se devuelve en el `x-amz-version-id` encabezado de respuesta. Si se suspende el control de versiones para el depósito de destino, entonces `x-amz-version-id` devuelve un valor "nulo".

Obtener objeto

Puede utilizar la solicitud `GetObject` de S3 para recuperar un objeto de un depósito de S3.

GetObject y objetos multipart

Puedes utilizar el `partNumber` parámetro de solicitud para recuperar una parte específica de un objeto multiparte o segmentado. El `x-amz-mp-parts-count` El elemento de respuesta indica cuántas partes tiene el objeto.

Puedes configurar `partNumber` a 1 tanto para objetos segmentados/multiparte como para objetos no segmentados/no multiparte; sin embargo, el `x-amz-mp-parts-count` El elemento de respuesta solo se devuelve para objetos segmentados o multiparte.

Caracteres UTF-8 en metadatos de usuario

StorageGRID no analiza ni interpreta caracteres UTF-8 escapados en metadatos definidos por el usuario. Las solicitudes `GET` para 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 la clave incluye caracteres no imprimibles.

Encabezado de solicitud compatible

Se admite el siguiente encabezado de solicitud:

- `x-amz-checksum-mode`: Especificar `ENABLED`

El Range El encabezado no es compatible con `x-amz-checksum-mode` para `ObtenerObjeto`. Cuando incluyes `Range` en la solicitud con `x-amz-checksum-mode` habilitado, StorageGRID no devuelve un valor de suma de comprobación en la respuesta.

Encabezado de solicitud no compatible

El siguiente encabezado de solicitud no es compatible y devuelve `XNotImplemented`:

- `x-amz-website-redirect-location`

Control de versiones

Si un `versionId` Si no se especifica el subrecurso, la operación obtiene la versión más reciente del objeto en un depósito versionado. Si la versión actual del objeto es un marcador de eliminación, se devuelve un estado "No encontrado" con el `x-amz-delete-marker` encabezado de respuesta establecido en `true`.

Encabezados de solicitud para cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)

Utilice los tres encabezados si el objeto está encriptado con una clave única que usted proporcionó.

- `x-amz-server-side-encryption-customer-algorithm`: Especificar AES256.
- `x-amz-server-side-encryption-customer-key`: Especifique su clave de cifrado para el 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 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 los objetos, revise las consideraciones en ["Utilice cifrado del lado del servidor"](#).

Comportamiento de GetObject para objetos del grupo de almacenamiento en la nube

Si un objeto ha sido almacenado en un ["Grupo de almacenamiento en la nube"](#), el comportamiento de una solicitud `GetObject` depende del estado del objeto. Ver ["Objeto principal"](#) Para más detalles.



Si un objeto está almacenado en un grupo de almacenamiento en la nube y también existen una o más copias del objeto en la red, las solicitudes `GetObject` intentarán recuperar datos de la red, antes de recuperarlos del grupo de almacenamiento en la nube.

Estado del objeto	Comportamiento de GetObject
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, u objeto almacenado en un grupo de almacenamiento tradicional o que utiliza codificación de borrado	200 OK Se recupera una copia del objeto.
Objeto en el grupo de almacenamiento en la nube pero que aún no ha pasado a un estado no recuperable	200 OK Se recupera una copia del objeto.
Objeto en transición a un estado no recuperable	403 Forbidden , InvalidObjectState Utilice un "Restaurar objeto" solicitud para restaurar el objeto a un estado recuperable.
Objeto en proceso de restauración desde un estado no recuperable	403 Forbidden , InvalidObjectState Espere a que se complete la solicitud <code>RestoreObject</code> .

Estado del objeto	Comportamiento de GetObject
Objeto completamente restaurado al grupo de almacenamiento en la nube	200 OK Se recupera una copia del objeto.

Objetos multiparte o segmentados en un grupo de almacenamiento en la nube

Si cargó un objeto de varias partes o si StorageGRID dividió un objeto grande en segmentos, StorageGRID determina si el objeto está disponible en el grupo de almacenamiento en la nube mediante el muestreo de un subconjunto de las partes o segmentos del objeto. En algunos casos, una solicitud GetObject podría devolver incorrectamente 200 OK cuando algunas partes del objeto ya han sido trasladadas a un estado no recuperable o cuando algunas partes del objeto aún no han sido restauradas.

En estos casos:

- La solicitud GetObject podría devolver algunos datos pero detenerse a mitad de la transferencia.
- Una solicitud GetObject posterior podría devolver 403 Forbidden .

GetObject y replicación entre cuadrículas

Si estas usando "federación de red" y "replicación entre redes" está habilitado para un bucket, el cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud GetObject. La respuesta incluye el StorageGRID específico x-ntap-sg-cgr-replication-status encabezado de respuesta, que tendrá uno de los siguientes valores:

Red	Estado de replicación
Fuente	• COMPLETADO: La replicación fue exitosa. • PENDIENTE: El objeto aún no ha sido replicado. • FALLO: La replicación falló con un error permanente. Un usuario debe resolver el error.
Destino	RÉPLICA : El objeto fue replicado desde la cuadrícula de origen.



StorageGRID no es compatible con x-amz-replication-status encabezamiento.

Objeto principal

Puede utilizar la solicitud S3 HeadObject para recuperar metadatos de un objeto sin devolver el objeto en sí. Si el objeto está almacenado en un grupo de almacenamiento en la nube, puede usar HeadObject para determinar el estado de transición del objeto.

Objetos HeadObject y multipart

Puedes utilizar el partNumber parámetro de solicitud para recuperar metadatos para una parte específica de un objeto multiparte o segmentado. El x-amz-mp-parts-count El elemento de respuesta indica cuántas partes tiene el objeto.

Puedes configurar `partNumber` a 1 tanto para objetos segmentados/multiparte como para objetos no segmentados/no multiparte; sin embargo, el `x-amz-mp-parts-count` El elemento de respuesta solo se devuelve para objetos segmentados o multiparte.

Caracteres UTF-8 en metadatos de usuario

StorageGRID no analiza ni interpreta caracteres UTF-8 escapados en metadatos definidos por el usuario. Las solicitudes HEAD para 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 la clave incluye caracteres no imprimibles.

Encabezado de solicitud compatible

Se admite el siguiente encabezado de solicitud:

- `x-amz-checksum-mode`

El `partNumber` parámetro y `Range` Los encabezados no son compatibles con `x-amz-checksum-mode` para `HeadObject`. Cuando los incluyas en la solicitud con `x-amz-checksum-mode` habilitado, StorageGRID no devuelve un valor de suma de comprobación en la respuesta.

Encabezado de solicitud no compatible

El siguiente encabezado de solicitud no es compatible y devuelve `XNotImplemented`:

- `x-amz-website-redirect-location`

Control de versiones

Si un `versionId` Si no se especifica el subrecurso, la operación obtiene la versión más reciente del objeto en un depósito versionado. Si la versión actual del objeto es un marcador de eliminación, se devuelve un estado "No encontrado" con el `x-amz-delete-marker` encabezado de respuesta establecido en `true`.

Encabezados de solicitud para cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)

Utilice estos tres encabezados si el objeto está encriptado con una clave única que usted proporcionó.

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique su clave de cifrado para el 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 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 los objetos, revise las consideraciones en "[Utilice cifrado del lado del servidor](#)".

Respuestas de HeadObject para objetos de Cloud Storage Pool

Si el objeto se almacena en un "[Grupo de almacenamiento en la nube](#)", se devuelven los siguientes encabezados de respuesta:

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Los encabezados de respuesta brindan información sobre el estado de un objeto a medida que se mueve a un grupo de almacenamiento en la nube, opcionalmente pasa a un estado no recuperable y se restaura.

Estado del objeto	Respuesta a HeadObject
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, u objeto almacenado en un grupo de almacenamiento tradicional o que utiliza codificación de borrado	200 OK(No se devuelve ningún encabezado de respuesta especial).
Objeto en el grupo de almacenamiento en la nube pero que aún no ha pasado a un estado no recuperable	200 OK <code>x-amz-storage-class: GLACIER</code> <code>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code> Hasta que el objeto pase a un estado no recuperable, el valor de <code>expiry-date</code> Está ambientado en un momento distante en el futuro. El tiempo exacto de transición no está controlado por el sistema StorageGRID .
El objeto ha pasado al estado no recuperable, pero también existe al menos una copia en la cuadrícula	200 OK <code>x-amz-storage-class: GLACIER</code> <code>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code> El valor de <code>expiry-date</code> Está ambientado en un momento distante en el futuro. Nota: Si la copia en la red no está disponible (por ejemplo, un nodo de almacenamiento está inactivo), debe emitir un "Restaurar objeto" solicitud para restaurar la copia del grupo de almacenamiento en la nube antes de poder recuperar el objeto con éxito.
El objeto pasó a un estado no recuperable y no existe ninguna copia en la cuadrícula	200 OK <code>x-amz-storage-class: GLACIER</code>

Estado del objeto	Respuesta a HeadObject
Objeto en proceso de restauración desde un estado no recuperable	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="true"
Objeto completamente restaurado al grupo de almacenamiento en la nube	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT" El expiry-date Indica cuándo el objeto en el grupo de almacenamiento en la nube volverá a un estado no recuperable.

Objetos multiparte o segmentados en el grupo de almacenamiento en la nube

Si cargó un objeto de varias partes o si StorageGRID dividió un objeto grande en segmentos, StorageGRID determina si el objeto está disponible en el grupo de almacenamiento en la nube mediante el muestreo de un subconjunto de las partes o segmentos del objeto. En algunos casos, una solicitud HeadObject podría devolver incorrectamente `x-amz-restore: ongoing-request="false"` cuando algunas partes del objeto ya han sido trasladadas a un estado no recuperable o cuando algunas partes del objeto aún no han sido restauradas.

Replicación de HeadObject y entre cuadrículas

Si estas usando ["federación de red"](#) y ["replicación entre redes"](#) está habilitado para un bucket, el cliente S3 puede verificar el estado de replicación de un objeto emitiendo una solicitud HeadObject. La respuesta incluye el StorageGRID específico `x-ntap-sg-cgr-replication-status` encabezado de respuesta, que tendrá uno de los siguientes valores:

Red	Estado de replicación
Fuente	• COMPLETADO: La replicación fue exitosa. • PENDIENTE: El objeto aún no ha sido replicado. • FALLO: La replicación falló con un error permanente. Un usuario debe resolver el error.
Destino	RÉPLICA: El objeto fue replicado desde la cuadrícula de origen.



StorageGRID no es compatible con `x-amz-replication-status` encabezamiento.

PonerObjeto

Puede utilizar la solicitud S3 PutObject para agregar un objeto a un depósito.

Resolver conflictos

Las solicitudes de clientes conflictivas, como dos clientes que escriben en la misma clave, se resuelven según el criterio del "último que gana". El momento de la evaluación de "últimas victorias" se basa en cuándo el sistema StorageGRID completa una solicitud determinada y no en cuándo los clientes S3 comienzan una operación.

Tamaño del objeto

El tamaño máximo *recomendado* para una sola operación PutObject es 5 GiB (5.368.709.120 bytes). Si tiene objetos de más de 5 GiB, utilice ["carga multiparte"](#) en cambio.

El tamaño máximo *admitido* para una sola operación PutObject es 5 TiB (5.497.558.138.880 bytes).



Si actualizó desde StorageGRID 11.6 o una versión anterior, se activará la alerta de tamaño de objeto PUT de S3 demasiado grande si intenta cargar un objeto que supere los 5 GiB. Si tiene una nueva instalación de StorageGRID 11.7 o 11.8, la alerta no se activará en este caso. Sin embargo, para alinearse con el estándar AWS S3, las futuras versiones de StorageGRID no admitirán cargas de objetos de más de 5 GiB.

Tamaño de los metadatos del usuario

Amazon S3 limita el tamaño de los metadatos definidos por el usuario dentro de cada encabezado de solicitud PUT a 2 KB. StorageGRID limita los metadatos del usuario a 24 KiB. El tamaño de los metadatos definidos por el usuario se mide tomando la suma de la cantidad de bytes en la codificación UTF-8 de cada clave y valor.

Caracteres UTF-8 en metadatos de usuario

Si una solicitud incluye valores UTF-8 (sin escapar) 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 caracteres UTF-8 escapados incluidos en el nombre de clave o el valor de los metadatos definidos por el usuario. Los caracteres UTF-8 escapados se tratan como caracteres ASCII:

- Las solicitudes PutObject, CopyObject, GetObject y HeadObject tienen éxito si los metadatos definidos por el usuario incluyen caracteres UTF-8 escapados.
- StorageGRID no devuelve el `x-amz-missing-meta` encabezado si el valor interpretado del nombre o valor de la clave incluye caracteres no imprimibles.

Límites de etiquetas de objetos

Puede agregar etiquetas a objetos nuevos cuando los cargue o puede agregarlas a objetos existentes. Tanto StorageGRID como Amazon S3 admiten hasta 10 etiquetas para cada objeto. Las etiquetas asociadas a un objeto deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener una longitud de hasta 128 caracteres Unicode y los valores de etiqueta pueden tener una longitud de hasta 256 caracteres Unicode. La clave y los valores distinguen entre mayúsculas y minúsculas.

Propiedad de los objetos

En StorageGRID, todos los objetos son propiedad de la cuenta del propietario del depósito, incluidos los objetos creados por una cuenta que no es del propietario o un usuario anónimo.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- Cache-Control
- Content-Disposition
- Content-Encoding

Cuando se especifica `aws-chunked` para `Content-Encoding` StorageGRID no verifica los siguientes elementos:

- StorageGRID no verifica la `chunk-signature` contra los datos del fragmento.
- StorageGRID no verifica el valor que usted proporciona `x-amz-decoded-content-length` contra el objeto.

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

Se admite la codificación de transferencia fragmentada si `aws-chunked`. También se utiliza la firma de carga útil.

- `x-amz-checksum-sha256`
- `x-amz-meta-`, seguido de un par nombre-valor que contiene metadatos definidos por el usuario.

Al especificar el par nombre-valor para los metadatos definidos por el usuario, utilice este formato general:

```
x-amz-meta-name: value
```

Si desea utilizar la opción **Hora de creación definida por el usuario** como Hora de referencia para una regla ILM, debe utilizar `creation-time` como el nombre de los metadatos que registran cuándo se creó el objeto. Por ejemplo:

```
x-amz-meta-creation-time: 1443399726
```

El valor de `creation-time` se evalúa en segundos desde el 1 de enero de 1970.



Una regla ILM no puede utilizar tanto un **tiempo de creación definido por el usuario** para el tiempo de referencia como la opción de ingesta equilibrada o estricta. Se devuelve un error cuando se crea la regla ILM.

- `x-amz-tagging`
- 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, se utilizan las configuraciones de retención predeterminadas del depósito para calcular el modo de versión del objeto y la fecha de retención. Ver ["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#).

- Encabezados de solicitud SSE:
 - `x-amz-server-side-encryption`
 - `x-amz-server-side-encryption-customer-key-MD5`
 - `x-amz-server-side-encryption-customer-key`
 - `x-amz-server-side-encryption-customer-algorithm`

Ver [Encabezados de solicitud para el cifrado del lado del servidor](#)

Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

El `x-amz-website-redirect-location` el encabezado regresa `XNotImplemented`.

Opciones de clase de almacenamiento

El `x-amz-storage-class` Se admite el encabezado de solicitud. El valor presentado para `x-amz-storage-class` afecta la forma en que StorageGRID protege los datos de los objetos durante la ingesta y no la cantidad de copias persistentes del objeto que se almacenan en el sistema StorageGRID (lo cual está determinado por ILM).

Si la regla ILM que coincide con un objeto ingerido utiliza la opción Ingesta estricta, `x-amz-storage-class` El encabezado no tiene efecto.

Los siguientes valores se pueden utilizar para `x-amz-storage-class`:

- STANDARD(Por defecto)

- **Confirmación dual:** si la regla ILM especifica la opción de confirmación dual para el comportamiento de ingesta, tan pronto como se ingiere un objeto, se crea una segunda copia de ese objeto y se distribuye a un nodo de almacenamiento diferente (confirmación dual). Cuando se evalúa el ILM, StorageGRID determina si estas copias provisionales iniciales satisfacen las instrucciones de ubicación de la regla. De lo contrario, es posible que sea necesario realizar nuevas copias de objetos en ubicaciones diferentes y eliminar las copias provisionales iniciales.
- **Equilibrado:** si la regla ILM especifica la opción Equilibrado y StorageGRID no puede realizar inmediatamente todas las copias especificadas en la regla, StorageGRID realiza dos copias provisionales en diferentes nodos de almacenamiento.

Si StorageGRID puede crear inmediatamente todas las copias de objetos especificadas en la regla ILM (ubicación sincrónica), `x-amz-storage-class` El encabezado no tiene ningún efecto.

- **REDUCED_REDUNDANCY**

- **Confirmación dual:** si la regla ILM especifica la opción de Confirmación dual para Comportamiento de ingesta, StorageGRID crea una única copia provisional a medida que se ingiere el objeto (confirmación única).
- **Equilibrado:** si la regla ILM especifica la opción Equilibrado, StorageGRID realiza una única copia provisional solo si el sistema no puede realizar inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar la colocación sincrónica, este encabezado no tiene ningún efecto. El `REDUCED_REDUNDANCY` Esta opción se utiliza mejor cuando la regla ILM que coincide con el objeto crea una única copia replicada. En este caso se utiliza `REDUCED_REDUNDANCY` Elimina la creación y eliminación innecesarias de una copia de objeto adicional para cada operación de ingesta.

Usando el `REDUCED_REDUNDANCY` Esta opción no se recomienda en otras circunstancias.

`REDUCED_REDUNDANCY` aumenta el riesgo de pérdida de datos de objetos durante la ingesta. Por ejemplo, podría perder datos si la copia única se almacena inicialmente en un nodo de almacenamiento que falla antes de que pueda ocurrir la evaluación de ILM.



Tener solo una copia replicada por un período de tiempo determinado pone los datos en riesgo de pérdida permanente. Si solo existe una copia replicada de un objeto, ese objeto se pierde si un nodo de almacenamiento falla o tiene un error significativo. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como actualizaciones.

Especificando `REDUCED_REDUNDANCY` Sólo afecta la cantidad de copias que se crean cuando se ingiere un objeto por primera vez. No afecta la cantidad de copias del objeto que se realizan cuando las políticas ILM activas evalúan el objeto y no hace que los datos se almacenen en niveles inferiores de redundancia en el sistema StorageGRID .



Si está ingiriendo un objeto en un depósito con el bloqueo de objetos S3 habilitado, `REDUCED_REDUNDANCY` La opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, el `REDUCED_REDUNDANCY` La opción devuelve un error. StorageGRID siempre realizará una ingesta de confirmación dual para garantizar que se cumplan los requisitos de cumplimiento.

Encabezados de solicitud para el cifrado del lado del servidor

Puede utilizar los siguientes encabezados de solicitud para cifrar un objeto con cifrado del lado 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 administrada por

StorageGRID.

- `x-amz-server-side-encryption`

Cuando el `x-amz-server-side-encryption` El encabezado no está incluido en la solicitud `PutObject`, la cuadrícula completa ["configuración de cifrado de objetos almacenados"](#) se omite de la respuesta `PutObject`.

- **SSE-C:** utilice estos tres encabezados si desea cifrar el objeto con una clave única que usted proporcione y administre.
 - `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256` .
 - `x-amz-server-side-encryption-customer-key`:Especifique su clave de cifrado para el nuevo objeto.
 - `x-amz-server-side-encryption-customer-key-MD5`:Especifique el resumen MD5 de la clave de cifrado del nuevo objeto.



Las claves de cifrado que 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 los objetos, revise las consideraciones para ["utilizando cifrado del lado del servidor"](#) .



Si un objeto está cifrado con SSE o SSE-C, se ignoran todas las configuraciones de cifrado a nivel de bucket o de cuadrícula.

Control de versiones

Si el control de versiones está habilitado para un bucket, se creará un único `versionId` Se genera automáticamente para la versión del objeto que se está almacenando. Este `versionId` También se devuelve en la respuesta utilizando el `x-amz-version-id` encabezado de respuesta.

Si se suspende el control de versiones, la versión del objeto se almacena con un valor nulo. `versionId` y si ya existe una versión nula, se sobrescribirá.

Cálculos de firma para el encabezado de autorización

Al utilizar el `Authorization` encabezado para autenticar solicitudes, StorageGRID se diferencia de AWS de las siguientes maneras:

- StorageGRID no requiere `host` encabezados que se incluirán dentro `CanonicalHeaders` .
- StorageGRID no requiere `Content-Type` para ser incluido dentro `CanonicalHeaders` .
- StorageGRID no requiere `x-amz-*` encabezados que se incluirán dentro `CanonicalHeaders` .



Como práctica recomendada general, incluya siempre estos encabezados dentro `CanonicalHeaders` para garantizar que se verifiquen; sin embargo, si excluye estos encabezados, StorageGRID no devuelve un error.

Para más detalles, consulte ["Cálculos de firma para el encabezado de autorización: transferencia de carga útil en un solo fragmento \(AWS Signature versión 4\)"](#) .

Información relacionada

- ["Administrar objetos con ILM"](#)
- ["Referencia de la API de Amazon Simple Storage Service: PutObject"](#)

Restaurar objeto

Puede utilizar la solicitud S3 RestoreObject para restaurar un objeto almacenado en un grupo de almacenamiento en la nube.

Tipo de solicitud admitido

StorageGRID solo admite solicitudes RestoreObject para restaurar un objeto. No es compatible con el `SELECT` tipo de restauración. Seleccione solicitudes de devolución `XNotImplemented`.

Control de versiones

Opcionalmente, especifique `versionId` para restaurar una versión específica de un objeto en un depósito versionado. Si no lo especifica `versionId`, se restaura la versión más reciente del objeto

Comportamiento de RestoreObject en objetos del grupo de almacenamiento en la nube

Si un objeto ha sido almacenado en un ["Grupo de almacenamiento en la nube"](#) Una solicitud RestoreObject tiene el siguiente comportamiento, según el estado del objeto. Ver ["Objeto principal"](#) Para más detalles.



Si un objeto está almacenado en un grupo de almacenamiento en la nube y también existen una o más copias del objeto en la red, no es necesario restaurar el objeto emitiendo una solicitud RestoreObject. En cambio, la copia local se puede recuperar directamente, mediante una solicitud GetObject.

Estado del objeto	Comportamiento de RestoreObject
Objeto ingerido en StorageGRID pero aún no evaluado por ILM, o el objeto no está en un grupo de almacenamiento en la nube	403 Forbidden , InvalidObjectState
Objeto en el grupo de almacenamiento en la nube pero que aún no ha pasado a un estado no recuperable	200 OK No se realizan cambios Nota: Antes de que un objeto pase a un estado no recuperable, no se puede cambiar su <code>expiry-date</code>.

Estado del objeto	Comportamiento de RestoreObject
Objeto en transición a un estado no recuperable	`202 Accepted` Restaura una copia recuperable del objeto en el grupo de almacenamiento en la nube durante la cantidad de días especificada en el cuerpo de la solicitud. Al final de este período, el objeto vuelve a un estado no recuperable. Opcionalmente, utilice el <code>Tier</code> Elemento de solicitud para determinar cuánto tiempo tardará en finalizar el trabajo de restauración(<code>Expedited</code>, <code>Standard</code>, o <code>Bulk</code>). Si no lo especifica <code>Tier</code>, el <code>Standard</code> Se utiliza el nivel. Importante: Si un objeto se ha transferido a S3 Glacier Deep Archive o el grupo de almacenamiento en la nube usa almacenamiento de blobs de Azure, no podrá restaurarlo mediante el <code>Expedited</code> nivel. Se devuelve el siguiente error <code>403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.</code>
Objeto en proceso de restauración desde un estado no recuperable	<code>409 Conflict, RestoreAlreadyInProgress</code>
Objeto completamente restaurado al grupo de almacenamiento en la nube	<code>200 OK</code> Nota: Si un objeto se ha restaurado a un estado recuperable, puede cambiar su <code>expiry-date</code> volviendo a emitir la solicitud <code>RestoreObject</code> con un nuevo valor para <code>Days</code>. La fecha de restauración se actualiza en relación con el momento de la solicitud.

Seleccionar contenido del objeto

Puede utilizar la solicitud S3 `SelectObjectContent` para filtrar el contenido de un objeto S3 según una declaración SQL simple.

Para más información véase ["Referencia de la API de Amazon Simple Storage Service: SelectObjectContent"](#).

Antes de empezar

- La cuenta de inquilino tiene el permiso S3 `Select`.
- Tienes `s3:GetObject` Permiso para el objeto que desea consultar.
- El objeto que desea consultar debe estar en uno de los siguientes formatos:
 - **CSV.** Se puede utilizar tal cual o comprimido en archivos GZIP o BZIP2.
 - **Parquet.** Requisitos adicionales para los objetos Parquet:
 - S3 Select solo admite la compresión en columnas mediante GZIP o Snappy. S3 Select no admite la compresión de objetos completos para objetos Parquet.
 - S3 Select no admite la salida Parquet. Debe especificar el formato de salida como CSV o JSON.
 - El tamaño máximo del grupo de filas sin comprimir es 512 MB.
 - Debe utilizar los tipos de datos especificados en el esquema del objeto.

- No se pueden utilizar los tipos lógicos INTERVAL, JSON, LIST, TIME o UUID.
- Su expresión SQL tiene una longitud máxima de 256 KB.
- Cualquier registro en la entrada o en los resultados tiene una longitud máxima de 1 MiB.

Ejemplo de sintaxis de solicitud CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <CSV>
      <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
      <Comments>#</Comments>
      <FieldDelimiter>\t</FieldDelimiter>
      <FileHeaderInfo>USE</FileHeaderInfo>
      <QuoteCharacter>'</QuoteCharacter>
      <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
      <RecordDelimiter>\n</RecordDelimiter>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

Ejemplo de sintaxis de solicitud de Parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <PARQUET>
    </PARQUET>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

Ejemplo de consulta SQL

Esta consulta obtiene el nombre del estado, las poblaciones de 2010, las poblaciones estimadas de 2015 y el porcentaje de cambio de los datos del censo de EE. UU. Los registros del archivo que no son estados se ignoran.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

Las primeras líneas del archivo a consultar, SUB-EST2020_ALL.csv , luce así:


```
SUMLEV, STATE, COUNTY, PLACE, COUSUB, CONCIT, PRIMGEO_FLAG, FUNCSTAT, NAME, STNAME,
CENSUS2010POP,
ESTIMATESBASE2010, POPESTIMATE2010, POPESTIMATE2011, POPESTIMATE2012, POPESTIM
ATE2013, POPESTIMATE2014,
POPESTIMATE2015, POPESTIMATE2016, POPESTIMATE2017, POPESTIMATE2018, POPESTIMAT
E2019, POPESTIMATE042020,
POPESTIMATE2020
040, 01, 000, 00000, 00000, 00000, 0, A, Alabama, Alabama, 4779736, 4780118, 4785514, 4
799642, 4816632, 4831586,
4843737, 4854803, 4866824, 4877989, 4891628, 4907965, 4920706, 4921532
162, 01, 000, 00124, 00000, 00000, 0, A, Abbeville
city, Alabama, 2688, 2705, 2699, 2694, 2645, 2629, 2610, 2602,
2587, 2578, 2565, 2555, 2555, 2553
162, 01, 000, 00460, 00000, 00000, 0, A, Adamsville
city, Alabama, 4522, 4487, 4481, 4474, 4453, 4430, 4399, 4371,
4335, 4304, 4285, 4254, 4224, 4211
162, 01, 000, 00484, 00000, 00000, 0, A, Addison
town, Alabama, 758, 754, 751, 750, 745, 744, 742, 734, 734, 728,
725, 723, 719, 717
```

Ejemplo de uso de AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Las primeras líneas del archivo de salida, changes.csv , luce así:

```
Alabama, 4779736, 4854803, 1.5705260708959658022953568983726297854
Alaska, 710231, 738430, 3.9703983633493891424057806544631253775
Arizona, 6392017, 6832810, 6.8959922978928247531256565807005832431
Arkansas, 2915918, 2979732, 2.1884703204959810255295244928012378949
California, 37253956, 38904296, 4.4299724839960620557988526104449148971
Colorado, 5029196, 5454328, 8.4532796097030221132761578590295546246
```

Ejemplo de uso de AWS-CLI (Parquet)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}' --output-serialization
'{"CSV":{}}' changes.csv
```

Las primeras líneas del archivo de salida, changes.csv, se ven así:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Operaciones para cargas multiparte

Operaciones para cargas multiparte

Esta sección describe cómo StorageGRID admite operaciones para cargas multiparte.

Las siguientes condiciones y notas se aplican a todas las operaciones de carga multiparte:

- No debe exceder las 1000 cargas multiparte simultáneas en un solo depósito porque los resultados de las consultas ListMultipartUploads para ese depósito podrían devolver resultados incompletos.
- StorageGRID aplica límites de tamaño de AWS para partes multiparte. Los clientes de S3 deben seguir estas pautas:
 - Cada parte de una carga multiparte debe tener entre 5 MiB (5.242.880 bytes) y 5 GiB (5.368.709.120 bytes).
 - La última parte puede ser menor a 5 MiB (5.242.880 bytes).
 - En general, los tamaños de las piezas deben ser lo más grandes posible. Por ejemplo, utilice tamaños de piezas de 5 GiB para un objeto de 100 GiB. Dado que cada parte se considera un objeto único, el uso de partes de gran tamaño reduce la sobrecarga de metadatos de StorageGRID .
 - Para objetos más pequeños que 5 GiB, considere usar una carga que no sea multiparte.
- ILM se evalúa para cada parte de un objeto multiparte a medida que se ingiere y para el objeto como un todo cuando se completa la carga multiparte, si la regla ILM usa Equilibrado o Estricto. ["opción de ingesta"](#) . Debes tener en cuenta cómo esto afecta la colocación de objetos y piezas:
 - Si ILM cambia mientras una carga multiparte de S3 está en progreso, es posible que algunas partes del objeto no cumplan con los requisitos de ILM actuales cuando se complete la carga multiparte. Cualquier pieza que no esté colocada correctamente se pone en cola para la reevaluación de ILM y se mueve a la ubicación correcta más tarde.

- Al evaluar ILM para una pieza, StorageGRID filtra el tamaño de la pieza, no el tamaño del objeto. Esto significa que partes de un objeto pueden almacenarse en ubicaciones que no cumplen los requisitos de ILM para el objeto en su totalidad. 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, cada parte de 1 GB de una carga multiparte de 10 partes se almacena en DC2 en la ingesta. Sin embargo, cuando se evalúa ILM para el objeto como un todo, todas las partes del objeto se mueven a DC1.

- Todas las operaciones de carga multiparte son compatibles con StorageGRID ["valores de consistencia"](#).
- Cuando se ingiere un objeto mediante una carga multiparte, el ["umbral de segmentación de objetos \(1 GiB\)"](#) no se aplica
- Según sea necesario, puede utilizar ["cifrado del lado del servidor"](#) con cargas multiparte. Para utilizar SSE (cifrado del lado del servidor con claves administradas por StorageGRID), incluya el `x-amz-server-side-encryption` encabezado de solicitud únicamente en la solicitud CreateMultipartUpload. Para utilizar SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente), debe especificar los mismos tres encabezados de solicitud de clave de cifrado en la solicitud CreateMultipartUpload y en cada solicitud UploadPart posterior.

Operación	Implementación
AbortarMultipartUpload	Implementado con todo el comportamiento de la API REST de Amazon S3. Sujeto a cambios sin previo aviso.
Carga completa de varias partes	Ver "Carga completa de varias partes"
Crear carga de varias partes (anteriormente llamado Iniciar carga multiparte)	Ver "Crear carga de varias partes"
Lista de cargas de varias partes	Ver "Lista de cargas de varias partes"
Lista de partes	Implementado con todo el comportamiento de la API REST de Amazon S3. Sujeto a cambios sin previo aviso.
Subir parte	Ver "Subir parte"
Subir copia parcial	Ver "Subir copia parcial"

Carga completa de varias partes

La operación CompleteMultipartUpload completa una carga multiparte de un objeto ensamblando las partes cargadas previamente.



StorageGRID admite valores no consecutivos en orden ascendente para el `partNumber` parámetro de solicitud con CompleteMultipartUpload. El parámetro puede comenzar con cualquier valor.

Resolver conflictos

Las solicitudes de clientes conflictivas, como dos clientes que escriben en la misma clave, se resuelven según el criterio del "último que gana". El momento de la evaluación de "últimas victorias" se basa en cuándo el sistema StorageGRID completa una solicitud determinada y no en cuándo los clientes S3 comienzan una operación.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

El `x-amz-storage-class` El encabezado afecta la cantidad de copias de objetos que crea StorageGRID si la regla ILM correspondiente especifica ["Opción de doble confirmación o ingesta equilibrada"](#).

- `STANDARD`

(Predeterminado) Especifica una operación de ingesta de confirmación dual cuando la regla ILM usa la opción Confirmación dual o cuando la opción Equilibrada recurre a la creación de copias provisionales.

- `REDUCED_REDUNDANCY`

Especifica una operación de ingesta de confirmación única cuando la regla ILM usa la opción de confirmación dual o cuando la opción Equilibrada recurre a la creación de copias provisionales.



Si está ingiriendo un objeto en un depósito con el bloqueo de objetos S3 habilitado, `REDUCED_REDUNDANCY` La opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, el `REDUCED_REDUNDANCY` La opción devuelve un error. StorageGRID siempre realizará una ingesta de confirmación dual para garantizar que se cumplan los requisitos de cumplimiento.



Si una carga de varias partes no se completa dentro de los 15 días, la operación se marca como inactiva y todos los datos asociados se eliminan del sistema.



El `ETag` El valor devuelto no es una suma MD5 de los datos, sino que sigue la implementación de la API de Amazon S3 de la `ETag` valor para objetos multiparte.

Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Control de versiones

Esta operación completa una carga de varias partes. Si el control de versiones está habilitado para un bucket, la versión del objeto se crea después de completar la carga de varias partes.

Si el control de versiones está habilitado para un bucket, se creará un único `versionId`. Se genera automáticamente para la versión del objeto que se está almacenando. Este `versionId` También se devuelve en la respuesta utilizando 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 el control de versiones está habilitado para un bucket, completar una carga multiparte siempre crea una nueva versión, incluso si hay cargas multiparte simultáneas completadas en la misma clave de objeto. Cuando el control de versiones no está habilitado para un bucket, es posible iniciar una carga multiparte y luego iniciar y completar primero otra carga multiparte en la misma clave de objeto. En los depósitos sin versiones, la carga multiparte que se completa en último lugar tiene prioridad.

Error de replicación, notificación o notificación de metadatos

Si el depósito donde se produce la carga multiparte está configurado para un servicio de plataforma, la carga multiparte se realiza correctamente incluso si falla la acción de replicación o notificación asociada.

Un inquilino puede activar la replicación o notificación fallida actualizando los metadatos o las etiquetas del objeto. Un inquilino puede volver a enviar los valores existentes para evitar realizar cambios no deseados.

Consulte "[Solucionar problemas de servicios de la plataforma](#)".

Crear carga de varias partes

La operación `CreateMultipartUpload` (anteriormente denominada Iniciar carga multiparte) inicia una carga multiparte para un objeto y devuelve un ID de carga.

El `x-amz-storage-class` Se admite el encabezado de solicitud. El valor presentado para `x-amz-storage-class` afecta la forma en que StorageGRID protege los datos de los objetos durante la ingesta y no la cantidad de copias persistentes del objeto que se almacenan en el sistema StorageGRID (lo cual está determinado por ILM).

Si la regla ILM que coincide con un objeto ingerido utiliza el método Estricto "[opción de ingesta](#)", el `x-amz-storage-class` El encabezado no tiene ningún efecto.

Los siguientes valores se pueden utilizar para `x-amz-storage-class`:

- **STANDARD**(Por defecto)
 - **Confirmación dual:** si la regla ILM especifica la opción de ingesta de confirmación dual, tan pronto como se ingiere un objeto, se crea una segunda copia de ese objeto y se distribuye a un nodo de almacenamiento diferente (confirmación dual). Cuando se evalúa el ILM, StorageGRID determina si estas copias provisionales iniciales satisfacen las instrucciones de ubicación de la regla. De lo contrario, es posible que sea necesario realizar nuevas copias de objetos en ubicaciones diferentes y eliminar las copias provisionales iniciales.
 - **Equilibrado:** si la regla ILM especifica la opción Equilibrado y StorageGRID no puede realizar inmediatamente todas las copias especificadas en la regla, StorageGRID realiza dos copias provisionales en diferentes nodos de almacenamiento.

Si StorageGRID puede crear inmediatamente todas las copias de objetos especificadas en la regla ILM (ubicación sincrónica), `x-amz-storage-class` El encabezado no tiene ningún efecto.

- `REDUCED_REDUNDANCY`

- **Confirmación dual:** si la regla ILM especifica la opción de confirmación dual, StorageGRID crea una única copia provisional a medida que se ingiere el objeto (confirmación única).
- **Equilibrado:** si la regla ILM especifica la opción Equilibrado, StorageGRID realiza una única copia provisional solo si el sistema no puede realizar inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar la colocación sincrónica, este encabezado no tiene ningún efecto. El `REDUCED_REDUNDANCY` Esta opción se utiliza mejor cuando la regla ILM que coincide con el objeto crea una única copia replicada. En este caso se utiliza `REDUCED_REDUNDANCY` Elimina la creación y eliminación innecesarias de una copia de objeto adicional para cada operación de ingesta.

Usando el `REDUCED_REDUNDANCY` Esta opción no se recomienda en otras circunstancias.

`REDUCED_REDUNDANCY` aumenta el riesgo de pérdida de datos de objetos durante la ingesta. Por ejemplo, podría perder datos si la copia única se almacena inicialmente en un nodo de almacenamiento que falla antes de que pueda ocurrir la evaluación de ILM.



Tener solo una copia replicada por un período de tiempo determinado pone los datos en riesgo de pérdida permanente. Si solo existe una copia replicada de un objeto, ese objeto se pierde si un nodo de almacenamiento falla o tiene un error significativo. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como actualizaciones.

Especificando `REDUCED_REDUNDANCY` Sólo afecta la cantidad de copias que se crean cuando se ingiere un objeto por primera vez. No afecta la cantidad de copias del objeto que se realizan cuando las políticas ILM activas evalúan el objeto y no hace que los datos se almacenen en niveles inferiores de redundancia en el sistema StorageGRID .



Si está ingiriendo un objeto en un depósito con el bloqueo de objetos S3 habilitado, `REDUCED_REDUNDANCY` La opción se ignora. Si está ingiriendo un objeto en un depósito compatible heredado, el `REDUCED_REDUNDANCY` La opción devuelve un error. StorageGRID siempre realizará una ingesta de confirmación dual para garantizar que se cumplan los requisitos de cumplimiento.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `Content-Type`
- `x-amz-checksum-algorithm`

Actualmente, solo el valor `SHA256` para `x-amz-checksum-algorithm` es compatible.

- `x-amz-meta-`, seguido de un par nombre-valor que contiene metadatos definidos por el usuario

Al especificar el par nombre-valor para los metadatos definidos por el usuario, utilice este formato general:

```
x-amz-meta-_name_: `value`
```

Si desea utilizar la opción **Hora de creación definida por el usuario** como Hora de referencia para una regla ILM, debe utilizar `creation-time` como el nombre de los metadatos que registran cuándo se creó el objeto. Por ejemplo:

```
x-amz-meta-creation-time: 1443399726
```

El valor de `creation-time` se evalúa en segundos desde el 1 de enero de 1970.



Añadiendo `creation-time` ya que no se permiten metadatos definidos por el usuario si está agregando un objeto a un depósito que tiene habilitado el Cumplimiento heredado. 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, se utilizan las configuraciones de retención predeterminadas del depósito para calcular la fecha de retención de la versión del objeto.

["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#)

- Encabezados de solicitud SSE:

- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-algorithm`

[Encabezados de solicitud para el cifrado del lado del servidor](#)



Para obtener información sobre cómo StorageGRID maneja los caracteres UTF-8, consulte ["PonerObjeto"](#).

Encabezados de solicitud para el cifrado del lado del servidor

Puede utilizar los siguientes encabezados de solicitud para cifrar un objeto multiparte con cifrado del lado del servidor. Las opciones SSE y SSE-C son mutuamente excluyentes.

- **SSE:** utilice el siguiente encabezado en la solicitud `CreateMultipartUpload` si desea cifrar el objeto con una clave única administrada por StorageGRID. No especifique este encabezado en ninguna de las solicitudes `UploadPart`.
 - `x-amz-server-side-encryption`
- **SSE-C:** utilice estos tres encabezados en la solicitud `CreateMultipartUpload` (y en cada solicitud `UploadPart` posterior) si desea cifrar el objeto con una clave única que usted proporcione y administre.
 - `x-amz-server-side-encryption-customer-algorithm`: Especifique `AES256`.
 - `x-amz-server-side-encryption-customer-key`: Especifique su clave de cifrado para el nuevo objeto.

- `x-amz-server-side-encryption-customer-key-MD5`:Especifique el resumen MD5 de la clave de cifrado del nuevo objeto.



Las claves de cifrado que 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 los objetos, revise las consideraciones para ["utilizando cifrado del lado del servidor"](#).

Encabezados de solicitud no admitidos

El siguiente encabezado de solicitud no es compatible:

- `x-amz-website-redirect-location`

El `x-amz-website-redirect-location` el encabezado regresa `XNotImplemented`.

Control de versiones

La carga multiparte consta de operaciones separadas para iniciar la carga, enumerar las cargas, cargar partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación `CompleteMultipartUpload`.

Lista de cargas de varias partes

La operación `ListMultipartUploads` enumera las cargas multiparte en curso para un depósito.

Se admiten los siguientes parámetros de solicitud:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Control de versiones

La carga multiparte consta de operaciones separadas para iniciar la carga, enumerar las cargas, cargar partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación `CompleteMultipartUpload`.

Subir parte

La operación `UploadPart` carga una parte en una carga multiparte para un objeto.

Encabezados de solicitud admitidos

Se admiten los siguientes encabezados de solicitud:

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

Encabezados de solicitud para el cifrado del lado del servidor

Si especificó el cifrado SSE-C para la solicitud `CreateMultipartUpload`, también debe incluir los siguientes encabezados de solicitud en cada solicitud `UploadPart`:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar `AES256`.
- `x-amz-server-side-encryption-customer-key`: Especifique la misma clave de cifrado que proporcionó en la solicitud `CreateMultipartUpload`.
- `x-amz-server-side-encryption-customer-key-MD5`: Especifique el mismo resumen MD5 que proporcionó en la solicitud `CreateMultipartUpload`.



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 los objetos, revise las consideraciones en ["Utilice cifrado del lado del servidor"](#).

Si especificó una suma de comprobación SHA-256 durante la solicitud `CreateMultipartUpload`, también debe incluir el siguiente encabezado de solicitud en cada solicitud `UploadPart`:

- `x-amz-checksum-sha256`: Especifique la suma de comprobación SHA-256 para esta parte.

Encabezados de solicitud no admitidos

Los siguientes encabezados de solicitud no son compatibles:

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Control de versiones

La carga multiparte consta de operaciones separadas para iniciar la carga, enumerar las cargas, cargar partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación `CompleteMultipartUpload`.

Subir copia parcial

La operación `UploadPartCopy` carga una parte de un objeto copiando datos de un objeto existente como fuente de datos.

La operación `UploadPartCopy` se implementa con todo el comportamiento de la API REST de Amazon S3. Sujeto a cambios sin previo aviso.

Esta solicitud lee y escribe los datos del objeto especificados en `x-amz-copy-source-range` dentro del 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`

Encabezados de solicitud para el cifrado del lado del servidor

Si especificó el cifrado SSE-C para la solicitud `CreateMultipartUpload`, también debe incluir los siguientes encabezados de solicitud en cada solicitud `UploadPartCopy`:

- `x-amz-server-side-encryption-customer-algorithm`: Especificar AES256 .
- `x-amz-server-side-encryption-customer-key`:Especifique la misma clave de cifrado que proporcionó en la solicitud `CreateMultipartUpload`.
- `x-amz-server-side-encryption-customer-key-MD5`:Especifique el mismo resumen MD5 que proporcionó en la solicitud `CreateMultipartUpload`.

Si el objeto de origen está cifrado mediante una clave proporcionada por el cliente (SSE-C), debe incluir los siguientes tres encabezados en la solicitud `UploadPartCopy`, para que el objeto pueda descifrarse y luego copiarse:

- `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 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 los objetos, revise las consideraciones en "[Utilice cifrado del lado del servidor](#)".

Control de versiones

La carga multiparte consta de operaciones separadas para iniciar la carga, enumerar las cargas, cargar partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si corresponde) cuando se realiza la operación `CompleteMultipartUpload`.

Respuestas de error

El sistema StorageGRID admite todas las respuestas de error de API REST S3 estándar que corresponden. Además, la implementación de StorageGRID agrega varias respuestas personalizadas.

Códigos de error de la API de S3 compatibles

Nombre	Estado HTTP
Acceso denegado	403 Prohibido
Mal resumen	400 Solicitud incorrecta
El cubo ya existe	409 Conflict
Cubo no vacío	409 Conflict
Cuerpo incompleto	400 Solicitud incorrecta
Error interno	500 Error interno del servidor
ID de clave de acceso no válido	403 Prohibido
Argumento inválido	400 Solicitud incorrecta
Nombre de cubo inválido	400 Solicitud incorrecta
Estado del cubo no válido	409 Conflict
Resumen inválido	400 Solicitud incorrecta
Error de algoritmo de cifrado no válido	400 Solicitud incorrecta
Parte inválida	400 Solicitud incorrecta
Orden de pieza no válida	400 Solicitud incorrecta
Rango inválido	416 Rango solicitado no satisfacible
Solicitud inválida	400 Solicitud incorrecta
Clase de almacenamiento no válida	400 Solicitud incorrecta
Etiqueta inválida	400 Solicitud incorrecta
URI no válido	400 Solicitud incorrecta
Clave demasiado larga	400 Solicitud incorrecta
XML malformado	400 Solicitud incorrecta

Nombre	Estado HTTP
Metadatos demasiado grandes	400 Solicitud incorrecta
Método no permitido	Método 405 no permitido
Longitud de contenido faltante	411 Longitud requerida
Error de cuerpo de solicitud faltante	400 Solicitud incorrecta
Encabezado de seguridad faltante	400 Solicitud incorrecta
NoSuchBucket	404 No encontrado
NoSuchKey	404 No encontrado
NoSuchUpload	404 No encontrado
No implementado	501 No implementado
Política de no usar este cubo	404 No encontrado
Error de configuración de bloqueo de objeto no encontrado	404 No encontrado
Precondición fallida	412 Precondición fallida
RequestTimeTooSkewed	403 Prohibido
Servicio No Disponible	503 Servicio no disponible
La firma no coincide	403 Prohibido
Demasiados cubos	400 Solicitud incorrecta
La clave de usuario debe especificarse	400 Solicitud incorrecta

Códigos de error personalizados de StorageGRID

Nombre	Descripción	Estado HTTP
Ciclo de vida de XBucket no permitido	La configuración del ciclo de vida del bucket no está permitida en un bucket compatible heredado	400 Solicitud incorrecta

Nombre	Descripción	Estado HTTP
Excepción de análisis de política de XBucket	No se pudo analizar el JSON de la política de depósito recibida.	400 Solicitud incorrecta
Conflicto de cumplimiento X	Operación denegada debido a configuraciones de cumplimiento heredadas.	403 Prohibido
XComplianceReducedRedundancyForbidden	No se permite redundancia reducida en el bucket compatible heredado	400 Solicitud incorrecta
Longitud máxima de la política de cubos X excedida	Su póliza excede la longitud máxima permitida de la póliza.	400 Solicitud incorrecta
XMissingInternalRequestHeader	Falta un encabezado de una solicitud interna.	400 Solicitud incorrecta
Cumplimiento de XNoSuchBucket	El depósito especificado no tiene habilitada la conformidad heredada.	404 No encontrado
XNo acceptable	La solicitud contiene uno o más encabezados de aceptación que no se pudieron satisfacer.	406 No acceptable
XNotImplemented	La solicitud que proporcionó implica una funcionalidad que no está implementada.	501 No implementado

Operaciones personalizadas de StorageGRID

Operaciones personalizadas de StorageGRID

El sistema StorageGRID admite operaciones personalizadas que se agregan a la API REST de S3.

La siguiente tabla enumera las operaciones personalizadas compatibles con StorageGRID.

Operación	Descripción
"Obtener consistencia del bucket"	Devuelve la consistencia que se aplica a un depósito en particular.
"Consistencia del depósito PUT"	Establece la consistencia aplicada a un depósito en particular.
"GET Hora del último acceso al bucket"	Devuelve si las actualizaciones del último tiempo de acceso están habilitadas o deshabilitadas para un depósito en particular.
"Hora del último acceso al depósito PUT"	Le permite habilitar o deshabilitar las actualizaciones del último tiempo de acceso para un depósito en particular.

Operación	Descripción
"Configuración de notificación de metadatos del depósito DELETE"	Elimina el XML de configuración de notificación de metadatos asociado con un depósito en particular.
"Configuración de notificación de metadatos del depósito GET"	Devuelve el XML de configuración de notificación de metadatos asociado con un depósito en particular.
"Configuración de notificación de metadatos del depósito PUT"	Configura el servicio de notificación de metadatos para un bucket.
"Uso de almacenamiento GET"	Le indica la cantidad total de almacenamiento en uso por una cuenta y para cada depósito asociado con la cuenta.
"Obsoleto: CreateBucket con configuración de cumplimiento"	Obsoleto y no compatible: ya no es posible crear nuevos depósitos con Cumplimiento habilitado.
"Obsoleto: cumplimiento del contenedor GET"	Obsoleto pero compatible: devuelve las configuraciones de cumplimiento actualmente vigentes para un bucket compatible heredado existente.
"Obsoleto: Cumplimiento del contenedor PUT"	Obsoleto pero compatible: le permite modificar la configuración de cumplimiento para un depósito compatible heredado existente.

Obtener consistencia del bucket

La solicitud de consistencia de depósito GET le permite determinar la consistencia que se aplica a un depósito en particular.

La consistencia predeterminada está configurada para garantizar la lectura después de la escritura para los objetos recién creados.

Debe tener el permiso `s3:GetBucketConsistency` o ser la cuenta `root` para completar esta operación.

Ejemplo de solicitud

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Respuesta

En el XML de respuesta, `<Consistency>` devolverá uno de los siguientes valores:

Consistencia	Descripción
todo	Todos los nodos reciben los datos inmediatamente o la solicitud fallará.
fuerte-global	Garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios.
sitio fuerte	Garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes dentro de un sitio.
lectura después de nueva escritura	(Predeterminado) Proporciona consistencia de lectura después de escritura para objetos nuevos y consistencia eventual para actualizaciones de objetos. Ofrece alta disponibilidad y garantías de protección de datos. Recomendado para la mayoría de los casos.
disponible	Proporciona consistencia eventual tanto para objetos nuevos como para actualizaciones de objetos. Para los depósitos S3, úselo solo cuando sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD o GET en claves que no existen). No compatible con depósitos S3 FabricPool .

Ejemplo de respuesta

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Información relacionada

["Valores de consistencia"](#)

Consistencia del depósito PUT

La solicitud de consistencia de PUT Bucket le permite especificar la consistencia que se aplicará a las operaciones realizadas en un bucket.

La consistencia predeterminada está configurada para garantizar la lectura después de la escritura para los objetos recién creados.

Antes de empezar

Debe tener el permiso `s3:PutBucketConsistency` o ser la cuenta `root` para completar esta operación.

Pedido

El `x-ntap-sg-consistency` El parámetro debe contener uno de los siguientes valores:

Consistencia	Descripción
todo	Todos los nodos reciben los datos inmediatamente o la solicitud fallará.
fuerte-global	Garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes en todos los sitios.
sitio fuerte	Garantiza la consistencia de lectura tras escritura para todas las solicitudes de clientes dentro de un sitio.
lectura después de nueva escritura	(Predeterminado) Proporciona consistencia de lectura después de escritura para objetos nuevos y consistencia eventual para actualizaciones de objetos. Ofrece alta disponibilidad y garantías de protección de datos. Recomendado para la mayoría de los casos.
disponible	Proporciona consistencia eventual tanto para objetos nuevos como para actualizaciones de objetos. Para los depósitos S3, úselo solo cuando sea necesario (por ejemplo, para un depósito que contiene valores de registro que rara vez se leen, o para operaciones HEAD o GET en claves que no existen). No compatible con depósitos S3 FabricPool .

Nota: En general, debe utilizar la consistencia "Lectura después de nueva 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 la consistencia para cada solicitud de API. Establezca la consistencia a nivel de depósito sólo como último recurso.

Ejemplo de solicitud

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Información relacionada

["Valores de consistencia"](#)

GET Hora del último acceso al bucket

La solicitud de hora de último acceso al bucket GET le permite determinar si las actualizaciones de hora de último acceso están habilitadas o deshabilitadas para buckets individuales.

Debe tener el permiso `s3:GetBucketLastAccessTime` o ser `root` de la cuenta para completar esta operación.

Ejemplo de solicitud

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Ejemplo de respuesta

Este ejemplo muestra que las actualizaciones del último tiempo de acceso están habilitadas para el depósito.

```
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>
```

Hora del último acceso al depósito PUT

La solicitud de hora de último acceso al depósito PUT le permite habilitar o deshabilitar actualizaciones de hora de último acceso para depósitos individuales. Deshabilitar las actualizaciones del último tiempo de acceso mejora el rendimiento y es la configuración predeterminada para todos los depósitos creados con la versión 10.3.0 o posterior.

Debe tener el permiso `s3:PutBucketLastAccessTime` para un bucket, o ser root de la cuenta, para completar esta operación.



A partir de la versión 10.3 de StorageGRID, las actualizaciones de la hora del último acceso están deshabilitadas de manera predeterminada para todos los depósitos nuevos. Si tiene depósitos que se crearon utilizando una versión anterior de StorageGRID y desea que coincidan con el nuevo comportamiento predeterminado, debe deshabilitar explícitamente las actualizaciones de la última hora de acceso para cada uno de esos depósitos anteriores. Puede habilitar o deshabilitar las actualizaciones de la última hora de acceso mediante la solicitud de última hora de acceso del depósito PUT o desde la página de detalles de un depósito en el Administrador de inquilinos. Ver ["Habilitar o deshabilitar las actualizaciones de la última hora de acceso"](#).

Si las actualizaciones del último tiempo de acceso están deshabilitadas para un depósito, se aplica el siguiente comportamiento a las operaciones en el depósito:

- Las solicitudes `GetObject`, `GetObjectAcl`, `GetObjectTagging` y `HeadObject` no actualizan la hora del último acceso. El objeto no se agrega a las colas para la evaluación de la gestión del ciclo de vida de la

información (ILM).

- Las solicitudes CopyObject y PutObjectTagging que actualizan solo los metadatos también actualizan la hora del último acceso. El objeto se agrega a las colas para la evaluación de ILM.
- Si las actualizaciones de la hora del último acceso están deshabilitadas para el depósito de origen, las solicitudes CopyObject no actualizan la hora del último acceso para el depósito de origen. El objeto que se copió no se agrega a las colas para la evaluación de ILM para el depósito de origen. Sin embargo, para el destino, las solicitudes CopyObject siempre actualizan la hora del último acceso. La copia del objeto se agrega a las colas para la evaluación de ILM.
- CompleteMultipartUpload solicita actualizar la hora del último acceso. El objeto completado se agrega a las colas para la evaluación de ILM.

Solicitar ejemplos

Este ejemplo habilita el último tiempo de acceso para un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Este ejemplo deshabilita el tiempo del último acceso para un depósito.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Configuración de notificación de metadatos del depósito DELETE

La solicitud de configuración de notificación de metadatos de depósito DELETE le permite deshabilitar el servicio de integración de búsqueda para depósitos individuales eliminando el XML de configuración.

Debe tener el permiso s3:DeleteBucketMetadataNotification para un bucket, o ser raíz de la cuenta, para completar esta operación.

Ejemplo de solicitud

Este ejemplo muestra cómo deshabilitar el servicio de integración de búsqueda para un depósito.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Configuración de notificación de metadatos del depósito GET

La solicitud de configuración de notificación de metadatos de bucket GET le permite recuperar el XML de configuración utilizado para configurar la integración de búsqueda para buckets individuales.

Debe tener el permiso `s3:GetBucketMetadataNotification` o ser la cuenta `root` para completar esta operación.

Ejemplo de solicitud

Esta solicitud recupera la configuración de notificación de metadatos para el depósito denominado `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Respuesta

El cuerpo de la respuesta incluye la configuración de notificación de metadatos para el depósito. La configuración de notificación de metadatos le permite determinar cómo se configura el depósito para la integración de búsqueda. Es decir, permite determinar qué objetos están indexados y a qué puntos finales se envían sus metadatos de 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 más reglas. Cada regla especifica los objetos a los que se aplica y el destino donde StorageGRID debe enviar los metadatos de los objetos. Los destinos deben especificarse utilizando el URN de un punto final de StorageGRID.

Nombre	Descripción	Requerido
Configuración de notificación de metadatos	Etiqueta contenedora para reglas utilizadas para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o más elementos de regla.	Sí
Regla	Etiqueta contenedora para una regla que identifica los objetos cuyos metadatos deben agregarse a un índice específico. Se rechazan las reglas con prefijos superpuestos. Incluido en el elemento MetadataNotificationConfiguration.	Sí
IDENTIFICACIÓN	Identificador único de la regla. Incluido en el elemento Regla.	No
Estado	El estado puede ser 'Habilitado' o 'Deshabilitado'. No se realiza ninguna acción para las reglas que están deshabilitadas. 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 que coincida con 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	Requerido
Urna	URN del destino donde se envían los metadatos del objeto. Debe ser la URN de un punto final de StorageGRID con las siguientes propiedades: • <code>`es`</code> Debe ser el tercer elemento. • La URN debe terminar con el índice y tipo donde se almacenan los metadatos, en el formato <code>domain-name/myindex/mytype</code>. Los puntos finales se configuran mediante el Administrador de inquilinos o la API de administración de inquilinos. Toman la siguiente forma: • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> El punto final debe configurarse antes de enviar el XML de configuración; de lo contrario, la configuración fallará con un error 404. La urna está incluida en el elemento Destino.	Sí

Ejemplo de respuesta

El XML incluido entre el

`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` Las etiquetas muestran cómo se configura la integración con un punto final de integración de búsqueda para el depósito. En este ejemplo, los metadatos del objeto se envían a un índice de Elasticsearch llamado `current` y tipo nombrado `2017` que está alojado 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

["Utilice una cuenta de inquilino"](#)

Configuración de notificación de metadatos del depósito PUT

La solicitud de configuración de notificación de metadatos de PUT Bucket le permite habilitar el servicio de integración de búsqueda para buckets individuales. El XML de configuración de notificación de metadatos que proporciona en el cuerpo de la solicitud especifica los objetos cuyos metadatos se envían al índice de búsqueda de destino.

Debe tener el permiso `s3:PutBucketMetadataNotification` para un bucket, o ser raíz de la cuenta, para completar esta operación.

Pedido

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 más reglas. Cada regla especifica los objetos a los que se aplica y el destino donde StorageGRID debe enviar los metadatos de los objetos.

Los objetos se pueden filtrar según el prefijo del nombre del objeto. Por ejemplo, podría enviar metadatos para objetos con el prefijo `/images` a 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 los objetos con el prefijo `test` y una segunda regla para los objetos con el prefijo `test2` No se permitiría.

Los destinos deben especificarse utilizando el URN de un punto final de StorageGRID . El punto final debe existir cuando se envía la configuración de notificación de metadatos, o la solicitud falla como resultado. 400

Bad Request El mensaje de error dice: 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>
```

La tabla describe los elementos del XML de configuración de notificación de metadatos.

Nombre	Descripción	Requerido
Configuración de notificación de metadatos	Etiqueta contenedora para reglas utilizadas para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o más elementos de regla.	Sí
Regla	Etiqueta contenedora para una regla que identifica los objetos cuyos metadatos deben agregarse a un índice específico. Se rechazan las reglas con prefijos superpuestos. Incluido en el elemento MetadataNotificationConfiguration.	Sí
IDENTIFICACIÓN	Identificador único de la regla. Incluido en el elemento Regla.	No
Estado	El estado puede ser 'Habilitado' o 'Deshabilitado'. No se realiza ninguna acción para las reglas que están deshabilitadas. Incluido en el elemento Regla.	Sí

Nombre	Descripción	Requerido
Prefijo	Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado. Para que coincida con 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
Urna	URN del destino donde se envían los metadatos del objeto. Debe ser la URN de un punto final de StorageGRID con las siguientes propiedades: • `es` Debe ser el tercer elemento. • La URN debe terminar con el índice y tipo donde se almacenan los metadatos, en el formato <code>domain-name/myindex/mytype</code>. Los puntos finales se configuran mediante el Administrador de inquilinos o la API de administración de inquilinos. Toman la siguiente forma: • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> El punto final debe configurarse antes de enviar el XML de configuración; de lo contrario, la configuración fallará con un error 404. La urna está incluida en el elemento Destino.	Sí

Solicitar ejemplos

Este ejemplo muestra cómo habilitar la integración de búsqueda para un depósito. En este ejemplo, los metadatos de todos los objetos se envían al mismo destino.


```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

En este ejemplo, metadatos de objeto para objetos que coinciden con el prefijo `/images` se envía a un destino, mientras que los metadatos del objeto para los objetos que coinciden con el prefijo `/videos` se envía a un segundo destino.

```

PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333: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

Cuando habilita el servicio de integración de búsqueda para un depósito, se genera un documento JSON y se envía al punto final de destino cada vez que se agregan, actualizan o eliminan metadatos o etiquetas de objeto.

Este ejemplo muestra un ejemplo del JSON que podría generarse cuando un objeto con la clave SGWS/Tagging.txt se crea en un depósito llamado test . El test El bucket no tiene versión, por lo que 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

La tabla enumera todos los campos que se incluyen en el documento JSON que se envía al punto final de destino cuando se habilita la integración de búsqueda.

El nombre del documento incluye el nombre del depósito, el nombre del objeto y el ID de la versión, si está presente.

Tipo	Nombre del artículo	Descripción
Información de depósito y objeto	balde	Nombre del bucket
Información de depósito y objeto	llave	Nombre de la clave del objeto
Información de depósito y objeto	ID de versión	Versión del objeto, para objetos en depósitos versionados
Información de depósito y objeto	región	Región del cubo, por ejemplo <code>us-east-1</code>
Metadatos del sistema	tamaño	Tamaño del objeto (en bytes) tal como lo ve un cliente HTTP
Metadatos del sistema	md5	Hash de objeto
Metadatos del usuario	metadatos <i>key:value</i>	Todos los metadatos de usuario para el objeto, como pares clave-valor

Tipo	Nombre del artículo	Descripción
Etiquetas	etiquetas <i>key:value</i>	Todas las etiquetas de objeto definidas para el objeto, como pares clave-valor



Para las etiquetas y los metadatos del usuario, StorageGRID pasa fechas y números a Elasticsearch como cadenas o como notificaciones de eventos S3. Para configurar Elasticsearch para que interprete estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para el mapeo de campos dinámicos y para el mapeo de formatos de fecha. Debe habilitar las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Una vez indexado un documento, no es posible editar los tipos de campos del documento en el índice.

Información relacionada

["Utilice una cuenta de inquilino"](#)

Solicitud de uso de almacenamiento GET

La solicitud de uso de almacenamiento GET le indica la cantidad total de almacenamiento en uso por una cuenta y para cada depósito asociado con la cuenta.

La cantidad de almacenamiento utilizada por una cuenta y sus depósitos se puede obtener mediante una solicitud ListBuckets modificada con el `x-ntap-sg-usage` parámetro de consulta. El uso del almacenamiento del bucket se rastrea por separado de las solicitudes PUT y DELETE procesadas por el sistema. Puede haber algún retraso antes de que los valores de uso coincidan con los valores esperados en función del procesamiento de las solicitudes, en particular si el sistema está bajo una carga pesada.

De forma predeterminada, StorageGRID intenta recuperar información de uso utilizando una consistencia global fuerte. Si no se puede lograr una consistencia global fuerte, StorageGRID intenta recuperar la información de uso con una consistencia de sitio fuerte.

Debe tener el permiso `s3:ListAllMyBuckets` o ser la cuenta `root` para completar esta operación.

Ejemplo de solicitud

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Ejemplo de respuesta

Este ejemplo muestra una cuenta que tiene cuatro objetos y 12 bytes de datos en dos grupos. Cada contenedor 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>
```

Control de versiones

Cada versión de objeto almacenada contribuirá a la `ObjectCount` y `DataBytes` valores en la respuesta. Los marcadores de eliminación no se agregan a la `ObjectCount` total.

Información relacionada

["Valores de consistencia"](#)

Solicitudes de depósito obsoletas para cumplimiento heredado

Solicitudes de depósito obsoletas para cumplimiento heredado

Es posible que necesite usar la API REST S3 de StorageGRID para administrar los depósitos que se crearon mediante la función de cumplimiento heredada.

Función de cumplimiento obsoleta

La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID está obsoleta y ha sido reemplazada por S3 Object Lock.

Si anteriormente habilitó la configuración de Cumplimiento global, la configuración de Bloqueo de objetos S3 global está habilitada en StorageGRID 11.6. Ya no es posible crear nuevos buckets con Cumplimiento habilitado; sin embargo, según sea necesario, puede usar la API REST de StorageGRID S3 para administrar cualquier bucket Cumplimiento heredado existente.

- ["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#)
- ["Administrar objetos con ILM"](#)
- ["Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5"](#)

Solicitudes de cumplimiento obsoletas:

- ["Obsoleto: modificaciones de la solicitud PUT Bucket para cumplimiento"](#)

El elemento XML SGCompliance está obsoleto. Anteriormente, podía incluir este elemento personalizado StorageGRID en el cuerpo de la solicitud XML opcional de las solicitudes PUT Bucket para crear un bucket compatible.

- ["Obsoleto: cumplimiento del contenedor GET"](#)

La solicitud de cumplimiento de GET Bucket está obsoleta. Sin embargo, puede seguir usando esta solicitud para determinar las configuraciones de cumplimiento actualmente vigentes para un bucket compatible heredado existente.

- ["Obsoleto: cumplimiento del contenedor PUT"](#)

La solicitud de cumplimiento de PUT Bucket está obsoleta. Sin embargo, puede seguir usando esta solicitud para modificar la configuración de cumplimiento de un depósito compatible heredado existente. Por ejemplo, puede colocar un depósito existente en retención legal o aumentar su período de retención.

Obsoleto: Modificaciones de la solicitud CreateBucket para cumplimiento

El elemento XML SGCompliance está obsoleto. Anteriormente, podía incluir este elemento personalizado StorageGRID en el cuerpo de la solicitud XML opcional de las solicitudes CreateBucket para crear un depósito compatible.



La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID está obsoleta y ha sido reemplazada por S3 Object Lock. Para más detalles, véase lo siguiente:

- ["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#)
- ["Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5"](#)

Ya no es posible crear nuevos depósitos con la opción Cumplimiento habilitada. Se devuelve el siguiente mensaje de error si intenta utilizar las modificaciones de la solicitud CreateBucket para cumplimiento para crear un nuevo depósito compatible:

The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant buckets.

Obsoleto: solicitud de cumplimiento de GET Bucket

La solicitud de cumplimiento de GET Bucket está obsoleta. Sin embargo, puede seguir usando esta solicitud para determinar las configuraciones de cumplimiento actualmente vigentes para un bucket compatible heredado existente.



La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID está obsoleta y ha sido reemplazada por S3 Object Lock. Para más detalles, véase lo siguiente:

- ["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#)
- ["Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5"](#)

Debe tener el permiso `s3:GetBucketCompliance` o ser la cuenta `root` para completar esta operación.

Ejemplo de solicitud

Esta solicitud de ejemplo le permite determinar la configuración de cumplimiento para el depósito denominado `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Ejemplo de respuesta

En el XML de respuesta, `<SGCompliance>` enumera las configuraciones de cumplimiento vigentes para el depósito. Esta respuesta de ejemplo muestra las configuraciones de cumplimiento para un depósito en el que cada objeto se conservará durante un año (525 600 minutos), a partir del momento en que el objeto se ingiere en la red. Actualmente no existe ninguna retención legal sobre este depósito. Cada objeto se eliminará automáticamente después de un año.

```

HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>

```

Nombre	Descripción
Minutos del período de retención	La duración del período de retención de los objetos agregados a este depósito, en minutos. El período de retención comienza cuando el objeto se incorpora a la red.
Retención legal	• Verdadero: Este depósito se encuentra actualmente bajo retención legal. Los objetos de este depósito no se pueden eliminar hasta que se levante la retención legal, incluso si su período de retención ha expirado. • Falso: este depósito no se encuentra actualmente bajo retención legal. Los objetos de este depósito se pueden eliminar cuando expire su período de retención.
Eliminación automática	• Verdadero: Los objetos de este depósito se eliminarán automáticamente cuando expire su período de retención, a menos que el depósito esté bajo una retención legal. • Falso: Los objetos de este depósito no se eliminarán automáticamente cuando expire el período de retención. Debes eliminar estos objetos manualmente si necesitas eliminarlos.

Respuestas de error

Si el depósito no se creó para ser compatible, el código de estado HTTP para la respuesta es 404 Not Found , con un código de error S3 de XNoSuchBucketCompliance .

Obsoleto: Solicitud de cumplimiento de PUT Bucket

La solicitud de cumplimiento de PUT Bucket está obsoleta. Sin embargo, puede seguir usando esta solicitud para modificar la configuración de cumplimiento de un depósito compatible heredado existente. Por ejemplo, puede colocar un depósito existente en retención legal o aumentar su período de retención.



La función de cumplimiento de StorageGRID que estaba disponible en versiones anteriores de StorageGRID está obsoleta y ha sido reemplazada por S3 Object Lock. Para más detalles, véase lo siguiente:

- ["Utilice la API REST de S3 para configurar el bloqueo de objetos de S3"](#)
- ["Base de conocimientos de NetApp : Cómo administrar los buckets compatibles heredados en StorageGRID 11.5"](#)

Debe tener el permiso `s3:PutBucketCompliance` o ser la cuenta `root` para completar esta operación.

Debe especificar un valor para cada campo de la configuración de cumplimiento al emitir una solicitud de cumplimiento de PUT Bucket.

Ejemplo de solicitud

Esta solicitud de ejemplo modifica la configuración de cumplimiento para el depósito denominado `mybucket`. En este ejemplo, los objetos en `mybucket` ahora se conservarán durante dos años (1.051.200 minutos) en lugar de un año, a partir del momento en que el objeto se incorpora a la red. No existe ninguna retención legal sobre este cubo. Cada objeto se eliminará automáticamente después de dos años.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nombre	Descripción
Minutos del período de retención	La duración del período de retención de los objetos agregados a este depósito, en minutos. El período de retención comienza cuando el objeto se incorpora a la red. Importante Al especificar un nuevo valor para <code>RetentionPeriodMinutes</code>, debe especificar un valor que sea igual o mayor que el período de retención actual del depósito. Una vez establecido el período de retención del depósito, no puedes disminuir ese valor; solo puedes aumentarlo.

Nombre	Descripción
Retención legal	• Verdadero: Este depósito se encuentra actualmente bajo retención legal. Los objetos de este depósito no se pueden eliminar hasta que se levante la retención legal, incluso si su período de retención ha expirado. • Falso: este depósito no se encuentra actualmente bajo retención legal. Los objetos de este depósito se pueden eliminar cuando expire su período de retención.
Eliminación automática	• Verdadero: Los objetos de este depósito se eliminarán automáticamente cuando expire su período de retención, a menos que el depósito esté bajo una retención legal. • Falso: Los objetos de este depósito no se eliminarán automáticamente cuando expire el período de retención. Debes eliminar estos objetos manualmente si necesitas eliminarlos.

Coherencia para la configuración de cumplimiento

Cuando actualiza la configuración de cumplimiento de un bucket S3 con una solicitud de cumplimiento de bucket PUT, StorageGRID intenta actualizar los metadatos del bucket en toda la red. De manera predeterminada, StorageGRID utiliza la consistencia **Strong-global** para garantizar que todos los sitios del centro de datos y todos los nodos de almacenamiento que contienen metadatos de bucket tengan consistencia de lectura después de escritura para las configuraciones de cumplimiento modificadas.

Si StorageGRID no puede lograr la consistencia **fuerte-global** porque un sitio de centro de datos o varios nodos de almacenamiento en un sitio no están disponibles, el código de estado HTTP para la respuesta es 503 Service Unavailable.

Si recibe esta respuesta, debe comunicarse con el administrador de la red para asegurarse de que los servicios de almacenamiento necesarios estén disponibles lo antes posible. Si el administrador de la red no puede poner a disposición suficientes nodos de almacenamiento en cada sitio, el soporte técnico puede indicarle que vuelva a intentar la solicitud fallida forzando la consistencia **Strong-site**.



Nunca fuerce la consistencia **Strong-site** para el cumplimiento del bucket PUT a menos que el soporte técnico se lo haya indicado y a menos que comprenda las posibles consecuencias de usar este nivel.

Cuando la consistencia se reduce a **Sitio fuerte**, StorageGRID garantiza que las configuraciones de cumplimiento actualizadas tendrán consistencia de lectura después de escritura solo para las solicitudes de clientes dentro de un sitio. Esto significa que el sistema StorageGRID podría tener temporalmente múltiples configuraciones inconsistentes para este depósito hasta que todos los sitios y nodos de almacenamiento estén disponibles. Las configuraciones inconsistentes pueden generar un comportamiento inesperado y no deseado. Por ejemplo, si coloca un depósito bajo una retención legal y fuerza una consistencia menor, las configuraciones de cumplimiento anteriores del depósito (es decir, retención legal) podrían seguir vigentes en algunos sitios de centros de datos. Como resultado, los objetos que usted considera que están en retención legal podrían eliminarse cuando expire su período de retención, ya sea por el usuario o por AutoDelete, si está habilitado.

Para forzar el uso de la consistencia **Strong-site**, vuelva a emitir la solicitud de cumplimiento de PUT Bucket e incluya la `Consistency-Control` Encabezado de solicitud HTTP, como sigue:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Respuestas de error

- Si el depósito no se creó para ser compatible, el código de estado HTTP para la respuesta es 404 Not Found.
- Si `RetentionPeriodMinutes` En la solicitud es menor que el período de retención actual del depósito, el código de estado HTTP es 400 Bad Request.

Información relacionada

["Obsoleto: modificaciones de la solicitud PUT Bucket para cumplimiento"](#)

Políticas de acceso a grupos y buckets

Utilice políticas de acceso a grupos y buckets

StorageGRID utiliza el lenguaje de políticas de Amazon Web Services (AWS) para permitir que los inquilinos de S3 controlen el acceso a los depósitos y los objetos dentro de esos depósitos. El sistema StorageGRID implementa un subconjunto del lenguaje de políticas de la API REST de S3. Las políticas de acceso para la API S3 están escritas en JSON.

Descripción general de la política de acceso

StorageGRID admite dos tipos de políticas de acceso.

- **Políticas de bucket**, que se administran mediante las operaciones de API S3 `GetBucketPolicy`, `PutBucketPolicy` y `DeleteBucketPolicy` o la API `Tenant Manager` o `Tenant Management`. Las políticas de depósito se adjuntan a los depósitos, por lo que están configuradas para controlar el acceso de los usuarios en la cuenta del propietario del depósito u otras cuentas al depósito y a los objetos que contiene. Una política de buckets se aplica solo a un bucket y posiblemente a varios grupos.
- **Políticas de grupo**, que se configuran mediante el Administrador de inquilinos o la API de administración de inquilinos. Las políticas de grupo están asociadas a un grupo en la cuenta, por lo que están configuradas para permitir que ese grupo acceda a recursos específicos que pertenecen a esa cuenta. Una política de grupo se aplica solo a un grupo y posiblemente a varios grupos.



No hay diferencia de prioridad entre las políticas de grupo y de grupo.

Las políticas de grupo y de depósito de StorageGRID siguen una gramática específica definida por Amazon. Dentro de cada política hay una serie de declaraciones de políticas, y cada declaración contiene los siguientes elementos:

- ID de declaración (Sid) (opcional)
- Efecto
- Director/No director
- Recurso/NoRecurso

- Acción/No acción
- Condición (opcional)

Las declaraciones de política se crean utilizando esta estructura para especificar permisos: Otorgar <Efecto> para permitir/denegar que <Principal> realice <Acción> en <Recurso> cuando se aplica <Condición>.

Cada elemento de política se utiliza para una función específica:

Elemento	Descripción
Sid	El elemento Sid es opcional. El Sid solo pretende servir como descripción para el usuario. Se almacena pero no es interpretado por el sistema StorageGRID .
Efecto	Utilice el elemento Efecto para establecer si las operaciones especificadas están permitidas o denegadas. Debe identificar las operaciones que permite (o deniega) en depósitos u objetos utilizando las palabras clave del elemento Acción compatible.
Director/No director	Puede permitir que usuarios, grupos y cuentas accedan a recursos específicos y realicen 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, solo la cuenta raíz tiene acceso a los recursos que posee la cuenta. Solo es necesario especificar el elemento Principal en una política de bucket. Para las políticas de grupo, el grupo al que está asociada la política es el elemento Principal implícito.
Recurso/NoRecurso	El elemento Recurso identifica depósitos y objetos. Puede permitir o denegar permisos para depósitos y objetos utilizando el nombre de recurso de Amazon (ARN) para identificar el recurso.
Acción/No acción	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 mismo. Se deniega el acceso a menos que usted asigne permisos específicos, pero puede usar la denegación explícita para anular un permiso otorgado por otra política.
Condición	El elemento Condición es opcional. Las condiciones le permiten crear expresiones para determinar cuándo se debe aplicar una política.

En el elemento Acción, 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 Recurso, puede utilizar los caracteres comodín (*) y (?). Mientras que el asterisco (*) coincide con 0 o más caracteres, el signo de interrogación (?) coincide con cualquier carácter individual.

En el elemento Principal, no se admiten caracteres comodín excepto para establecer acceso anónimo, que otorga permiso a todos. Por ejemplo, establece el comodín (*) como valor principal.

```
"Principal": "*"}
```

```
"Principal": {"AWS": "*"}
```

En el siguiente ejemplo, la declaración utiliza los elementos Efecto, Principal, Acción y Recurso. Este ejemplo muestra una declaración de política de bucket completa que utiliza el efecto "Permitir" para otorgar a los principales, el grupo de administración `federated-group/admin` y el grupo financiero `federated-group/finance`, permisos para realizar la Acción `s3:ListBucket` en el cubo llamado `mybucket` y la Acción `s3:GetObject` en todos los objetos dentro de ese cubo.

```
{
  "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:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

La política de depósito tiene un límite de tamaño de 20 480 bytes y la política de grupo tiene un límite de tamaño de 5120 bytes.

Coherencia de las políticas

De forma predeterminada, cualquier actualización que realice en las políticas de grupo será coherente en el futuro. Cuando una política de grupo se vuelve consistente, los cambios pueden tardar 15 minutos adicionales en surtir efecto, debido al almacenamiento en caché de la política. De forma predeterminada, todas las actualizaciones que realice en las políticas de depósito serán muy coherentes.

Según sea necesario, puede cambiar las garantías de consistencia para las actualizaciones de la política de

bucket. Por ejemplo, es posible que desee que un cambio en una política de depósito esté disponible durante una interrupción del sitio.

En este caso, puede configurar el `Consistency-Control` encabezado en la solicitud `PutBucketPolicy`, o puede utilizar la solicitud de consistencia `PUT Bucket`. Cuando una política de bucket se vuelve consistente, los cambios pueden tardar 8 segundos adicionales en surtir efecto, debido al almacenamiento en caché de políticas.



Si establece la consistencia en un valor diferente para solucionar una situación temporal, asegúrese de restablecer la configuración de nivel de depósito a su valor original cuando haya terminado. De lo contrario, todas las futuras solicitudes de bucket utilizarán la configuración modificada.

Utilice ARN en declaraciones de políticas

En las declaraciones de políticas, el ARN se utiliza en los elementos `Principal` y `Recurso`.

- Utilice esta sintaxis para especificar el ARN del recurso S3:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Utilice esta sintaxis para especificar el ARN del recurso de identidad (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 del objeto.
- Los caracteres internacionales, que se pueden especificar en la clave del objeto, deben codificarse utilizando JSON UTF-8 o utilizando secuencias de escape JSON `\u`. No se admite la codificación porcentual.

"Sintaxis URN RFC 2141"

El cuerpo de la solicitud HTTP para la operación `PutBucketPolicy` debe estar codificado con `charset=UTF-8`.

Especificar recursos en una política

En las declaraciones de políticas, puede utilizar el elemento `Recurso` para especificar el depósito o el objeto para el cual se permiten o deniegan permisos.

- Cada declaración de política requiere un elemento de recurso. En una política, los recursos se denotan mediante el elemento `Resource` , o alternativamente, `NotResource` para exclusión.
- Usted especifica recursos con un ARN de recurso S3. Por ejemplo:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- También puede utilizar variables de política dentro de la clave del objeto. Por ejemplo:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- El valor del recurso puede especificar un depósito que aún no existe cuando se crea una política de grupo.

Especificar los principales en una política

Utilice el elemento `Principal` para identificar el usuario, grupo o cuenta de inquilino a quien se le permite o deniega el acceso al recurso mediante la declaración de política.

- Cada declaración de política en una política de grupo 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 principales se indican con el elemento `"Principal"` o, alternativamente, `"NoPrincipal"` para su exclusión.
- Las identidades basadas en cuentas deben especificarse mediante un ID o un ARN:

```
"Principal": { "AWS": "account_id" }
"Principal": { "AWS": "identity_arn" }
```

- Este ejemplo 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 solo la cuenta raíz:

```
"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 ("Administradores"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-group/Managers" }
```

- Puede especificar un principal anónimo:

```
"Principal": "*" 
```

- Para evitar ambigüedades, puede utilizar el UUID del 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 elimina. Si un nuevo Alex se une a la organización y se le asigna el mismo `Alex` nombre de usuario, el nuevo usuario podría heredar involuntariamente los permisos otorgados al usuario original.

- El valor principal puede especificar un nombre de grupo/usuario que aún no existe cuando se crea una política de depósito.

Especificar permisos en una política

En una política, el elemento Acción se utiliza para permitir o denegar permisos a un recurso. Hay un conjunto de permisos que puedes especificar en una política, que se indican con el elemento "Acción" o, alternativamente, "No acción" para la exclusión. Cada uno de estos elementos se asigna a operaciones específicas de la API REST de S3.

Las tablas enumeran los permisos que se aplican a los depósitos y los permisos que se aplican a los objetos.



Amazon S3 ahora usa el permiso `s3:PutReplicationConfiguration` para las acciones `PutBucketReplication` y `DeleteBucketReplication`. `StorageGRID` utiliza permisos separados para cada acción, lo que coincide con la especificación original de Amazon S3.



Se realiza una eliminación cuando se utiliza una operación `put` para sobrescribir un valor existente.

Permisos que se aplican a los buckets

Permisos	Operaciones de la API REST de S3	Personalizado para StorageGRID
<code>s3:CrearCubo</code>	Crear cubo	Sí. Nota: Úselo solo en políticas de grupo.
<code>s3:Eliminar depósito</code>	Eliminar cubo	

Permisos	Operaciones de la API REST de S3	Personalizado para StorageGRID
s3:Notificación de metadatos de eliminación de depósito	Configuración de notificación de metadatos del depósito DELETE	Sí
s3: Eliminar política de depósito	Política de eliminación de cubos	
s3:Eliminar configuración de replicación	EliminarReplicaciónDeBucket	Sí, permisos separados para PUT y DELETE
s3:ObtenerAcl del depósito	ObtenerBucketAcl	
s3:Obtener cumplimiento del cubo	Cumplimiento de GET Bucket (obsoleto)	Sí
s3: Obtener consistencia del cubo	Obtener consistencia del bucket	Sí
s3:ObtenerBucketCORS	ObtenerBucketCors	
s3:Obtener configuración de cifrado	Obtener cifrado de cubo	
s3: Obtener hora del último acceso al depósito	GET Hora del último acceso al bucket	Sí
s3: Obtener ubicación del depósito	Obtener la ubicación del cubo	
s3:Obtener notificación de metadatos del depósito	Configuración de notificación de metadatos del depósito GET	Sí
s3:Obtener notificación del cubo	Configuración de GetBucketNotification	
s3:Configuración de bloqueo de objeto de depósito	Obtener configuración de bloqueo de objeto	
s3: Obtener política de depósito	Obtener política de cubo	
s3: Obtener etiquetado de cubo	Obtener etiquetado de cubos	
s3: Obtener versiones de Bucket	Obtener versiones de Bucket	
s3:Obtener configuración del ciclo de vida	Obtener configuración del ciclo de vida del cubo	
s3:Obtener configuración de replicación	Obtener réplica de cubo	

Permisos	Operaciones de la API REST de S3	Personalizado para StorageGRID
s3: Listar todos mis cubos	• Lista de cubos • Uso de almacenamiento GET	Sí, para el uso de almacenamiento GET. Nota: Úselo solo en políticas de grupo.
s3:ListBucket	• Lista de objetos • Cubo de cabeza • Restaurar objeto	
s3:ListBucketMultipartUploads	• Lista de cargas de varias partes • Restaurar objeto	
s3:ListBucketVersions	GET Versiones del Bucket	
s3:Cumplimiento de PutBucket	Cumplimiento del contenedor PUT (obsoleto)	Sí
s3:Consistencia del cubo de colocación	Consistencia del depósito PUT	Sí
s3:PonerCuboCORS	• EliminarBucketCors† • PonerBucketCors	
s3:PonerConfiguraciónDeCifrado	• Eliminar cifrado del cubo • Cifrado de PutBucket	
s3:PonerBucketÚltimoAccesoHora	Hora del último acceso al depósito PUT	Sí
s3:Notificación de metadatos de PutBucket	Configuración de notificación de metadatos del depósito PUT	Sí
s3:Notificación de depósito de colocación	Configuración de notificación de PutBucket	
s3:Configuración de bloqueo de objeto PutBucket	• CreateBucket con el x-amz-bucket-object-lock-enabled: true encabezado de solicitud (también requiere el permiso s3:CreateBucket) • Configuración de bloqueo de objeto de colocación	
s3:Política de depósito de colocación	Política de depósito de basura	

Permisos	Operaciones de la API REST de S3	Personalizado para StorageGRID
s3:Etiquetado de cubo de colocación	• Eliminar etiquetado de cubos† • Etiquetado de PutBucket	
s3:Versión de PutBucket	Versiones de PutBucket	
s3:Configuración del ciclo de vida de PutLifecycle	• Eliminar ciclo de vida del cubo† • Configuración del ciclo de vida de PutBucket	
s3:PonerConfiguraciónDeReplicación	Replicación de PutBucket	Sí, permisos separados para PUT y DELETE

Permisos que se aplican a los objetos

Permisos	Operaciones de la API REST de S3	Personalizado para StorageGRID
s3:AbortarCargaMultiparte	• AbortarMultipartUpload • Restaurar objeto	
s3: Retención de gobernanza de bypass	• Eliminar objeto • Eliminar objetos • PonerRetenciónDeObjeto	
s3:EliminarObjeto	• Eliminar objeto • Eliminar objetos • Restaurar objeto	
s3:EliminarEtiquetadoDeObjeto	Eliminar etiquetado de objetos	
s3: Eliminar etiquetado de versión de objeto	DeleteObjectTagging (una versión específica del objeto)	
s3:EliminarVersiónDeObjeto	DeleteObject (una versión específica del objeto)	
s3:Obtener objeto	• Obtener objeto • Objeto principal • Restaurar objeto • Seleccionar contenido del objeto	

Permisos	Operaciones de la API REST de S3	Personalizado para StorageGRID
s3:ObtenerAclObjeto	ObtenerObjetoAcl	
s3:ObtenerRetenciónLegalDeObjeto	Obtener retención legal de objeto	
s3:ObtenerRetenciónDeObjeto	Obtener retención de objetos	
s3:Obtener etiquetado de objeto	Obtener etiquetado de objetos	
s3: Obtener etiquetado de versión de objeto	GetObjectTagging (una versión específica del objeto)	
s3:ObtenerVersiónDeObjeto	GetObject (una versión específica del objeto)	
s3:ListaMultiparteSubirPartes	Lista de partes, Restaurar objeto	
s3:PonerObjeto	• PonerObjeto • Copiar objeto • Restaurar objeto • Crear carga de varias partes • Carga completa de varias partes • Subir parte • Subir copia parcial	
s3:PonerObjetoLegalRetenido	PonerObjetoLegalRetención	
s3:PonerRetenciónDeObjeto	PonerRetenciónDeObjeto	
s3:Etiquetado de objetos de colocación	Etiquetado de objetos puestos	
s3:Etiquetado de versión de objeto de colocación	PutObjectTagging (una versión específica del objeto)	
s3:PonerObjetoSobrescrito	• PonerObjeto • Copiar objeto • Etiquetado de objetos puestos • Eliminar etiquetado de objetos • Carga completa de varias partes	Sí
s3:RestaurarObjeto	Restaurar objeto	

Utilice el permiso PutOverwriteObject

El permiso s3:PutOverwriteObject es un permiso de StorageGRID personalizado que se aplica a las operaciones que crean o actualizan objetos. La configuración de este permiso determina si el cliente puede sobrescribir los datos de un objeto, los metadatos definidos por el usuario o el etiquetado de objetos S3.

Las posibles configuraciones para este permiso incluyen:

- **Permitir:** El cliente puede sobrescribir un objeto. Esta es la configuración predeterminada.
- **Denegar:** El cliente no puede sobrescribir un objeto. Cuando se establece en Denegar, el permiso PutOverwriteObject funciona de la siguiente manera:
 - Si se encuentra un objeto existente en la misma ruta:
 - Los datos del objeto, los metadatos definidos por el usuario o el etiquetado del objeto S3 no se pueden sobrescribir.
 - Cualquier operación de ingesta en curso se cancela y se devuelve un error.
 - Si el control de versiones S3 está habilitado, la configuración Denegar evita que las operaciones PutObjectTagging o DeleteObjectTagging modifiquen el TagSet de 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 estuviera configurado Permitir.



Si la política S3 actual permite sobrescribir y el permiso PutOverwriteObject está configurado en Denegar, el cliente no puede sobrescribir los datos de un objeto, los metadatos definidos por el usuario ni el etiquetado de objetos. Además, si se selecciona la casilla de verificación **Evitar modificación del cliente (CONFIGURACIÓN > Configuración de seguridad > Red y objetos)**, esa configuración anula la configuración del permiso PutOverwriteObject.

Especificar condiciones en una póliza

Las condiciones definen cuándo entrará en vigor una política. Las condiciones constan de operadores y pares clave-valor.

Las condiciones utilizan pares clave-valor para la evaluación. Un elemento Condición puede contener múltiples condiciones, y cada condición puede contener múltiples pares clave-valor. El bloque de condición utiliza el siguiente formato:

```
Condition: {  
  condition_type: {  
    condition_key: condition_values
```

En el siguiente ejemplo, la condición IpAddress utiliza la clave de condición Sourcelp.

```

"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
}

```

Operadores de condición admitidos

Los operadores de condición se clasifican de la siguiente manera:

- Cadena
- Numérico
- Booleano
- Dirección IP
- Comprobación nula

Operadores de condición	Descripción
Cadenalqual	Compara una clave con un valor de cadena basándose en la coincidencia exacta (distingue entre mayúsculas y minúsculas).
CadenaNolqual	Compara una clave con un valor de cadena basándose en la coincidencia negada (distingue entre mayúsculas y minúsculas).
CadenalqualIgnorarMayúsculas y Minúsculas	Compara una clave con un valor de cadena basándose en la coincidencia exacta (ignora mayúsculas y minúsculas).
CadenaNolqualIgnorarMayúsculas y Minúsculas	Compara una clave con un valor de cadena basándose en la coincidencia negada (ignora mayúsculas y minúsculas).
Similar a una cadena	Compara una clave con un valor de cadena basándose en la coincidencia exacta (distingue entre mayúsculas y minúsculas). Puede incluir caracteres comodín * y ?.
CadenaNoMe Gusta	Compara una clave con un valor de cadena basándose en la coincidencia negada (distingue entre mayúsculas y minúsculas). Puede incluir caracteres comodín * y ?.
NumericEquals	Compara una clave con un valor numérico basándose en la coincidencia exacta.
NuméricoNolqual	Compara una clave con un valor numérico basándose en la coincidencia negada.

Operadores de condición	Descripción
NuméricoMayorQue	Compara una clave con un valor numérico basándose en la coincidencia "mayor que".
NuméricoMayorQueIgual	Compara una clave con un valor numérico basándose en la coincidencia "mayor o igual que".
NuméricoMenosQue	Compara una clave con un valor numérico basándose en la coincidencia "menor que".
NuméricoMenorQueIgual	Compara una clave con un valor numérico basándose en la coincidencia "menor o igual que".
Bool	Compara una clave con un valor booleano basándose en la coincidencia "verdadero o falso".
Dirección IP	Compara una clave con una dirección IP o un rango de direcciones IP.
No dirección IP	Compara una clave con una dirección IP o un rango de direcciones IP basándose en la coincidencia negada.
Nulo	Comprueba si una clave de condición está presente en el contexto de solicitud actual.

Claves de condición admitidas

Claves de condición	Comportamiento	Descripción
aws:Fuentelp	Operadores de IP	Se comparará con la dirección IP desde la que se envió la solicitud. Se puede utilizar para operaciones con cubos o con objetos. Nota: Si la solicitud S3 se envió a través del servicio Load Balancer en los nodos de administración y los nodos de puerta de enlace, esto se comparará con la dirección IP ascendente del servicio Load Balancer. Nota: Si se utiliza un balanceador de carga de terceros no transparente, esto se comparará con la dirección IP de ese balanceador de carga. Cualquier X-Forwarded-For El encabezado se ignorará porque no se puede determinar su validez.
aws:nombre de usuario	Recurso/Identidad	Se comparará con el nombre de usuario del remitente desde el que se envió la solicitud. Se puede utilizar para operaciones con cubos o con objetos.

Claves de condición	Comportamiento	Descripción
s3:delimitador	s3:ListBucket y Permisos s3:ListBucketVersions	Se comparará con el parámetro delimitador especificado en una solicitud ListObjects o ListObjectVersions.
s3:ExistingObjectTag/<clave de etiqueta>	s3:EliminarEtiquetadoDeObjeto s3: Eliminar etiquetado de versión de objeto s3:Obtener objeto s3:ObtenerAclObjeto 3: Obtener etiquetado de objetos s3:ObtenerVersiónDeObjeto s3:ObtenerAcl de versión de objeto s3: Obtener etiquetado de versión de objeto s3:PonerObjetoAcl s3:Etiquetado de objetos de colocación s3:PonerObjetoVersiónAcl s3:Etiquetado de versión de objeto de colocación	Requerirá que el objeto existente tenga la clave y el valor de etiqueta específicos.
s3:máximo de teclas	s3:ListBucket y Permisos s3:ListBucketVersions	Se comparará con el parámetro max-keys especificado en una solicitud ListObjects o ListObjectVersions.

Claves de condición	Comportamiento	Descripción
s3: días de retención restantes del bloqueo de objeto	s3:PonerObjeto	Se compara con la fecha de conservación especificada en el <code>x-amz-object-lock-retain-until-date</code> encabezado de solicitud o calculado a partir del período de retención predeterminado del depósito para asegurarse de que estos valores estén dentro del rango permitido para las siguientes solicitudes: • PonerObjeto • Copiar objeto • Crear carga de varias partes
s3: días de retención restantes del bloqueo de objeto	s3:PonerRetenciónDeObjeto	Se compara con la fecha de retención hasta especificada en la solicitud <code>PutObjectRetention</code> para garantizar que esté dentro del rango permitido.
s3:prefijo	s3:ListBucket y Permisos s3:ListBucketVersions	Se comparará con el parámetro de prefijo especificado en una solicitud <code>ListObjects</code> o <code>ListObjectVersions</code> .
s3:RequestObjectTag/<clave de etiqueta>	s3:PonerObjeto s3:Etiquetado de objetos de colocación s3:Etiquetado de versión de objeto de colocación	Requerirá una clave y un valor de etiqueta específicos cuando la solicitud de objeto incluya etiquetado.

Especificar variables en una política

Puede utilizar variables en las políticas para completar la información de políticas cuando esté disponible. Puede utilizar variables de política en el `Resource` elemento y en comparaciones de cadenas en el `Condition` elemento.

En este ejemplo, la variable `${aws:username}` es parte del elemento Recurso:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

En este ejemplo, la variable `${aws:username}` es parte del valor de la condición en el bloque de condición:

```

"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}

```

Variable	Descripción
<code>\${aws:SourceIp}</code>	Utiliza la clave SourceIp como variable proporcionada.
<code>\${aws:username}</code>	Utiliza la clave de nombre de usuario como variable proporcionada.
<code>\${s3:prefix}</code>	Utiliza la clave de prefijo específica del servicio como la variable proporcionada.
<code>\${s3:max-keys}</code>	Utiliza la clave max-keys específica del servicio como variable proporcionada.
<code>\${*}</code>	Carácter especial. Utiliza el carácter como un carácter literal *.
<code>\${?}</code>	Carácter especial. Utiliza el carácter como un carácter literal ?.
<code>\${\$}</code>	Carácter especial. Utiliza el carácter como un carácter literal \$.

Crear políticas que requieran un manejo especial

A veces, una política puede otorgar permisos que son peligrosos para la seguridad o para las operaciones continuas, como bloquear al usuario raíz de la cuenta. La implementación de la API REST S3 de StorageGRID es menos restrictiva durante la validación de políticas que Amazon, pero igualmente estricta durante la evaluación de políticas.

Descripción de la política	Tipo de póliza	Comportamiento de Amazon	Comportamiento de StorageGRID
Negarse a sí mismo cualquier permiso a la cuenta raíz	Balde	Válido y aplicado, pero la cuenta de usuario raíz conserva el permiso para todas las operaciones de política de bucket de S3	Mismo
Negarme cualquier permiso a un usuario o grupo	Grupo	Válido y ejecutado	Mismo

Descripción de la política	Tipo de póliza	Comportamiento de Amazon	Comportamiento de StorageGRID
Permitir a un grupo de cuentas extranjeras cualquier permiso	Balde	Principal inválido	Válido, pero los permisos para todas las operaciones de políticas de bucket S3 devuelven un error 405 Método no permitido cuando lo permite una política
Permitir a una cuenta externa root o a un usuario cualquier permiso	Balde	Válido, pero los permisos para todas las operaciones de políticas de bucket S3 devuelven un error 405 Método no permitido cuando lo permite una política	Mismo
Permitir a todos permisos para todas las acciones	Balde	Válido, pero los permisos para todas las operaciones de política de bucket S3 devuelven un error 405 Método no permitido para la raíz de la cuenta externa y los usuarios	Mismo
Negar a todos los permisos para todas las acciones	Balde	Válido y aplicado, pero la cuenta de usuario raíz conserva el permiso para todas las operaciones de política de bucket de S3	Mismo
El principal es un usuario o grupo inexistente	Balde	Principal inválido	Válido
El recurso es un bucket S3 inexistente	Grupo	Válido	Mismo
Principal es un grupo local	Balde	Principal inválido	Válido
La política otorga a una cuenta que no es de propietario (incluidas las cuentas anónimas) permisos para colocar objetos.	Balde	Válido. Los objetos son propiedad de la cuenta del creador y la política de buckets no se aplica. La cuenta del creador debe otorgar permisos de acceso para el objeto mediante listas de control de acceso (ACL) de objeto.	Válido. Los objetos son propiedad de la cuenta del propietario del depósito. Se aplica la política de cubos.

Protección de escritura única y lectura múltiple (WORM)

Puede crear depósitos de escritura única y lectura múltiple (WORM) para proteger datos, metadatos de objetos definidos por el usuario y etiquetado de objetos S3. Configura los depósitos WORM para permitir la creación de nuevos objetos y evitar sobrescrituras o eliminaciones de contenido existente. Utilice uno de los enfoques descritos aquí.

Para garantizar que siempre se rechacen las sobrescrituras, puede:

- Desde el Administrador de red, vaya a **CONFIGURACIÓN > Seguridad > Configuración de seguridad > Red y objetos** y seleccione la casilla de verificación **Evitar modificación del cliente**.
- Aplicar las siguientes reglas y políticas S3:
 - Agregue una operación PutOverwriteObject DENY a la política S3.
 - Agregue una operación DeleteObject DENY a la política S3.
 - Agregue una operación PutObject ALLOW a la política S3.



Establecer DeleteObject como DENY en una política S3 no impide que ILM elimine objetos cuando existe una regla como "cero copias después de 30 días".



Incluso cuando se aplican todas estas reglas y políticas, no protegen contra escrituras simultáneas (ver Situación A). Protegen contra sobrescrituras completadas secuenciales (ver Situación B).

Situación A: Escrituras concurrentes (sin protección)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -----> OK
```

Situación B: Sobrescrituras secuenciales completadas (protegidas contra)

```
/mybucket/important.doc
PUT#1 -----> PUT#2 ---X (denied)
```

Información relacionada

- ["Cómo las reglas ILM de StorageGRID administran los objetos"](#)
- ["Ejemplos de políticas de depósito"](#)
- ["Políticas de grupo de ejemplo"](#)
- ["Administrar objetos con ILM"](#)
- ["Utilice una cuenta de inquilino"](#)

Ejemplos de políticas de depósito

Utilice los ejemplos de esta sección para crear políticas de acceso de StorageGRID para los buckets.

Las políticas de depósito especifican los permisos de acceso para el depósito al que está asociada la política. Puede configurar una política de bucket mediante la API S3 PutBucketPolicy a través de una de estas herramientas:

- ["Administrador de inquilinos"](#) .
- AWS CLI usando este comando (consulte ["Operaciones en buckets"](#)):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Ejemplo: Permitir a todos el acceso de solo lectura a un depósito

En este ejemplo, todos, incluso los anónimos, pueden enumerar objetos en el depósito y realizar operaciones GetObject en todos los objetos del depósito. Se denegarán todas las demás operaciones. Tenga en cuenta que esta política puede no ser particularmente útil porque nadie excepto la cuenta raíz tiene permisos para escribir en el depósito.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ]
    }
  ]
}
```

Ejemplo: Permitir a todos los usuarios de una cuenta acceso completo y a todos los usuarios de otra cuenta acceso de solo lectura a un depósito.

En este ejemplo, a todos en una cuenta específica se les permite acceso completo a un depósito, mientras que a todos en otra cuenta específica solo se les permite listar el depósito y realizar operaciones GetObject en objetos en el depósito comenzando con el `shared/` prefijo de clave de objeto.



En StorageGRID, los objetos creados por una cuenta que no es de propietario (incluidas las cuentas anónimas) son propiedad de la cuenta del propietario del depósito. La política de bucket 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 a todos acceso de solo lectura a un depósito y acceso completo a un grupo específico

En este ejemplo, todos, incluido el anónimo, pueden listar el depósito y realizar operaciones `GetObject` en todos los objetos del depósito, mientras que solo los usuarios que pertenecen al grupo `Marketing` En la cuenta especificada se permite el acceso completo.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Ejemplo: Permitir a todos el acceso de lectura y escritura a un depósito si el cliente está en el rango de IP

En este ejemplo, todos, incluso los anónimos, pueden enumerar el depósito y realizar cualquier operación de objeto en todos los objetos del depósito, siempre que las solicitudes provengan de un rango de IP específico (54.240.143.0 a 54.240.143.255, excepto 54.240.143.188). Se rechazarán todas las demás operaciones y todas las solicitudes 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 depósito exclusivamente a un usuario federado específico

En este ejemplo, al usuario federado Alex se le permite acceso completo a la `examplebucket` cubo y sus objetos. A todos los demás usuarios, incluido 'root', se les niega explícitamente todas las operaciones. Sin embargo, tenga en cuenta que a 'root' nunca se le niegan los permisos para Put/Get/DeleteBucketPolicy.


```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Ejemplo: Permiso PutOverwriteObject

En este ejemplo, el `Deny` El efecto para `PutOverwriteObject` y `DeleteObject` garantiza que nadie pueda sobrescribir o 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/*"
    }
  ]
}

```

Políticas de grupo de ejemplo

Utilice los ejemplos de esta sección para crear políticas de acceso de StorageGRID para grupos.

Las políticas de grupo especifican los permisos de acceso para el grupo al que está asociada la política. No hay `Principal` elemento de la política porque es implícito. Las políticas de grupo se configuran mediante el Administrador de inquilinos o la API.

Ejemplo: Establecer una política de grupo mediante el Administrador de inquilinos

Cuando agrega o edita un grupo en el Administrador de inquilinos, puede seleccionar una política de grupo para determinar qué permisos de acceso a S3 tendrán los miembros de este grupo. Ver ["Crear grupos para un inquilino de S3"](#).

- **Sin acceso S3:** Opción predeterminada. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que se les conceda acceso con una política de bucket. Si selecciona esta opción, solo el usuario root tendrá acceso a los recursos de S3 de forma predeterminada.
- **Acceso de solo lectura:** los usuarios de este grupo tienen acceso de solo lectura a los recursos de S3. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas. Cuando selecciona esta opción, la cadena JSON para una política de grupo de solo lectura aparece en el cuadro de texto. No puedes editar esta cadena.
- **Acceso completo:** los usuarios de este grupo tienen acceso completo a los recursos de S3, incluidos los buckets. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puedes editar esta cadena.
- **Mitigación de ransomware:** esta política de muestra se aplica a todos los depósitos de este inquilino. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden eliminar de forma permanente objetos de los depósitos que tienen habilitada la versión de objetos.

Los usuarios del administrador de inquilinos que tienen el permiso Administrar todos los depósitos pueden anular esta política de grupo. Limite el permiso Administrar todos los depósitos a usuarios de confianza y utilice la autenticación multifactor (MFA) cuando esté disponible.

- **Personalizado:** A los usuarios del grupo se les otorgan los permisos que usted especifique en el cuadro de texto.

Ejemplo: Permitir al grupo acceso completo a todos los depósitos

En este ejemplo, a todos los miembros del grupo se les permite acceso total a todos los depósitos propiedad de la cuenta del inquilino, a menos que la política del depósito lo deniegue explícitamente.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Ejemplo: Permitir acceso de solo lectura al grupo a todos los depósitos

En este ejemplo, todos los miembros del grupo tienen acceso de solo lectura a los recursos de S3, a menos que la política del bucket lo niegue explícitamente. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas.

```

{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}

```

Ejemplo: Permitir a los miembros del grupo acceso completo únicamente a su "carpeta" en un depósito

En este ejemplo, a los miembros del grupo solo se les permite enumerar y acceder a su carpeta específica (prefijo de clave) en el depósito especificado. Tenga en cuenta que los permisos de acceso de otras políticas de grupo y la política de depósito deben considerarse 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}/*"
    }
  ]
}

```

Operaciones de S3 rastreadas en los registros de auditoría

Los mensajes de auditoría son generados por los servicios de StorageGRID y almacenados en archivos de registro de texto. Puede revisar los mensajes de auditoría específicos de S3 en el registro de auditoría para obtener detalles sobre las operaciones de buckets y objetos.

Operaciones de bucket rastreadas en los registros de auditoría

- Crear cubo
- Eliminar cubo
- Eliminar etiquetado de cubo
- Eliminar objetos
- Obtener etiquetado de cubos
- Cubo de cabeza
- Lista de objetos
- Lista de versiones de objetos
- Cumplimiento del contenedor PUT
- Etiquetado de PutBucket
- Versiones de PutBucket

Operaciones de objetos rastreadas en los registros de auditoría

- Carga completa de varias partes
- Copiar objeto
- Eliminar objeto
- Obtener objeto
- Objeto principal
- PonerObjeto
- Restaurar objeto
- Seleccionar objeto
- UploadPart (cuando una regla ILM utiliza ingesta equilibrada o estricta)
- UploadPartCopy (cuando una regla ILM utiliza ingesta equilibrada o estricta)

Información relacionada

- ["Archivo de registro de auditoría de acceso"](#)
- ["El cliente escribe mensajes de auditoría"](#)
- ["El cliente lee mensajes de auditoría"](#)

Utilice la API REST de Swift (fin de vida útil)

Utilice la API REST de Swift

El soporte para la API Swift ha llegado al final de su vida útil y se eliminará en una versión futura.



Se han eliminado los detalles rápidos de esta versión del sitio de documentación. Ver ["StorageGRID 11.8: Usar la API REST de Swift"](#) .

Supervisar y solucionar problemas de un sistema StorageGRID

Supervisar el sistema StorageGRID

Supervisar un sistema StorageGRID

Supervise periódicamente su sistema StorageGRID para asegurarse de que funcione como se espera.

Antes de empezar

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



Para cambiar las unidades de los valores de almacenamiento que se muestran en el Administrador de cuadrícula, seleccione el menú desplegable de usuario en la parte superior derecha del Administrador de cuadrícula y luego seleccione **Preferencias de usuario**.

Acerca de esta tarea

Estas instrucciones describen cómo:

- ["Ver y administrar el panel de control"](#)
- ["Ver la página de Nodos"](#)
- ["Supervise periódicamente estos aspectos del sistema:"](#)
 - ["Salud del sistema"](#)
 - ["Capacidad de almacenamiento"](#)
 - ["Gestión del ciclo de vida de la información"](#)
 - ["Recursos de redes y sistemas"](#)
 - ["Actividad de los inquilinos"](#)
 - ["Operaciones de equilibrio de carga"](#)
 - ["Conexiones de federación de red"](#)
- ["Administrar alertas"](#)
- ["Ver archivos de registro"](#)
- ["Configurar mensajes de auditoría y destinos de registro"](#)
- ["Utilice un servidor syslog externo"](#) para recopilar información de auditoría
- ["Utilice SNMP para la monitorización"](#)
- ["Obtener datos adicionales de StorageGRID"](#), incluidas métricas y diagnósticos

Ver y administrar el panel de control

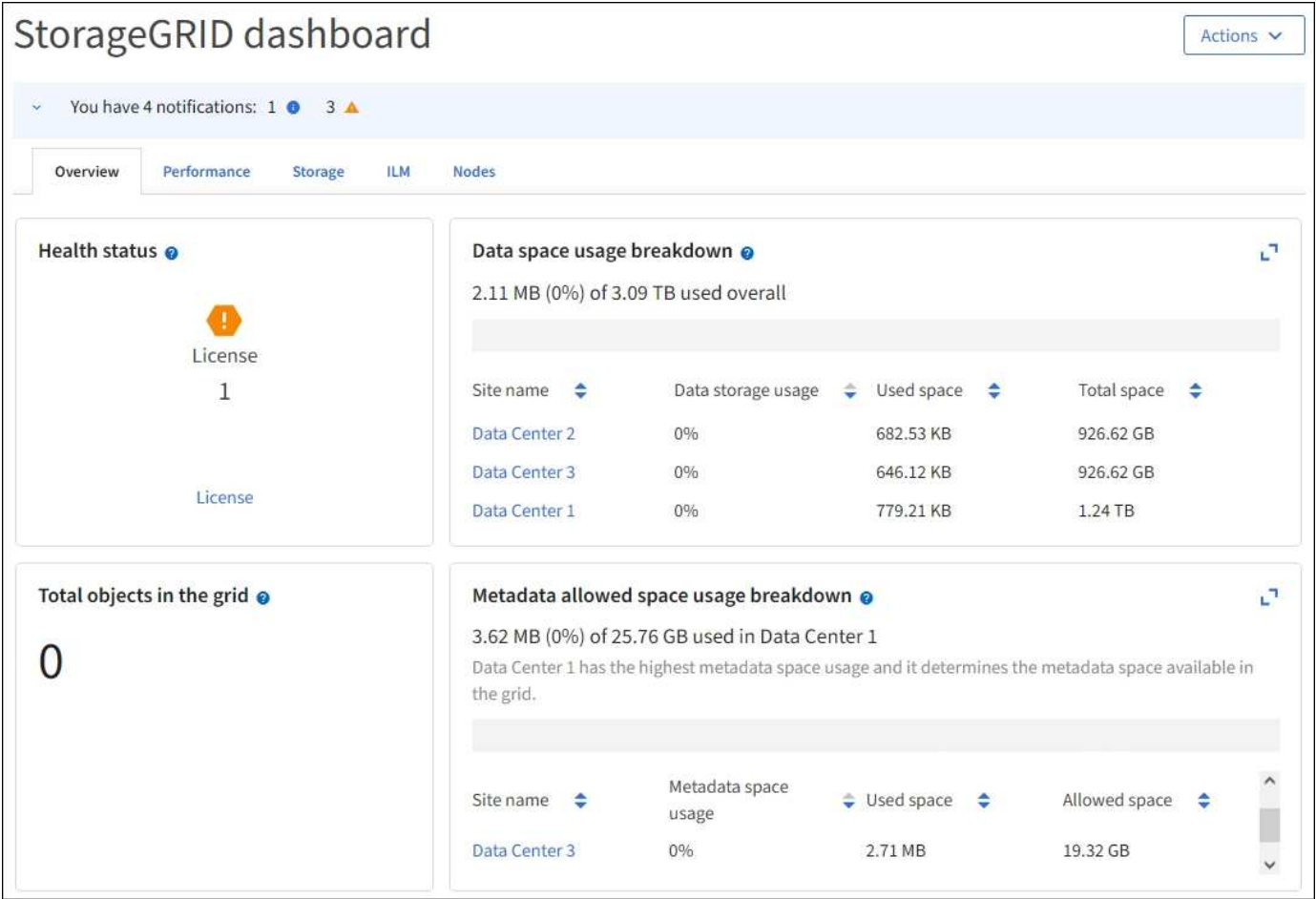
Puede utilizar el panel de control para supervisar las actividades del sistema de un vistazo. Puede crear paneles personalizados para supervisar su implementación de

StorageGRID.



Para cambiar las unidades de los valores de almacenamiento que se muestran en el Administrador de cuadrícula, seleccione el menú desplegable de usuario en la parte superior derecha del Administrador de cuadrícula y luego seleccione **Preferencias de usuario**.

Su panel de control puede ser diferente según la configuración del sistema.



Ver el panel de control

El panel de control consta de pestañas que contienen información específica sobre el sistema StorageGRID . Cada pestaña contiene categorías de información que se muestran en las tarjetas.

Puede utilizar el panel de control proporcionado por el sistema tal como está. Además, puede crear paneles personalizados que contengan solo las pestañas y tarjetas que son relevantes para monitorear su implementación de StorageGRID.

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

Pestaña en el panel de control proporcionado por el sistema	Contiene
Descripción general	Información general sobre la cuadrícula, como alertas activas, uso de espacio y total de objetos en la cuadrícula.
Actuación	Uso de espacio, almacenamiento utilizado a lo largo del tiempo, operaciones S3, duración de la solicitud, tasa de error.
Almacenamiento	Uso de cuota de inquilino y uso de espacio lógico. Pronósticos de uso de espacio para datos de usuario y metadatos.
ILM	Cola de gestión del ciclo de vida de la información y tasa de evaluación.
Nodos	Uso de CPU, datos y memoria por nodo. Operaciones S3 por nodo. Distribución de nodo a sitio.

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

Administrar paneles de control

Si tiene acceso root (ver "[Permisos del grupo de administradores](#)"), puede realizar las siguientes tareas de administración de paneles:

- Crea un panel de control personalizado desde cero. Puede utilizar paneles personalizados para controlar qué información de StorageGRID se muestra y cómo se organiza esa información.
- Clonar un panel para crear paneles personalizados.
- Establecer un panel activo para un usuario. El panel activo puede ser el panel proporcionado por el sistema o un panel personalizado.
- Establezca un panel predeterminado, que es lo que ven todos los usuarios a menos que activen su propio panel.
- Editar el nombre de un panel.
- Edite un panel para agregar o eliminar pestañas y tarjetas. Puedes tener un mínimo de 1 y un máximo de 20 pestañas.
- Quitar un tablero.



Si tiene algún otro permiso además del acceso root, solo podrá configurar un panel activo.

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



Configurar paneles de control

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

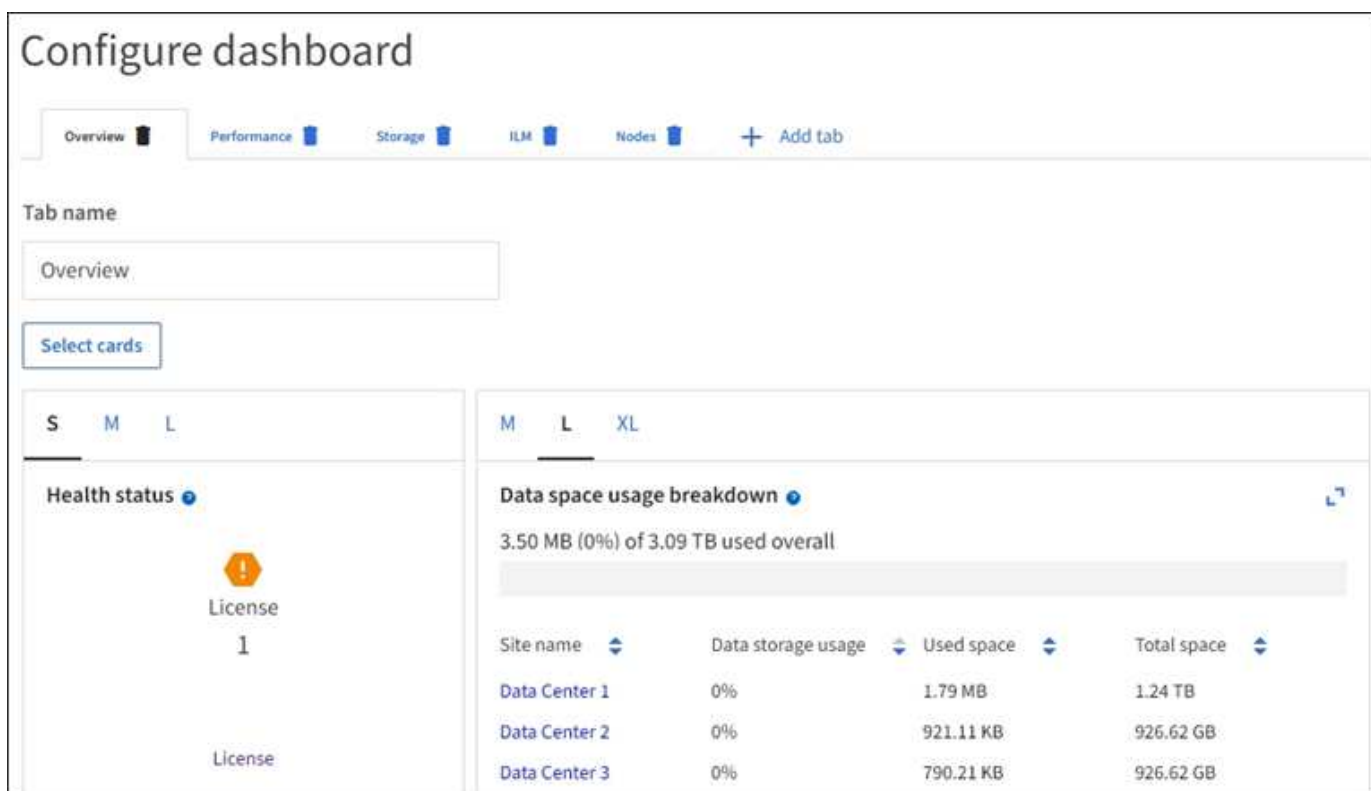
Para editar o clonar un panel existente, seleccione **Acciones > Administrar paneles**.



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

Al configurar un panel, puedes:

- Agregar o quitar pestañas
- Cambiar el nombre de las pestañas y asignarles nombres únicos a las nuevas pestañas
- Agregar, eliminar o reorganizar (arrastrar) tarjetas para cada pestaña
- Seleccione el tamaño de las tarjetas individuales seleccionando **S**, **M**, **L** o **XL** en la parte superior de la tarjeta.



Ver la página de Nodos

Ver la página de Nodos

Cuando necesite información más detallada sobre su sistema StorageGRID que la que

proporciona el panel, puede usar la página Nodos para ver las métricas de toda la red, cada sitio de la red y cada nodo de un sitio.

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



Cuando un nodo no está conectado a la red, como durante una actualización o en un estado desconectado, ciertas métricas podrían no estar disponibles o estar excluidas de los totales del sitio y de la red. Después de que un nodo se vuelva a conectar a la red, espere varios minutos para que los valores se estabilicen.



Para cambiar las unidades de los valores de almacenamiento que se muestran en el Administrador de cuadrícula, seleccione el menú desplegable de usuario en la parte superior derecha del Administrador de cuadrícula y luego seleccione **Preferencias de usuario**.



Las capturas de pantalla que se muestran son ejemplos. Los resultados pueden variar según la versión de StorageGRID .

Nodes

View the list and status of sites and grid nodes.

Total node count: 12

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

Iconos de estado de conexión

Si un nodo se desconecta de la red, aparecerá cualquiera de los siguientes íconos junto al nombre del nodo.

Icono	Descripción	Acción requerida
	No conectado - Desconocido Por una razón desconocida, un nodo se desconecta o los servicios en el nodo dejan de funcionar inesperadamente. Por ejemplo, es posible que se haya detenido un servicio en el nodo o que el nodo haya perdido su conexión a la red debido a un corte de energía o una interrupción inesperada. También podría activarse la alerta No se puede comunicar con el nodo. También podrían estar activas otras alertas.	Requiere atención inmediata. "Seleccione cada alerta" y siga las acciones recomendadas. Por ejemplo, es posible que necesite reiniciar un servicio que se ha detenido o reiniciar el host del nodo. Nota: Un nodo puede aparecer como Desconocido durante las operaciones de apagado administrado. Puedes ignorar el estado Desconocido en estos casos.
	No conectado - Administrativamente caído Por una razón esperada, el nodo no está conectado a la red. Por ejemplo, el nodo, o los servicios en el nodo, se han apagado correctamente, el nodo se está reiniciando o se está actualizando el software. También podrían estar activas una o más alertas. Dependiendo del problema subyacente, estos nodos a menudo vuelven a estar en línea sin ninguna intervención.	Determinar si hay alguna alerta que afecte a este nodo. Si una o más alertas están activas, "Seleccione cada alerta" y siga las acciones recomendadas.

Si un nodo está desconectado de la red, puede tener una alerta subyacente, pero solo aparece el ícono "No conectado". Para ver las alertas activas de un nodo, seleccione el nodo.

Iconos de alerta

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

 **Crítico:** Existe una condición anormal que ha detenido las operaciones normales de un nodo o servicio de StorageGRID. Debes abordar el problema subyacente inmediatamente. Si no se resuelve el problema podría producirse una interrupción del servicio y pérdida de datos.

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

 **Menor:** El sistema está funcionando normalmente, pero existe una condición anormal que podría afectar la capacidad del sistema para funcionar si continúa. Debes supervisar y resolver las alertas menores que no desaparecen por sí solas para garantizar que no provoquen un problema más grave.

Ver detalles de un sistema, sitio o nodo

Para filtrar la información que se muestra en la tabla Nodos, ingrese una cadena de búsqueda en el campo **Buscar**. Puede buscar por nombre del sistema, nombre para mostrar o tipo (por ejemplo, ingrese **gat** para localizar rápidamente todos los nodos de puerta de enlace).

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

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

Ver la pestaña Descripción general

La pestaña Descripción general proporciona información básica sobre cada nodo. También muestra cualquier alerta que afecte actualmente al nodo.

La pestaña Descripción general se muestra para todos los nodos.

Información del nodo

La sección Información del nodo de la pestaña Descripción general enumera información básica sobre el nodo.

NYC-ADM1 (Primary Admin Node)

Overview

Hardware

Network

Storage

Load balancer

Tasks

Node information

Display name:

NYC-ADM1

System name:

DC1-ADM1

Type:

Primary Admin Node

ID:

3adb1aa8-9c7a-4901-8074-47054aa06ae6

Connection state:

Connected

Software version:

11.7.0

IP addresses:

10.96.105.85 - eth0 (Grid Network)

Show additional IP addresses

La información general de un nodo incluye lo siguiente:

- **Nombre para mostrar** (se muestra solo si se ha cambiado el nombre del nodo): el nombre para mostrar actual del nodo. Utilice el "[Cambiar el nombre de la cuadrícula, los sitios y los nodos](#)" procedimiento para actualizar este valor.
- **Nombre del sistema**: el nombre que ingresó para el nodo durante la instalación. Los nombres del sistema se utilizan para operaciones internas de StorageGRID y no se pueden cambiar.
- **Tipo**: El tipo de nodo: nodo de administración, nodo de administración principal, nodo de almacenamiento o nodo de puerta de enlace.
- **ID**: El identificador único del nodo, también conocido como UUID.
- **Estado de conexión**: Uno de tres estados. Se muestra el icono del estado más grave.

- **Desconocido***  : Por alguna razón desconocida, el nodo no está conectado a la red o uno o más servicios están inactivos inesperadamente. Por ejemplo, se ha perdido la conexión de red entre los nodos, se ha cortado la energía o se ha caído un servicio. También podría activarse la alerta ***No se puede comunicar con el nodo**. También podrían estar activas otras alertas. Esta situación requiere atención inmediata.



Un nodo podría aparecer como Desconocido durante las operaciones de apagado administrado. Puedes ignorar el estado Desconocido en estos casos.

- ***Administrativamente caído***  : El nodo no está conectado a la red por una razón esperada. Por ejemplo, el nodo, o los servicios en el nodo, se han apagado correctamente, el nodo se está reiniciando o se está actualizando el software. También podrían estar activas una o más alertas.
- ***Conectado***  : El nodo está conectado a la red.

- **Almacenamiento utilizado**: Solo para nodos de almacenamiento.
 - **Datos de objeto**: el porcentaje del espacio total utilizable para datos de objeto que se ha utilizado en el nodo de almacenamiento.
 - **Metadatos del objeto**: el porcentaje del espacio total permitido para los metadatos del objeto que se ha utilizado en el nodo de almacenamiento.
- **Versión de software**: la versión de StorageGRID que está instalada en el nodo.
- **Grupos HA**: solo para nodos de administración y nodos de puerta de enlace. Se muestra si una interfaz de red en el nodo está incluida 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 del nodo y las asignaciones de interfaz.

Alertas

La sección Alertas de la pestaña Descripción general enumera todas las "[alertas que actualmente afectan a este nodo y que no han sido silenciadas](#)". Seleccione el nombre de la alerta para ver detalles adicionales y acciones recomendadas.

Alerts			
Alert name	Severity	Time triggered	Current values
Low installed node memory The amount of installed memory on a node is low.	✖ Critical	11 hours ago	Total RAM size: 8.37 GB

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

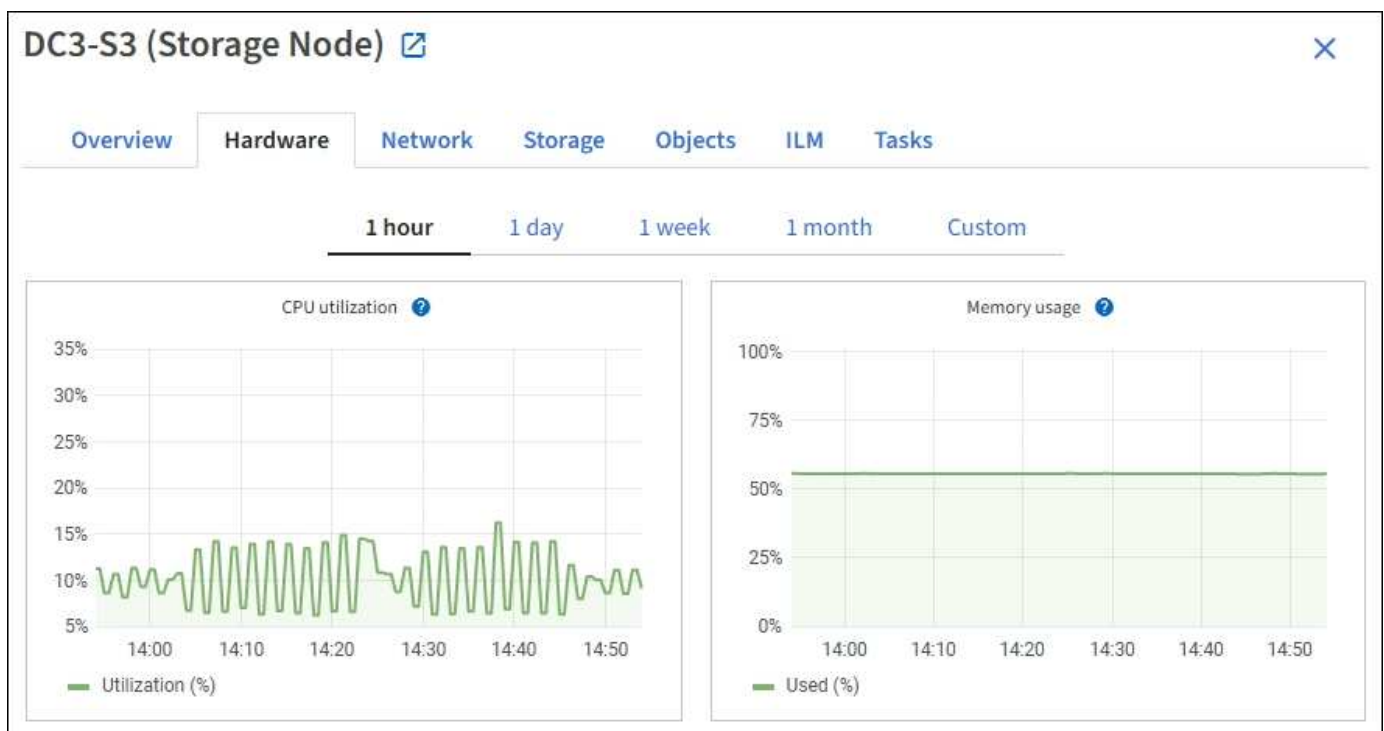
Ver la pestaña Hardware

La pestaña Hardware muestra la utilización de la CPU y la utilización de la memoria para cada nodo, e información de hardware adicional sobre los dispositivos.



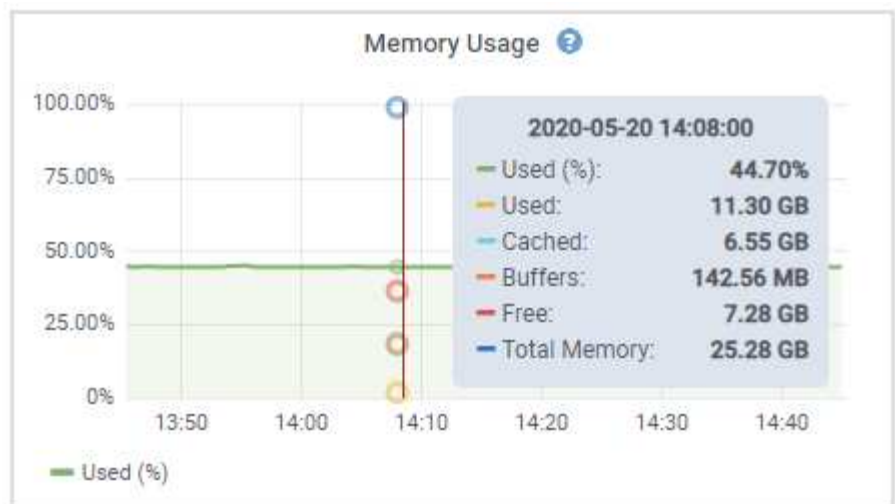
El Grid Manager se actualiza con cada versión y es posible que no coincida con las capturas de pantalla de ejemplo en esta página.

La pestaña Hardware se muestra para todos los nodos.



Para mostrar un intervalo de tiempo diferente, seleccione uno de los controles sobre el gráfico. Puede mostrar 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 rangos de fecha y hora.

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



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

Ver información sobre los nodos de almacenamiento del dispositivo

La página Nodos enumera información sobre el estado del servicio y todos los recursos computacionales, de dispositivos de disco y de red para cada nodo de almacenamiento del dispositivo. También puede ver la memoria, el hardware de almacenamiento, la versión del firmware del controlador, los recursos de red, las interfaces de red, las direcciones de red y recibir y transmitir datos.

Pasos

1. Desde la página Nodos, seleccione un nodo de almacenamiento del dispositivo.
2. Seleccione **Descripción general**.

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

- **eth**: La red de cuadrícula, la red de administración o la red de clientes.
- **hic**: Uno de los puertos físicos de 10, 25 o 100 GbE en el dispositivo. Estos puertos se pueden unir y conectar a la red de cuadrícula StorageGRID (eth0) y a la red de cliente (eth2).
- **mtc**: Uno de los puertos físicos de 1 GbE en el dispositivo. Una o más interfaces mtc están vinculadas para formar la interfaz de red de administración de StorageGRID (eth1). Puede dejar otras interfaces mtc disponibles para conectividad local temporal para un técnico en el centro de datos.

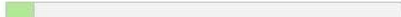
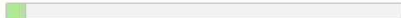
[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state:  **Connected**

Storage used:
Object data  7% [?](#)
Object metadata  5% [?](#)

Software version: 11.6.0 (build 20210915.1941.afce2d9)

IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

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

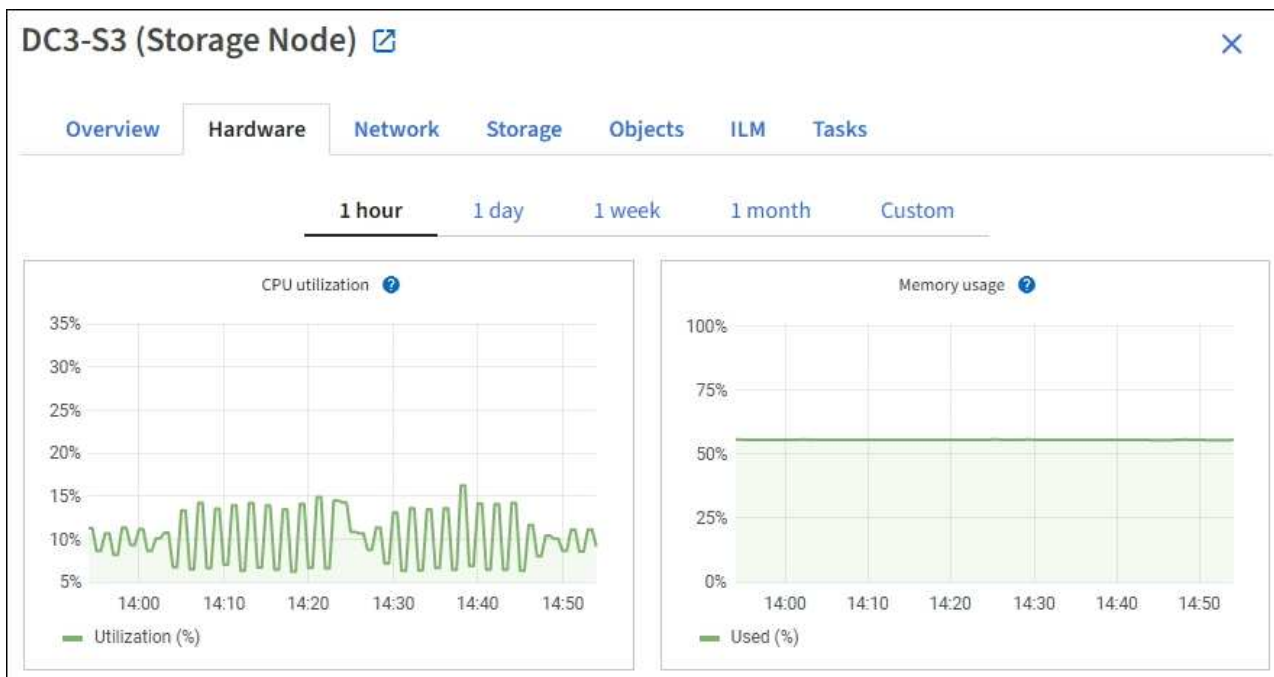
Alerts

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

La sección Alertas de la pestaña Descripción general muestra todas las alertas activas para el nodo.

3. Seleccione **Hardware** para ver más información sobre el dispositivo.

- Vea 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 sobre el gráfico. Puede mostrar 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 rangos de fecha y hora.



- b. Desplácese hacia abajo para ver la tabla de componentes del dispositivo. Esta tabla contiene información como el nombre del modelo del dispositivo, los nombres de los controladores, los números de serie y las direcciones IP, y el estado de cada componente.



Algunos campos, como la dirección IP del controlador de cómputo BMC y el hardware de cómputo, aparecen solo para dispositivos con esa función.

Los componentes de los estantes de almacenamiento y los estantes de expansión, si son parte de la instalación, aparecen en una tabla separada debajo de la tabla de electrodomésticos.

StorageGRID Appliance

Appliance model:	SG6060	
Storage controller name:	StorageGRID-Lab79-SG6060-7-134	
Storage controller A management IP:	10.2	
Storage controller B management IP:	10.2	
Storage controller WWID:	6d039ea0000173e50000000065b7b761	
Storage appliance chassis serial number:	721924500068	
Storage controller firmware version:	08.53.00.09	
Storage controller SANtricity OS version:	11.50.3R2	
Storage controller NVRAM version:	N280X-853834-DG1	
Storage hardware:	Nominal	
Storage controller failed drive count:	0	
Storage controller A:	Nominal	
Storage controller B:	Nominal	
Storage controller power supply A:	Nominal	
Storage controller power supply B:	Nominal	
Storage data drive type:	NL-SAS HDD	
Storage data drive size:	4.00 TB	
Storage RAID mode:	DDP16	
Storage connectivity:	Nominal	
Overall power supply:	Degraded	
Compute controller BMC IP:	10.2	
Compute controller serial number:	721917500060	
Compute hardware:	Needs Attention	
Compute controller CPU temperature:	Nominal	
Compute controller chassis temperature:	Nominal	
Compute controller power supply A:	Failed	
Compute controller power supply B:	Nominal	

Storage shelves

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

Campo en la tabla de dispositivos	Descripción
Modelo de electrodoméstico	El número de modelo de este dispositivo StorageGRID que se muestra en SANtricity OS.
Nombre del controlador de almacenamiento	El nombre de este dispositivo StorageGRID que se muestra en SANtricity OS.
Controlador de almacenamiento Una IP de gestión	Dirección IP para el puerto de administración 1 en el controlador de almacenamiento A. Utilice esta IP para acceder a SANtricity OS para solucionar problemas de almacenamiento.

Campo en la tabla de dispositivos	Descripción
IP de gestión del controlador de almacenamiento B	Dirección IP para el puerto de administración 1 en el controlador de almacenamiento B. Utilice esta IP para acceder a SANtricity OS para solucionar problemas de almacenamiento. Algunos modelos de electrodomésticos no tienen un controlador de almacenamiento B.
WWID del controlador de almacenamiento	El identificador mundial del controlador de almacenamiento que se muestra en SANtricity OS.
Número de serie del chasis del dispositivo de almacenamiento	El número de serie del chasis del aparato.
Versión del firmware del controlador de almacenamiento	La versión del firmware del controlador de almacenamiento para este dispositivo.
Controlador de almacenamiento SANtricity Versión del sistema operativo	La versión del sistema operativo SANtricity del controlador de almacenamiento A.
Versión NVSRAM del controlador de almacenamiento	Versión NVSRAM del controlador de almacenamiento según lo informado por SANtricity System Manager. Para SG6060 y SG6160, si hay una discrepancia en la versión de NVSRAM entre los dos controladores, se muestra la versión del controlador A. Si el controlador A no está instalado o no está operativo, se muestra la versión del controlador B.
Hardware de almacenamiento	El estado general del hardware del controlador de almacenamiento. Si SANtricity System Manager informa un estado de Necesita atención para el hardware de almacenamiento, el sistema StorageGRID también informa este valor. Si el estado es "requiere atención", primero verifique el controlador de almacenamiento usando SANtricity OS. Luego, asegúrese de que no existan otras alertas que se apliquen al controlador de cómputo.
Recuento de unidades fallidas del controlador de almacenamiento	La cantidad de unidades que no son óptimas.
Controlador de almacenamiento A	El estado del controlador de almacenamiento A.
Controlador de almacenamiento B	El estado del controlador de almacenamiento B. Algunos modelos de dispositivos no tienen un controlador de almacenamiento B.
Fuente de alimentación del controlador de almacenamiento A	El estado de la fuente de alimentación A para el controlador de almacenamiento.

Campo en la tabla de dispositivos	Descripción
Fuente de alimentación del controlador de almacenamiento B	El estado de la fuente de alimentación B para el controlador de almacenamiento.
Tipo de unidad de datos de almacenamiento	El tipo de unidades en el dispositivo, como HDD (disco duro) o SSD (unidad de estado sólido).
Tamaño de la unidad de datos de almacenamiento	El tamaño efectivo de una unidad de datos. En el caso del SG6160, también se muestra el tamaño de la unidad de caché. Nota: Para nodos con estantes de expansión, utilice el Tamaño de la unidad de datos para cada estante en cambio. El tamaño efectivo de la unidad puede variar según el estante.
Modo RAID de almacenamiento	El modo RAID configurado para el dispositivo.
Conectividad de almacenamiento	El estado de conectividad de almacenamiento.
Fuente de alimentación general	El estado de todas las fuentes de alimentación del aparato.
Controlador de cómputo BMC IP	La dirección IP del puerto del controlador de administración de placa base (BMC) en el controlador de cómputo. Utilice esta IP para conectarse a la interfaz BMC para supervisar y diagnosticar el hardware del dispositivo. Este campo no se muestra para los modelos de dispositivos que no contienen un BMC.
Número de serie del controlador de cómputo	El número de serie del controlador de cálculo.
hardware de cómputo	El estado del hardware del controlador de cómputo. Este campo no se muestra para los modelos de dispositivos que no tienen hardware de procesamiento y hardware de almacenamiento separados.
Temperatura de la CPU del controlador de cómputo	El estado de temperatura de la CPU del controlador de cómputo.
Temperatura del chasis del controlador de cómputo	El estado de temperatura del controlador de cálculo.

+

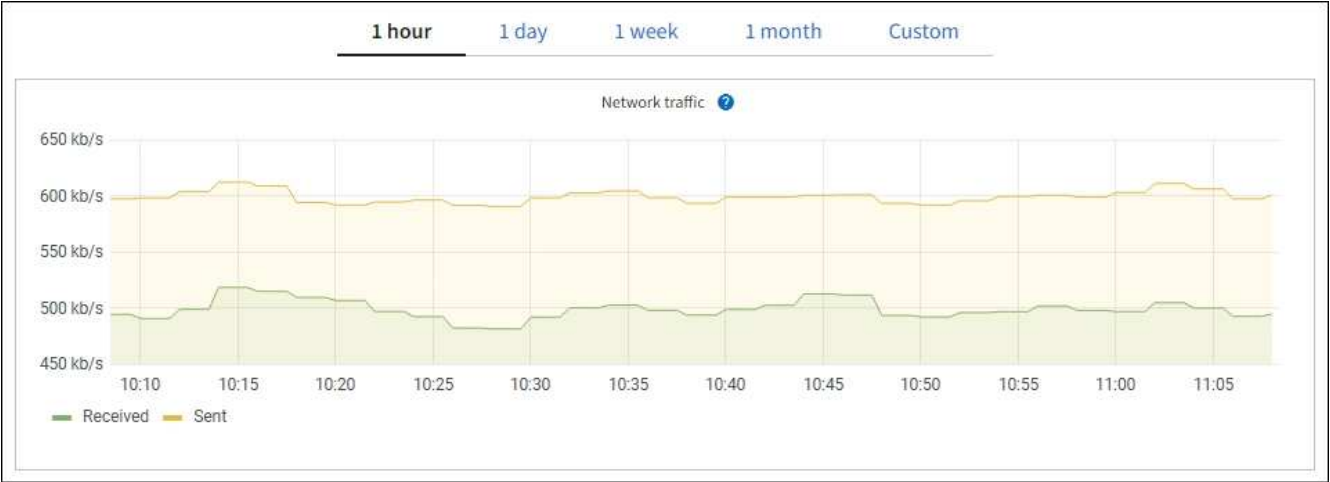
Columna en la tabla Estantes de almacenamiento	Descripción
Número de serie del chasis del estante	El número de serie del chasis del estante de almacenamiento.
Identificación del estante	El identificador numérico del estante de almacenamiento. • 99: Estante del controlador de almacenamiento • 0: Primer estante de expansión • 1: Segundo estante de expansión Nota: Los estantes de expansión se aplican únicamente a los modelos SG6060 y SG6160.
Estado del estante	El estado general del estante de almacenamiento.
Estado de la OIM	El estado de los módulos de entrada/salida (IOM) en cualquier estante de expansión. N/A si no se trata de un estante de expansión.
Estado de la fuente de alimentación	El estado general de las fuentes de alimentación del estante de almacenamiento.
Estado del cajón	El estado de los cajones en el estante de almacenamiento. N/A si el estante no contiene cajones.
Estado del ventilador	El estado general de los ventiladores de refrigeración en el estante de almacenamiento.
Ranuras de unidad	El número total de ranuras de unidad en el estante de almacenamiento.
Unidades de datos	La cantidad de unidades en el estante de almacenamiento que se utilizan para el almacenamiento de datos.
Tamaño de la unidad de datos	El tamaño efectivo de una unidad de datos en el estante de almacenamiento.
Unidades de caché	La cantidad de unidades en el estante de almacenamiento que se utilizan como caché.
Tamaño de la unidad de caché	El tamaño de la unidad de caché más pequeña en el estante de almacenamiento. Normalmente, las unidades de caché tienen todas el mismo tamaño.
Estado de configuración	El estado de configuración del estante de almacenamiento.

a. Confirme que todos los estados sean "Nominal".

Si un estado no es "Nominal", revise las alertas actuales. También puede utilizar SANtricity System Manager para obtener más información sobre algunos de estos valores de hardware. Consulte las instrucciones de instalación y mantenimiento de su aparato.

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

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



a. Revise la sección Interfaces de red.

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** en la tabla Interfaces de red para determinar si los puertos de red 10/25-GbE en el dispositivo se configuraron para usar el modo activo/de respaldo o el modo LACP.



Los valores que se muestran en la tabla suponen que se utilizan los cuatro enlaces.

Modo de enlace	Modo de enlace	Velocidad de enlace HIC individual (hic1, hic2, hic3, hic4)	Velocidad esperada de la red de cuadrícula/cliente (eth0,eth2)
Agregar	LACP	25	100
Fijado	LACP	25	50
Fijado	Activo/Copia de seguridad	25	25
Agregar	LACP	10	40

Modo de enlace	Modo de enlace	Velocidad de enlace HIC individual (hic1, hic2, hic3, hic4)	Velocidad esperada de la red de cuadrícula/cliente (eth0,eth2)
Fijado	LACP	10	20
Fijado	Activo/Copia de seguridad	10	10

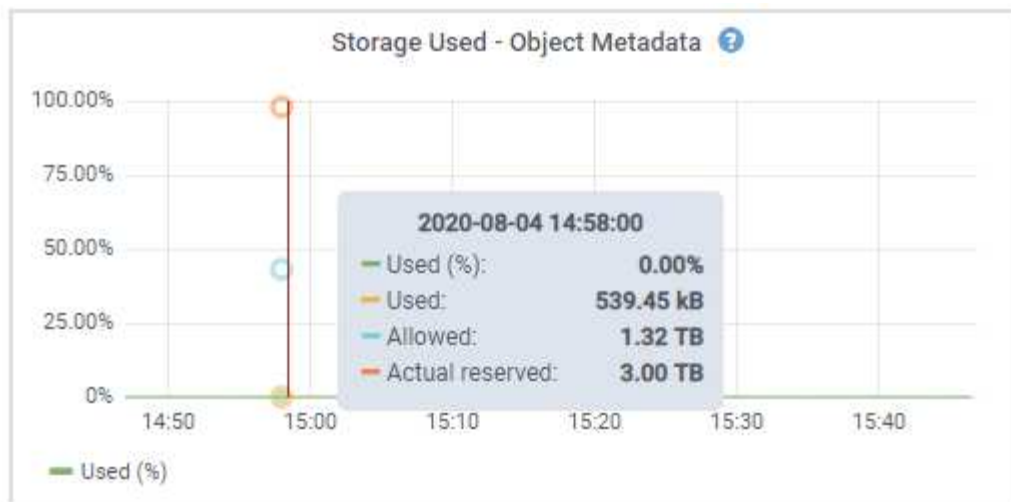
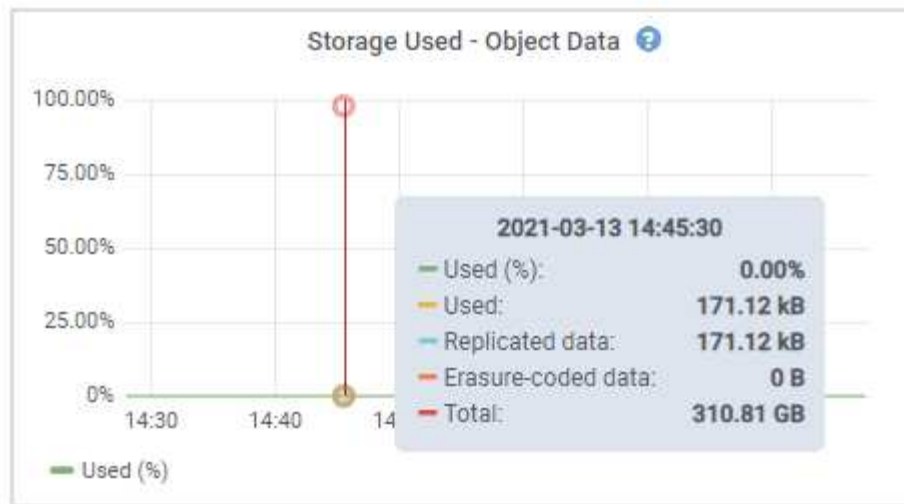
Ver "[Configurar enlaces de red](#)" para obtener más información sobre la configuración de los puertos 10/25-GbE.

- b. Revise la sección Comunicación en red.

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

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

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



- a. Desplácese hacia abajo para ver las cantidades de almacenamiento disponible para cada volumen y almacén de objetos.

El nombre mundial de cada disco coincide con el identificador mundial de volumen (WWID) que aparece cuando se ven las propiedades de volumen estándar en SANtricity OS (el software de administración conectado al controlador de almacenamiento del dispositivo).

Para ayudarlo a interpretar las estadísticas de lectura y escritura del disco relacionadas con los puntos de montaje del volumen, la primera parte del nombre que se muestra 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 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

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

La página Nodos enumera información sobre el estado del servicio y todos los recursos computacionales, de dispositivos 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 la memoria, el hardware de almacenamiento, los recursos de red, las interfaces de red, las direcciones de red y recibir y transmitir datos.

Pasos

1. Desde la página Nodos, seleccione un nodo de administración del dispositivo o un nodo de puerta de enlace del dispositivo.
2. Seleccione **Descripción general**.

La sección Información del nodo de la pestaña Descripción general muestra información resumida del

nodo, como el nombre, el tipo, el ID y el estado de la conexión del nodo. La lista de direcciones IP incluye el nombre de la interfaz para cada dirección, de la siguiente manera:

- **adllb** y **adlli**: se muestran si se utiliza el enlace activo/de respaldo para la interfaz de red de administración
- **eth**: La red de cuadrícula, la red de administración o la red de clientes.
- **hic**: Uno de los puertos físicos de 10, 25 o 100 GbE en el dispositivo. Estos puertos se pueden unir y conectar a la red de cuadrícula StorageGRID (eth0) y a la red de cliente (eth2).
- **mtc**: Uno de los puertos físicos de 1 GbE en el dispositivo. Una o más interfaces mtc están vinculadas para formar la interfaz de red de administración (eth1). Puede dejar otras interfaces mtc disponibles para conectividad local temporal para un técnico en el centro de datos.

10-224-6-199-ADM1 (Primary Admin Node)

Overview

Hardware

Network

Storage

Load balancer

Tasks

SANtricity System Manager

Node information

Name:

10-224-6-199-ADM1

Type:

Primary Admin Node

ID:

6fdc1890-ca0a-4493-acdd-72ed317d95fb

Connection state:

Connected

Software version:

11.6.0 (build 20210928.1321.6687ee3)

IP addresses:

172.16.6.199 - eth0 (Grid Network)

10.224.6.199 - eth1 (Admin Network)

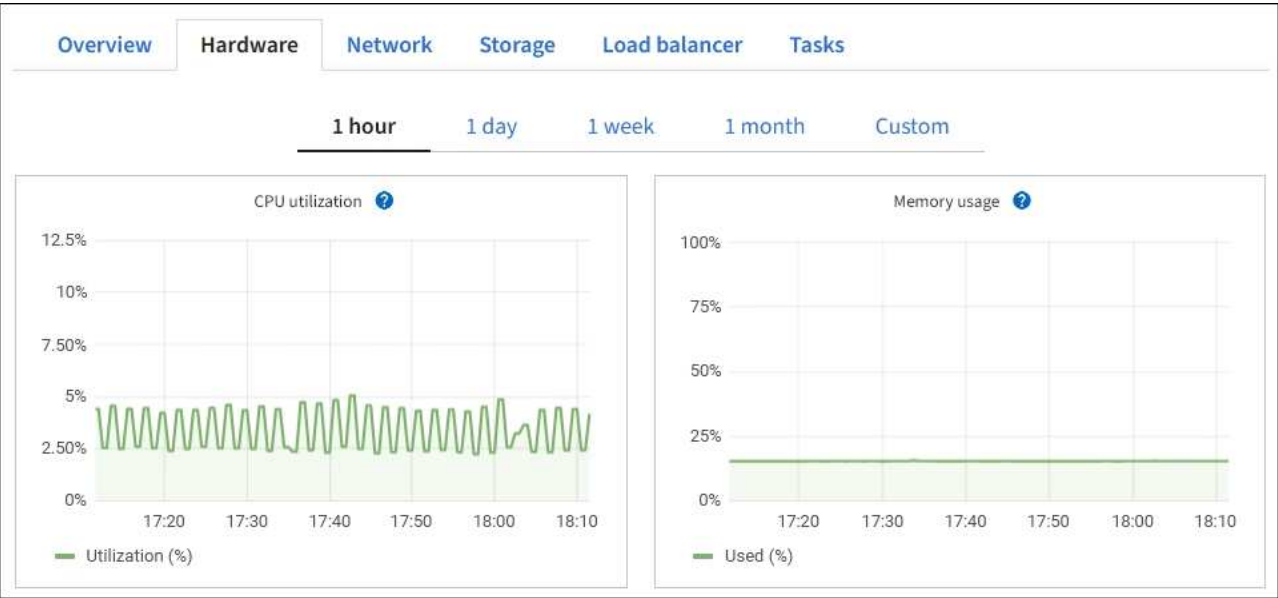
47.47.7.241 - eth2 (Client Network)

Hide additional IP addresses

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

La sección Alertas de la pestaña Descripción general muestra todas las alertas activas para el nodo.

3. Seleccione **Hardware** para ver más información sobre el dispositivo.
- a. Vea 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 sobre el gráfico. Puede mostrar 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 rangos de fecha y hora.



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

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

Campo en la tabla de dispositivos	Descripción
Modelo de electrodoméstico	El número de modelo de este dispositivo StorageGRID .

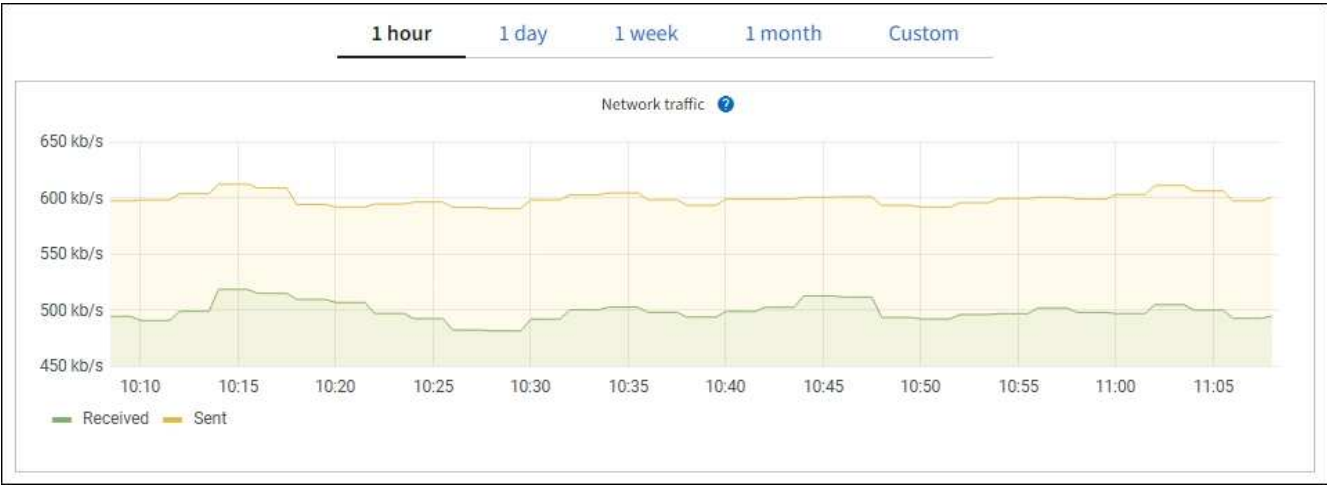
Campo en la tabla de dispositivos	Descripción
Recuento de unidades fallidas del controlador de almacenamiento	La cantidad de unidades que no son óptimas.
Tipo de unidad de datos de almacenamiento	El tipo de unidades en el dispositivo, como HDD (disco duro) o SSD (unidad de estado sólido).
Tamaño de la unidad de datos de almacenamiento	El tamaño efectivo de una unidad de datos.
Modo RAID de almacenamiento	El modo RAID del dispositivo.
Fuente de alimentación general	El estado de todas las fuentes de alimentación del aparato.
Controlador de cómputo BMC IP	La dirección IP del puerto del controlador de administración de placa base (BMC) en el controlador de cómputo. Puede utilizar esta IP para conectarse a la interfaz BMC para supervisar y diagnosticar el hardware del dispositivo. Este campo no se muestra para los modelos de dispositivos que no contienen un BMC.
Número de serie del controlador de cómputo	El número de serie del controlador de cálculo.
hardware de cómputo	El estado del hardware del controlador de cómputo.
Temperatura de la CPU del controlador de cómputo	El estado de temperatura de la CPU del controlador de cómputo.
Temperatura del chasis del controlador de cómputo	El estado de temperatura del controlador de cálculo.

a. Confirme que todos los estados sean "Nominal".

Si un estado no es "Nominal", revise las alertas actuales.

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

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



a. Revise la sección Interfaces de red.

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** en la tabla Interfaces de red para determinar si los cuatro puertos de red 40/100-GbE en el dispositivo se configuraron para usar el modo activo/de respaldo o el modo LACP.



Los valores que se muestran en la tabla suponen que se utilizan los cuatro enlaces.

Modo de enlace	Modo de enlace	Velocidad de enlace HIC individual (hic1, hic2, hic3, hic4)	Velocidad esperada de la red de cuadrícula/cliente (eth0, eth2)
Agregar	LACP	100	400
Fijado	LACP	100	200
Fijado	Activo/Copia de seguridad	100	100
Agregar	LACP	40	160
Fijado	LACP	40	80
Fijado	Activo/Copia de seguridad	40	40

b. Revise la sección Comunicación en 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 volúmenes en el dispositivo de servicios.

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

Ver la pestaña Red

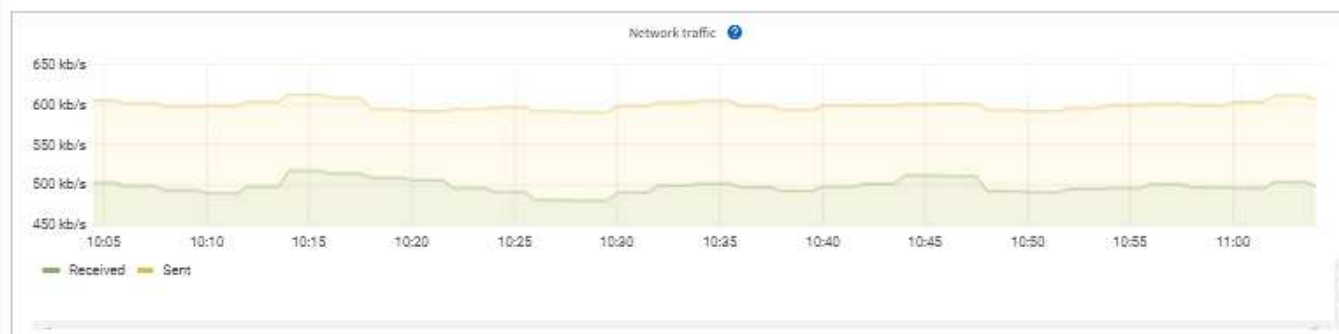
La pestaña Red muestra un gráfico que muestra el tráfico de red recibido y enviado a través de todas las interfaces de red en el nodo, sitio o red.

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

Para mostrar un intervalo de tiempo diferente, seleccione uno de los controles sobre el gráfico. Puede mostrar 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 rangos de fecha y hora.

Para los nodos, la tabla de interfaces de red proporciona información sobre los puertos de red físicos de cada nodo. La tabla de comunicaciones de red proporciona detalles sobre las operaciones de recepción y transmisión de cada nodo y cualquier contador de fallas informadas por el controlador.

DC1-S2 (Storage Node)

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

Network interfaces

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

Network communication

Receive

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

Transmit

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

Información relacionada

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

Ver la pestaña Almacenamiento

La pestaña Almacenamiento resume la disponibilidad de almacenamiento y otras métricas de almacenamiento.

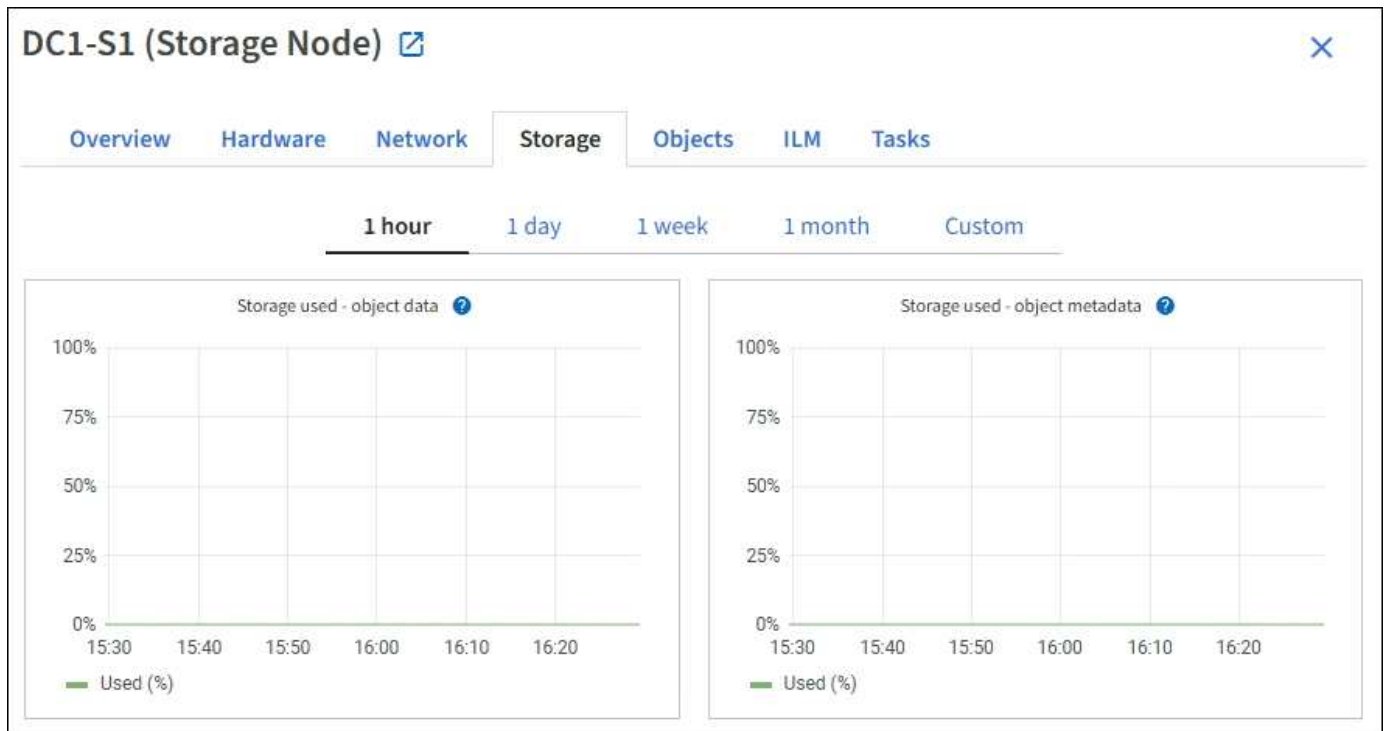
La pestaña Almacenamiento se muestra para todos los nodos, cada sitio y toda la cuadrícula.

Gráficos utilizados en almacenamiento

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



Cuando un nodo no está conectado a la red, como durante una actualización o en un estado desconectado, ciertas métricas podrían no estar disponibles o estar excluidas de los totales del sitio y de la red. Después de que un nodo se vuelva a conectar a la red, espere varios minutos para que los valores se estabilicen.



Tablas de dispositivos de disco, volúmenes y almacenes de objetos

Para todos los nodos, la pestaña Almacenamiento contiene detalles de los dispositivos de disco y volúmenes del nodo. Para los nodos de almacenamiento, la tabla Almacenes de objetos 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

["Supervisar la capacidad de almacenamiento"](#)

Ver la pestaña Objetos

La pestaña Objetos proporciona información sobre ["Tasas de ingesta y recuperación de S3"](#).

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

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

Object counts

Total objects: ? 1,295

Lost objects: ? 0

S3 buckets and Swift containers: ? 161

Metadata store queries

Average latency: ? 10.00 milliseconds

Queries - successful: ? 14,587

Queries - failed (timed out): ? 0

Queries - failed (consistency level unmet): ? 0

Verification

Status: ? No errors

Percent complete: ? 47.14%

Average stat time: ? 0.00 microseconds

Objects verified: ? 0

Object verification rate: ? 0.00 objects / second

Data verified: ? 0 bytes

Data verification rate: ? 0.00 bytes / second

Missing objects: ? 0

Corrupt objects: ? 0

Corrupt objects unidentified: ? 0

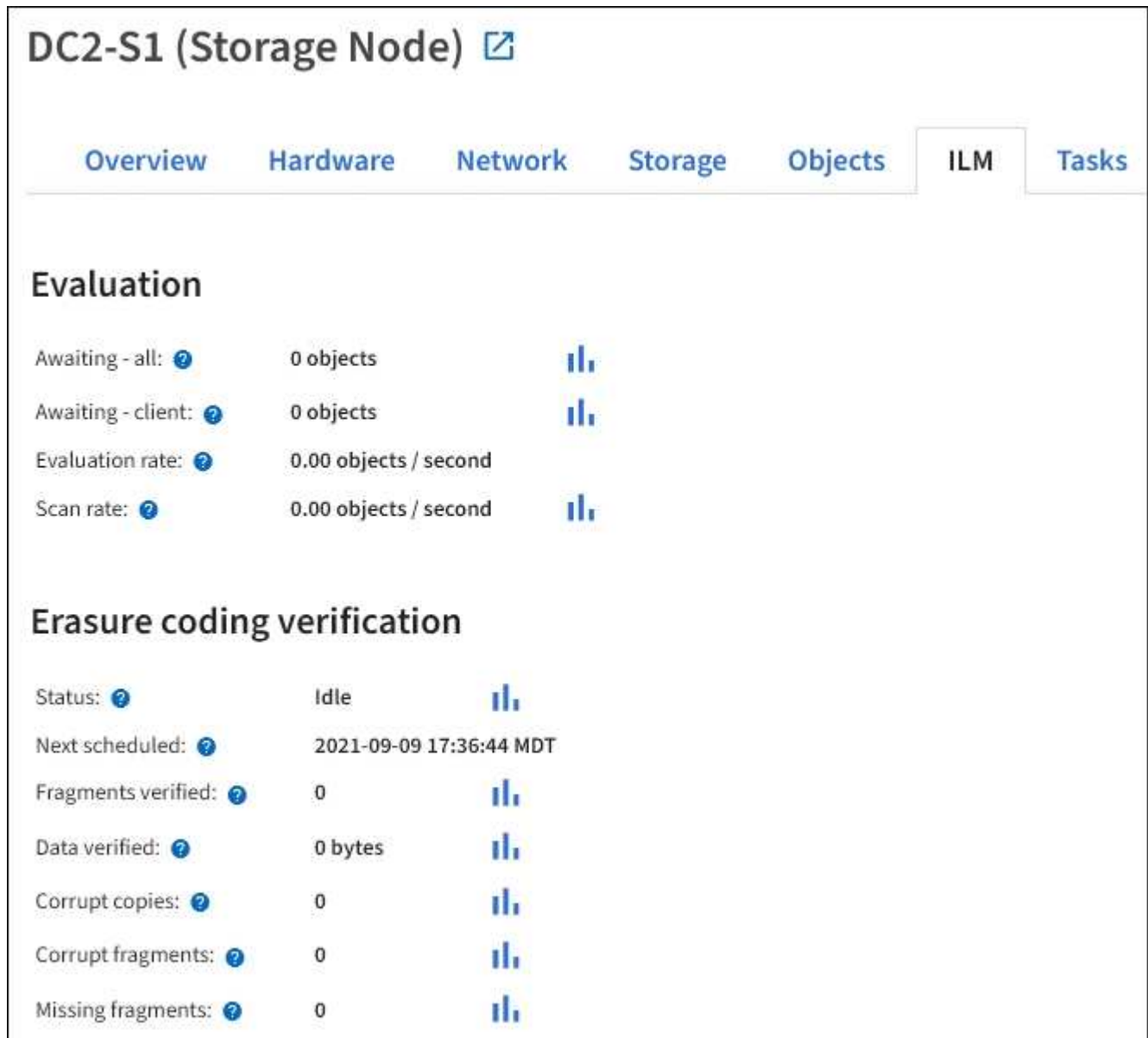
Quarantined objects: ? 0

Ver la pestaña ILM

La pestaña ILM proporciona información sobre 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 red. Para cada sitio y la cuadrícula, la pestaña ILM muestra un gráfico de la cola de ILM a lo largo del tiempo. Para la cuadrícula, esta pestaña también proporciona el tiempo estimado para completar un escaneo ILM completo de todos los objetos.

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



Información relacionada

- ["Supervisar la gestión del ciclo de vida de la información"](#)
- ["Administrar StorageGRID"](#)

Utilice la pestaña Tareas

La pestaña Tareas se muestra para todos los nodos. Puede utilizar esta pestaña para cambiar el nombre o reiniciar un nodo o para poner un nodo del dispositivo en modo de mantenimiento.

Para conocer los requisitos completos y las instrucciones para cada opción en esta pestaña, consulte lo siguiente:

- ["Cambiar el nombre de la cuadrícula, los sitios y los nodos"](#)
- ["Reiniciar el nodo de la red"](#)
- ["Coloque el aparato en modo de mantenimiento"](#)

Ver la pestaña Balanceador de carga

La pestaña Load Balancer incluye gráficos de rendimiento y diagnóstico relacionados con el funcionamiento del servicio Load Balancer.

La pestaña Balanceador de carga se muestra para los nodos de administración y los nodos de puerta de enlace, cada sitio y toda la red. Para cada sitio, la pestaña Balanceador de carga proporciona un resumen agregado de las estadísticas de todos los nodos de ese sitio. Para toda la cuadrícula, la pestaña Balanceador de carga proporciona un resumen agregado de las estadísticas de todos los sitios.

Si no se ejecuta ninguna operación de E/S a través del servicio Load Balancer, o no hay ningún balanceador de carga configurado, los gráficos muestran "No hay datos".



Solicitar tráfico

Este gráfico proporciona un promedio móvil de 3 minutos del rendimiento de los datos transmitidos entre los puntos finales del balanceador 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 en tasas de solicitud bajas o para solicitudes de duración muy larga. Puede consultar la pestaña Red para obtener una visión más realista del comportamiento actual de la red.

Tasa de solicitudes entrantes

Este gráfico proporciona un promedio móvil de 3 minutos de la cantidad 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 promedio de la solicitud (sin errores)

Este gráfico proporciona un promedio móvil de 3 minutos de duraciones de solicitudes, desglosado por tipo de solicitud (GET, PUT, HEAD y DELETE). La duración de cada solicitud comienza cuando el servicio Load Balancer analiza un encabezado 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 de la cantidad de respuestas de error devueltas a los clientes por segundo, desglosado por el código de respuesta de error.

Información relacionada

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

Ver la pestaña de servicios de la plataforma

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

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

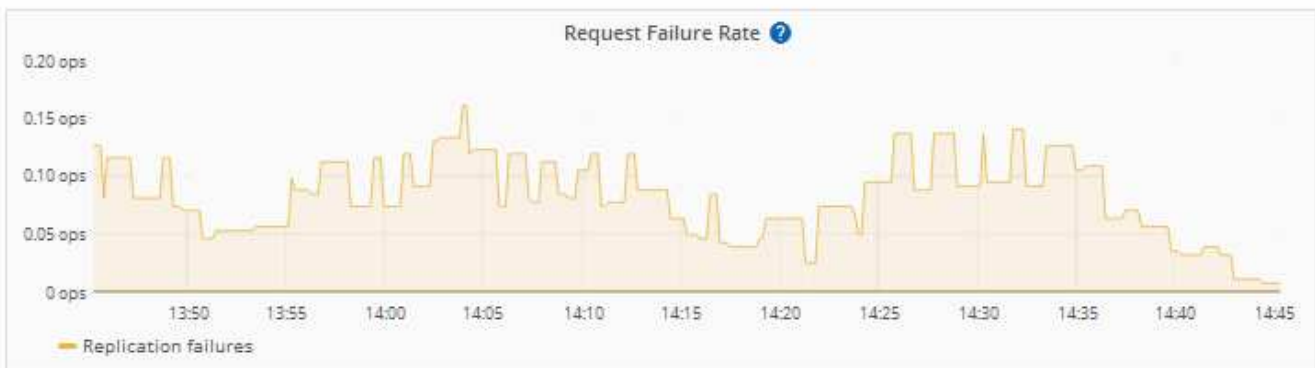
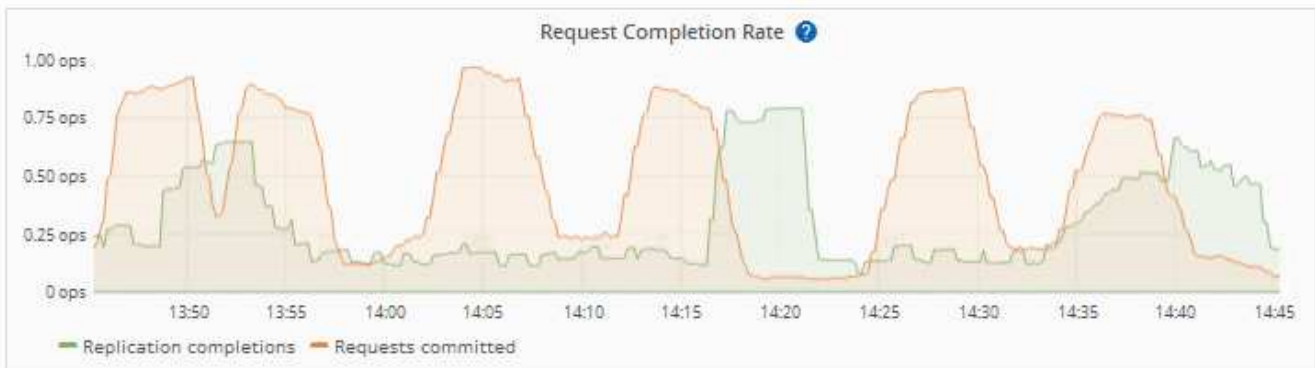
1 hour

1 day

1 week

1 month

Custom



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

Ver la pestaña Administrar unidades

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

Usando la pestaña Administrar unidades, puede hacer lo siguiente:

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

Para acceder a la pestaña Administrar unidades, debe tener la ["Administrador del dispositivo de almacenamiento o permiso de acceso raíz"](#) .

Para obtener información sobre el uso de la pestaña Administrar unidades, consulte ["Utilice la pestaña Administrar unidades"](#) .

Ver la pestaña SANtricity System Manager (solo serie E)

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



El acceso a SANtricity System Manager desde Grid Manager generalmente está destinado únicamente a monitorear el hardware del dispositivo y configurar E-Series AutoSupport. Muchas funciones y operaciones dentro de SANtricity System Manager, como la actualización de firmware, no se aplican al monitoreo de su dispositivo StorageGRID . Para evitar problemas, siga siempre las instrucciones de mantenimiento de hardware de su dispositivo. Para actualizar el firmware de SANtricity , consulte la ["Procedimientos de configuración de mantenimiento"](#) para su dispositivo de almacenamiento.



La pestaña Administrador del sistema SANtricity se muestra solo para los nodos de dispositivos de almacenamiento que utilizan hardware de la serie E.

Con SANtricity System Manager, puede hacer lo siguiente:

- Vea datos de rendimiento, como el rendimiento a nivel de matriz de almacenamiento, la latencia de E/S, la utilización de la CPU del controlador de almacenamiento y el rendimiento.
- Verifique el estado del componente de hardware.
- Realizar funciones de soporte, incluida la visualización de datos de diagnóstico y la configuración de E-Series AutoSupport.



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

Para acceder a SANtricity System Manager a través de Grid Manager, debe tener la ["Administrador del dispositivo de almacenamiento o permiso de acceso raíz"](#) .



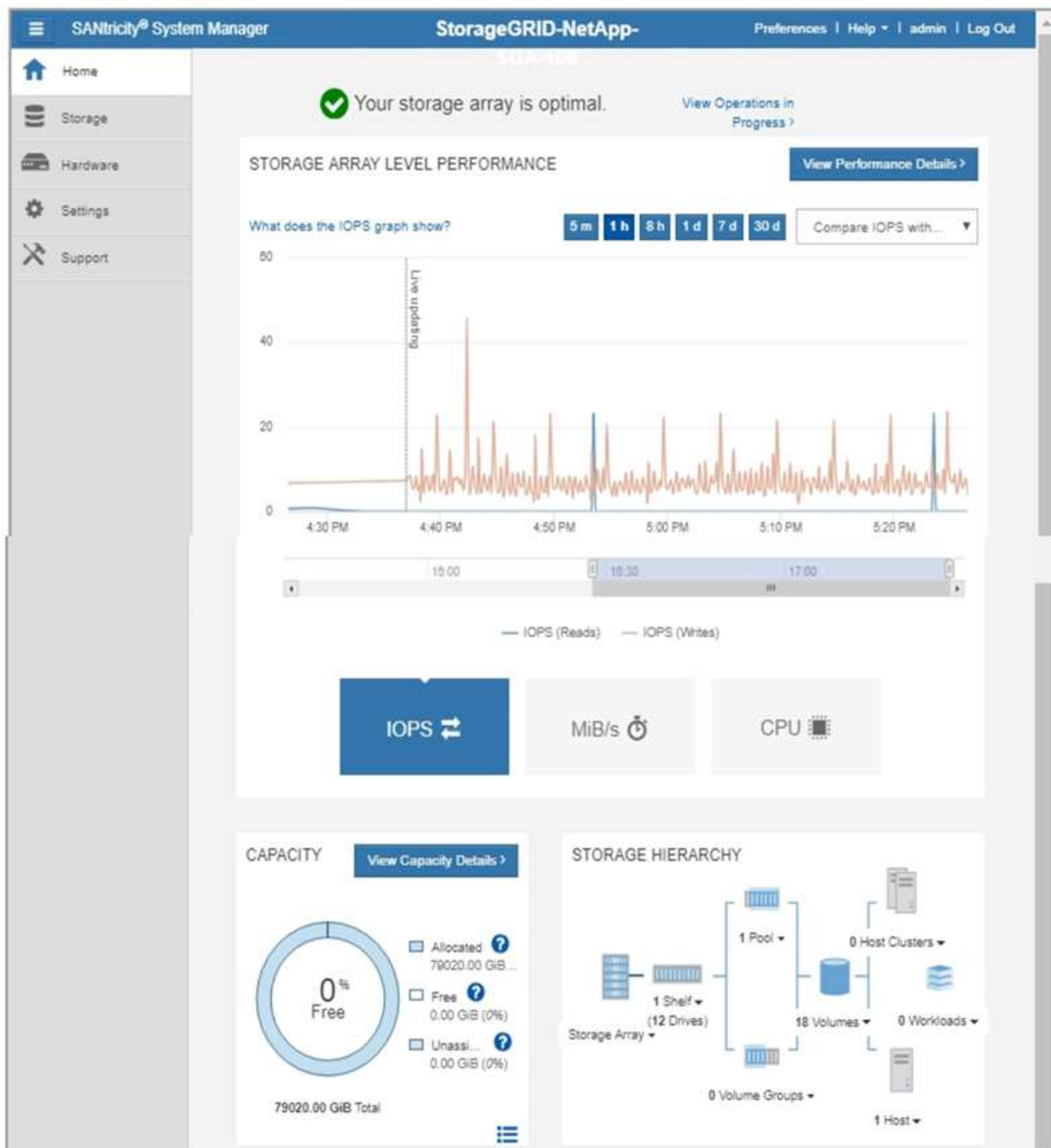
Debe tener el firmware SANtricity 8.70 o superior para acceder a SANtricity System Manager mediante Grid Manager.

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

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

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

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



Puede utilizar el enlace SANtricity System Manager para abrir SANtricity System Manager en una nueva ventana del navegador para una visualización más sencilla.

Para ver detalles sobre el rendimiento a nivel de matriz de almacenamiento y el uso de la capacidad, coloque

el cursor sobre cada gráfico.

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

Información a monitorear regularmente

Qué y cuándo monitorear

Si bien el sistema StorageGRID puede seguir funcionando cuando ocurren errores o partes de la red no están disponibles, debe monitorear y abordar los posibles problemas antes de que afecten la eficiencia o disponibilidad de la red.

Antes de empezar

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

Acerca de las tareas de monitoreo

Un sistema ocupado genera grandes cantidades de información. La siguiente lista ofrece orientación sobre la información más importante que se debe monitorear de manera continua.

Qué monitorear	Frecuencia
"Estado de salud del sistema"	Diario
Tasa a la que "Capacidad de objetos y metadatos del nodo de almacenamiento" se está consumiendo	Semanalmente
"Operaciones de gestión del ciclo de vida de la información"	Semanalmente
"Recursos de redes y sistemas"	Semanalmente
"Actividad de los inquilinos"	Semanalmente
"Operaciones del cliente S3"	Semanalmente
"Operaciones de equilibrio de carga"	Después de la configuración inicial y después de cualquier cambio de configuración
"Conexiones de federación de red"	Semanalmente

Monitorear la salud del sistema

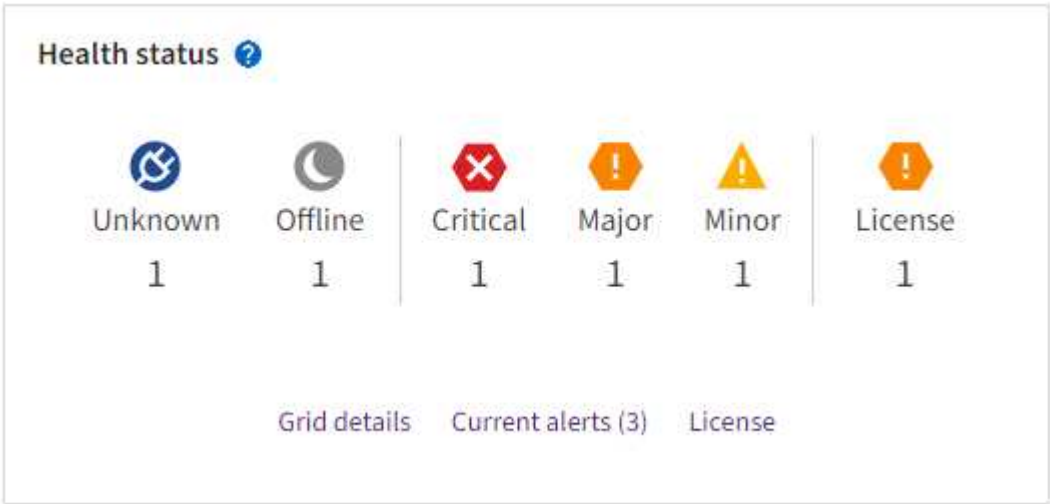
Supervise el estado general de su sistema StorageGRID diariamente.

Acerca de esta tarea

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

sistema. Investigar los problemas resumidos en la tarjeta de estado de salud del panel de control de Grid Manager.

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



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

Enlace	Aparece cuando...
Detalles de la cuadrícula	Todos los nodos están desconectados (estado de conexión desconocido o administrativamente inactivo).
Alertas actuales (críticas, graves, leves)	Las alertas son actualmente activo .
Alertas resueltas recientemente	Alertas activadas la semana pasada ya estan resueltos .
Licencia	Hay un problema con la licencia de software para este sistema StorageGRID . Puede "Actualice la información de la licencia según sea necesario" Es

Supervisar los estados de conexión de los nodos

Si uno o más nodos se desconectan de la red, las operaciones críticas de StorageGRID podrían verse afectadas. Supervise los estados de conexión de los nodos y solucione cualquier problema rápidamente.

Icono	Descripción	Acción requerida
	No conectado - Desconocido Por una razón desconocida, un nodo se desconecta o los servicios en el nodo dejan de funcionar inesperadamente. Por ejemplo, es posible que se haya detenido un servicio en el nodo o que el nodo haya perdido su conexión a la red debido a un corte de energía o una interrupción inesperada. También podría activarse la alerta No se puede comunicar con el nodo. También podrían estar activas otras alertas.	Requiere atención inmediata. Seleccione cada alerta y siga las acciones recomendadas. Por ejemplo, es posible que necesite reiniciar un servicio que se ha detenido o reiniciar el host del nodo. Nota: Un nodo puede aparecer como Desconocido durante las operaciones de apagado administrado. Puedes ignorar el estado Desconocido en estos casos.
	No conectado - Administrativamente caído Por una razón esperada, el nodo no está conectado a la red. Por ejemplo, el nodo, o los servicios en el nodo, se han apagado correctamente, el nodo se está reiniciando o se está actualizando el software. También podrían estar activas una o más alertas. Dependiendo del problema subyacente, estos nodos a menudo vuelven a estar en línea sin ninguna intervención.	Determinar si hay alguna alerta que afecte a este nodo. Si una o más alertas están activas, seleccione cada alerta y siga las acciones recomendadas.
	Conectado El nodo está conectado a la red.	No se requiere ninguna acción

Ver alertas actuales y resueltas

Alertas actuales: cuando se activa una alerta, se muestra un ícono de alerta en el panel. También se muestra un icono de alerta para el nodo en la página Nodos. Si "[Las notificaciones de alerta por correo electrónico están configuradas](#)" También se enviará una notificación por correo electrónico, a menos que se haya silenciado la alerta.

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

Opcionalmente has visto el vídeo: "[Vídeo: Descripción general de las alertas](#)"



La siguiente tabla describe la información que se muestra en el Administrador de cuadrícula para las alertas actuales y resueltas.

Encabezado de columna	Descripción
Nombre o título	El nombre de la alerta y su descripción.
Gravedad	La gravedad de la alerta. Para las alertas actuales, si se agrupan varias alertas, la fila de título muestra cuántas instancias de esa alerta ocurren en cada nivel de gravedad.  Crítico: Existe una condición anormal que ha detenido las operaciones normales de un nodo o servicio de StorageGRID . Debes abordar el problema subyacente inmediatamente. Si no se resuelve el problema podría producirse una interrupción del servicio y pérdida de datos.  Importante: Existe una condición anormal que está afectando las operaciones actuales o acercándose al umbral de una alerta crítica. Debe investigar las alertas principales y abordar cualquier problema subyacente para garantizar que la condición anormal no detenga el funcionamiento normal de un nodo o servicio de StorageGRID .  Menor: El sistema está funcionando normalmente, pero existe una condición anormal que podría afectar la capacidad del sistema para funcionar si continúa. Debes supervisar y resolver las alertas menores que no desaparecen por sí solas para garantizar que no provoquen un problema más grave.
Tiempo activado	Alertas actuales: La fecha y hora en que se activó la alerta en su hora local y en UTC. Si se agrupan varias alertas, la fila de título muestra los tiempos de la instancia más reciente de la alerta (<i>newest</i>) y la instancia más antigua de la alerta (<i>oldest</i>). Alertas resueltas: Hace cuánto tiempo se activó la alerta.
Sitio/Nodo	El nombre del sitio y el nodo donde se produce o se ha producido la alerta.

Encabezado de columna	Descripción
Estado	Si la alerta está activa, silenciada o resuelta. Si se agrupan varias alertas y se selecciona Todas las alertas en el menú desplegable, la fila de título muestra cuántas instancias de esa alerta están activas y cuántas instancias se han silenciado.
Tiempo resuelto (solo alertas resueltas)	¿Cuánto tiempo hace que se resolvió la alerta?
Valores actuales o <i>valores de datos</i>	El valor de la métrica que provocó que se activara la alerta. Para algunas alertas, se muestran valores adicionales para ayudarlo a comprender e investigar la alerta. Por ejemplo, los valores que se muestran para una alerta de Almacenamiento de datos de objetos bajo incluyen el porcentaje de espacio en disco utilizado, la cantidad total de espacio en disco y la cantidad de espacio en disco utilizado. Nota: Si se agrupan varias alertas actuales, los valores actuales no se muestran en la fila de título.
Valores activados (solo alertas resueltas)	El valor de la métrica que provocó que se activara la alerta. Para algunas alertas, se muestran valores adicionales para ayudarlo a comprender e investigar la alerta. Por ejemplo, los valores que se muestran para una alerta de Almacenamiento de datos de objetos bajo incluyen el porcentaje de espacio en disco utilizado, la cantidad total de espacio en disco y la cantidad de espacio en disco utilizado.

Pasos

1. Seleccione el enlace **Alertas actuales** o **Alertas resueltas** para ver una lista de alertas en esas categorías. También puede ver los detalles de una alerta seleccionando **Nodos > nodo > Descripción general** y luego seleccionando la alerta en la tabla Alertas.

De forma predeterminada, las alertas actuales se muestran de la siguiente manera:

- Las alertas activadas más recientemente se muestran primero.
- Varias alertas del mismo tipo se muestran como un grupo.
- Las alertas que han sido silenciadas no se muestran.
- Para una alerta específica en un nodo específico, si se alcanzan los umbrales para más de un nivel de gravedad, solo se muestra la alerta más grave. Es decir, si se alcanzan los umbrales de alerta para los niveles de gravedad menor, mayor y crítico, solo se muestra la alerta crítica.

La página de alertas actuales se actualiza cada dos minutos.

2. Para expandir grupos de alertas, seleccione el cursor hacia abajo ▼ . Para contraer alertas individuales en un grupo, seleccione el símbolo hacia arriba ▲ , o seleccione el nombre del grupo.
3. Para mostrar alertas individuales en lugar de grupos de alertas, desmarque la casilla **Alertas de grupo**.
4. Para ordenar las alertas actuales o los grupos de alertas, seleccione las flechas arriba/abajo ⬆️⬆️ en cada encabezado de columna.
 - Cuando se selecciona **Alertas de grupo**, se ordenan tanto los grupos de alertas como las alertas individuales dentro de cada grupo. Por ejemplo, es posible que desee ordenar las alertas de un grupo

por **Hora de activación** para encontrar la instancia más reciente de una alerta específica.

- Cuando se borra **Alertas de grupo**, se ordena toda la lista de alertas. Por ejemplo, es posible que desee ordenar todas las alertas por **Nodo/Sitio** para ver todas las alertas que afectan a un nodo específico.

5. Para filtrar las alertas actuales por estado (**Todas las alertas**, **Activas** o **Silenciadas**), utilice el menú desplegable en la parte superior de la tabla.

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

6. Para ordenar las alertas resueltas:

- Seleccione un período de tiempo en el menú desplegable **Cuando se activa**.
- Seleccione uno o más niveles de gravedad del menú desplegable **Gravedad**.
- Seleccione una o más reglas de alerta predeterminadas o personalizadas del menú desplegable **Regla de alerta** para filtrar las alertas resueltas relacionadas con una regla de alerta específica.
- Seleccione uno o más nodos del menú desplegable **Nodo** para filtrar las alertas resueltas relacionadas con un nodo específico.

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

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

Debes tener el "[Administrar alertas o permisos de acceso root](#)" para silenciar una regla de alerta.



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

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

- a. Desde los detalles de la alerta, seleccione **Ver condiciones**.

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

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

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

Debes tener el "[Administrar alertas o permisos de acceso root](#)" para editar una regla de alerta.



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

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

Supervisar 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 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 por los metadatos de los objetos, así como las tendencias en la cantidad de espacio consumido para cada uno. Esto le permitirá planificar con anticipación la incorporación de nodos y evitar interrupciones del servicio.

Puede [ver información sobre la capacidad de almacenamiento](#) para toda la red, para cada sitio y para cada nodo de almacenamiento en su sistema StorageGRID .

Monitorizar la capacidad de almacenamiento de toda la red

Supervise la capacidad de almacenamiento general de su red para garantizar que quede suficiente espacio libre para los datos de los objetos y los metadatos de los objetos. Comprender cómo cambia la capacidad de almacenamiento con el tiempo puede ayudarle a planificar la adición de nodos de almacenamiento o volúmenes de almacenamiento antes de que se consuma la capacidad de almacenamiento utilizable de la red.

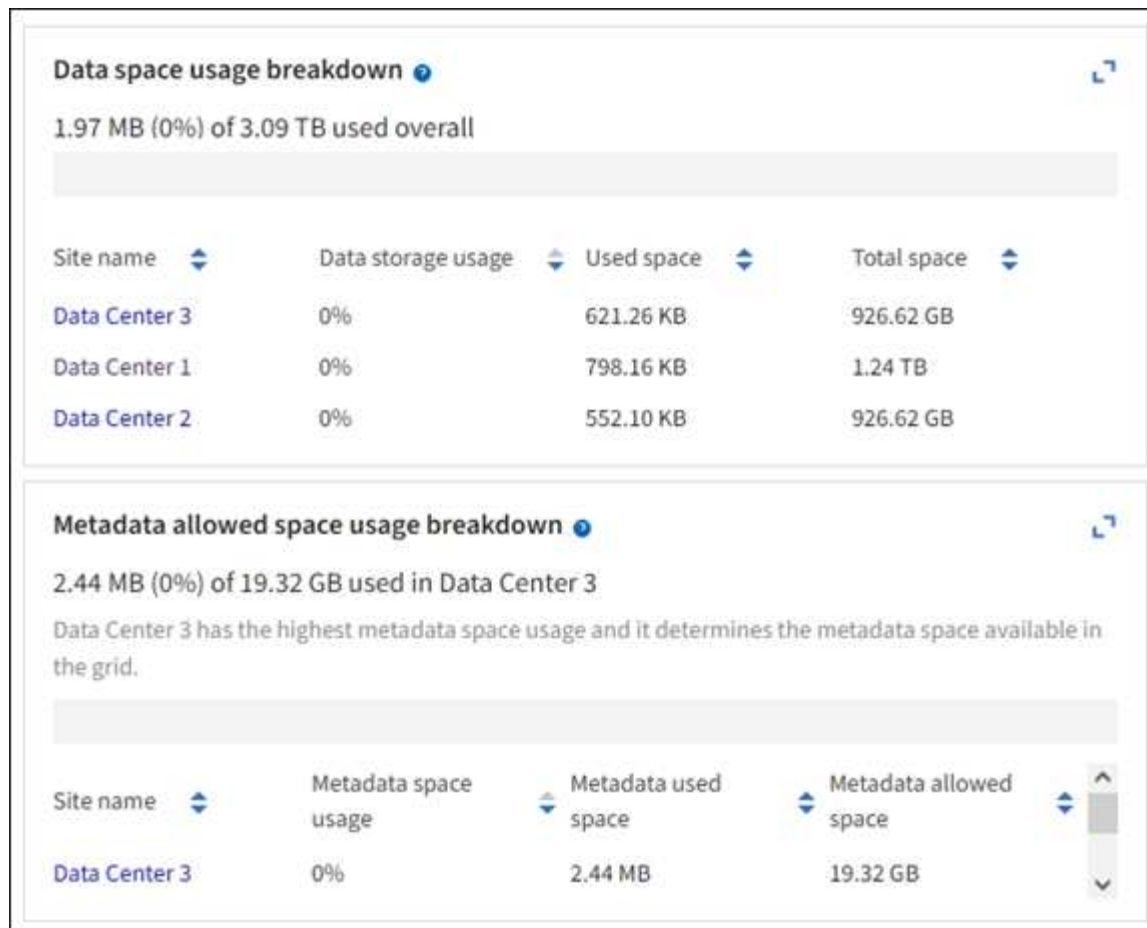
El panel de control de Grid Manager le permite evaluar rápidamente cuánto almacenamiento está disponible para toda la red y para cada centro de datos. La página Nodos proporciona valores más detallados para los datos y metadatos de los objetos.

Pasos

1. Evalúe la cantidad de almacenamiento disponible para toda la red y para cada centro de datos.
 - a. Seleccione **Panel de control > Descripción general**.
 - b. Tenga en cuenta los valores en las tarjetas Desglose del uso del espacio de datos y Desglose del uso del espacio permitido de metadatos. Cada tarjeta enumera un porcentaje de uso de almacenamiento, la capacidad de espacio utilizado y el espacio total disponible o permitido por sitio.



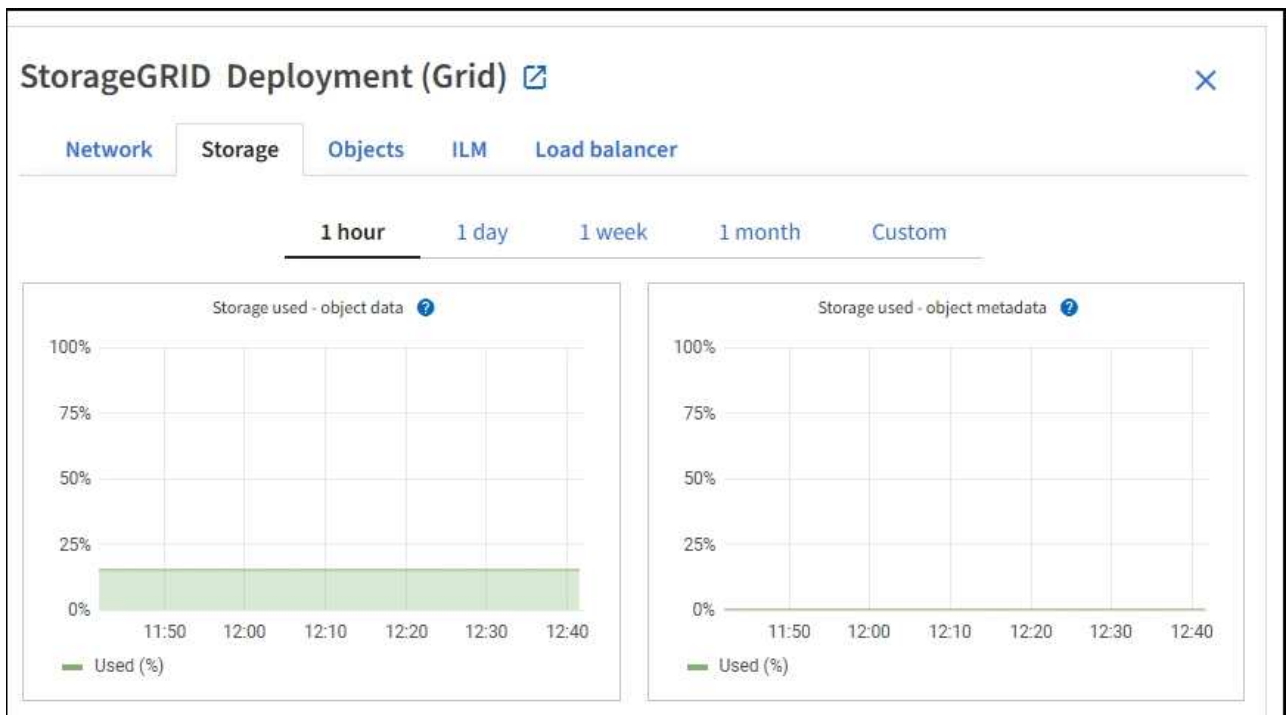
El resumen no incluye medios de archivo.



- a. Tenga en cuenta el gráfico en la tarjeta de almacenamiento a lo largo del tiempo. Utilice el menú desplegable del período de tiempo para ayudarle a determinar qué tan rápido se consume el almacenamiento.



2. Utilice la página Nodos para obtener detalles adicionales sobre cuánto almacenamiento se ha utilizado y cuánto almacenamiento queda disponible en la red para datos de objetos y metadatos de objetos.
 - a. Seleccione **NODOS**.
 - b. Seleccione **grid > Almacenamiento**.



- c. Coloque el cursor sobre los gráficos **Almacenamiento utilizado - datos de objeto** y **Almacenamiento utilizado - metadatos de objeto** para ver cuánto almacenamiento de objeto y almacenamiento de metadatos de objeto 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 red no incluyen los nodos que no han informado métricas durante al menos cinco minutos, como los nodos fuera de línea.

3. Planifique realizar una expansión para agregar nodos de almacenamiento o volúmenes de almacenamiento antes de que se consuma la capacidad de almacenamiento utilizable de la red.

Al planificar el momento de una expansión, considere cuánto tiempo llevará adquirir e instalar almacenamiento adicional.



Si su política ILM utiliza codificación de borrado, es posible que prefiera expandirse cuando los nodos de almacenamiento existentes estén aproximadamente al 70 % de su capacidad para reducir la cantidad de nodos que se deben agregar.

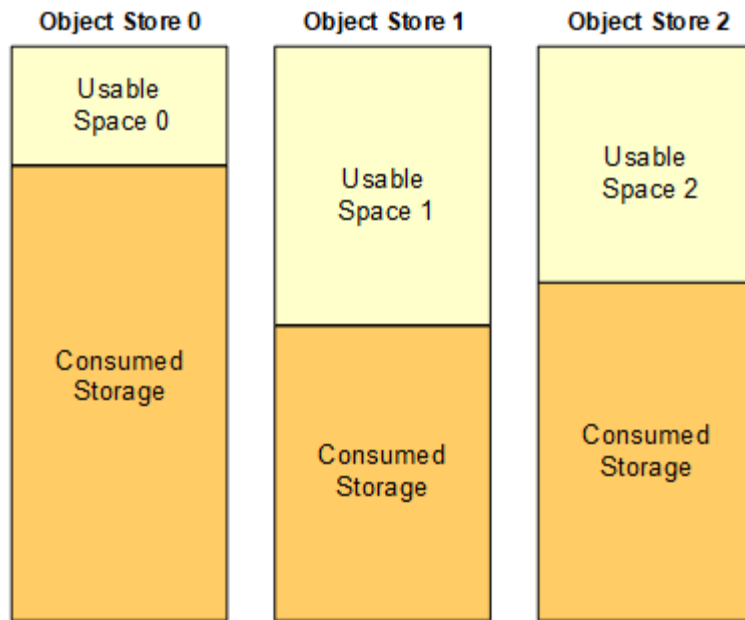
Para obtener más información sobre la planificación de una expansión de almacenamiento, consulte la ["Instrucciones para expandir StorageGRID"](#).

Supervisar la capacidad de almacenamiento de cada nodo de almacenamiento

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

Acerca de esta tarea

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



Total Usable Space = Usable Space 0 + Usable Space 1 + Usable Space 2

Pasos

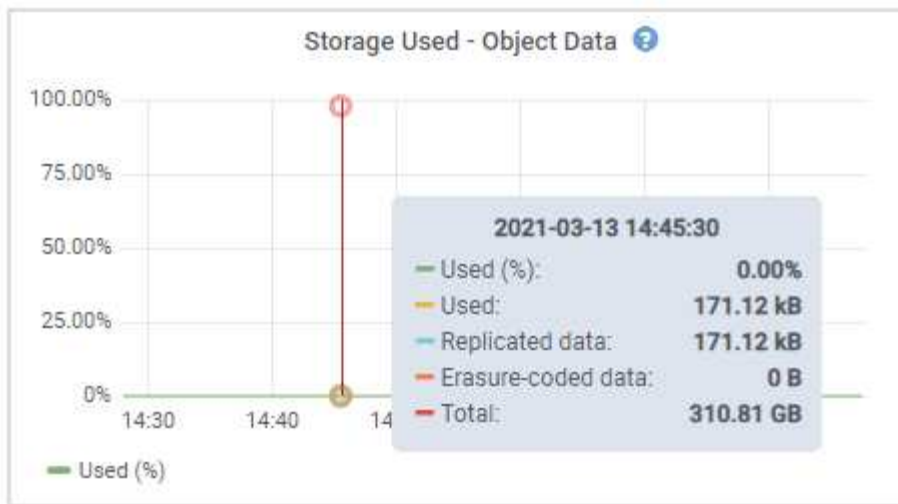
1. Seleccione **NODOS > Nodo de almacenamiento > Almacenamiento**.

Aparecen los gráficos y tablas del nodo.

2. Coloque el cursor sobre el gráfico Almacenamiento utilizado - datos del objeto.

Se muestran los siguientes valores:

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



3. Revise los valores disponibles en las tablas Volúmenes y Almacenes de objetos, debajo de los gráficos.



Para ver gráficos de estos valores, haga clic en los íconos de gráficos  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

- Monitoree los valores a lo largo del tiempo para estimar la velocidad a la que se consume el espacio de almacenamiento utilizable.
- Para mantener las operaciones normales del sistema, agregue nodos de almacenamiento, agregue volúmenes de almacenamiento o archive datos de objetos antes de que se consuma el espacio utilizable.

Al planificar el momento de una expansión, considere cuánto tiempo llevará adquirir e instalar almacenamiento adicional.



Si su política ILM utiliza codificación de borrado, es posible que prefiera expandirse cuando los nodos de almacenamiento existentes estén aproximadamente al 70 % de su capacidad para reducir la cantidad de nodos que se deben agregar.

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

la "Instrucciones para expandir StorageGRID" .

El "Almacenamiento de datos de objetos reducido" La alerta se activa cuando no queda suficiente espacio para almacenar datos de objetos en un nodo de almacenamiento.

Supervisar la capacidad de metadatos de objetos para cada nodo de almacenamiento

Supervise el uso de metadatos para cada nodo de almacenamiento para garantizar que haya suficiente espacio disponible para las operaciones esenciales de la base de datos. Debe agregar nuevos nodos de almacenamiento en cada sitio antes de que los metadatos del objeto excedan el 100 % del espacio de metadatos permitido.

Acerca de esta tarea

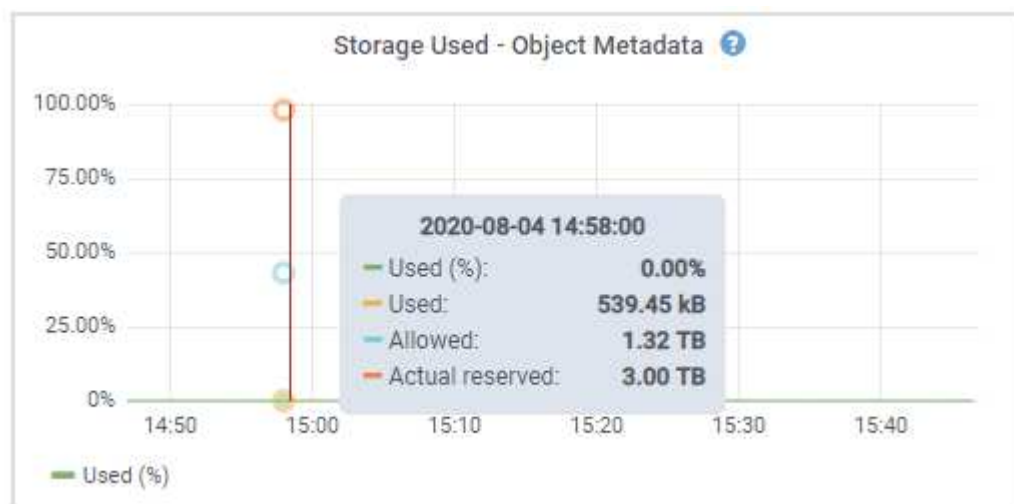
StorageGRID mantiene tres copias de metadatos de objetos en cada sitio para proporcionar redundancia y proteger los metadatos de objetos contra pérdidas. Las tres copias se distribuyen uniformemente entre todos los nodos de almacenamiento en cada sitio utilizando el espacio reservado para metadatos en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

En algunos casos, la capacidad de metadatos de objetos de la red podría consumirse más rápido que su capacidad de almacenamiento de objetos. Por ejemplo, si normalmente ingieres grandes cantidades de objetos pequeños, es posible que necesites agregar nodos de almacenamiento para aumentar la capacidad de metadatos incluso aunque todavía quede suficiente capacidad de almacenamiento de objetos.

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

Pasos

1. Seleccione **NODOS > Nodo de almacenamiento > Almacenamiento**.
2. Coloque el cursor sobre el gráfico de metadatos del objeto Almacenamiento utilizado para ver los valores de un tiempo específico.



Usado (%)

El porcentaje del espacio de metadatos permitido que se ha utilizado en este nodo de almacenamiento.

Métricas de Prometheus: `storagegrid_storage_utilization_metadata_bytes` y `storagegrid_storage_utilization_metadata_allowed_bytes`

Usado

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

Métrica de Prometeo: `storagegrid_storage_utilization_metadata_bytes`

Permitido

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

Métrica de Prometeo: `storagegrid_storage_utilization_metadata_allowed_bytes`

Reservado actual

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

La métrica Prometheus se agregará en una versión futura.



Los valores totales de un sitio o de la red no incluyen los nodos que no han informado métricas durante al menos cinco minutos, como los nodos fuera de línea.

3. Si el valor **Usado (%)** es 70% o superior, expanda su sistema StorageGRID agregando nodos de almacenamiento a cada sitio.



La alerta **Almacenamiento de metadatos bajo** se activa cuando el valor **Usado (%)** alcanza ciertos umbrales. Pueden producirse resultados no deseados si los metadatos del objeto utilizan más del 100% del espacio permitido.

Cuando agrega nuevos nodos, el sistema reequilibra automáticamente los metadatos de los objetos en todos los nodos de almacenamiento dentro del sitio. Ver el ["Instrucciones para expandir un sistema StorageGRID"](#).

Monitorear las previsiones de uso del espacio

Monitoree los pronósticos de uso del espacio para los datos de usuario y metadatos para estimar cuándo los necesitará. ["expandir una cuadrícula"](#).

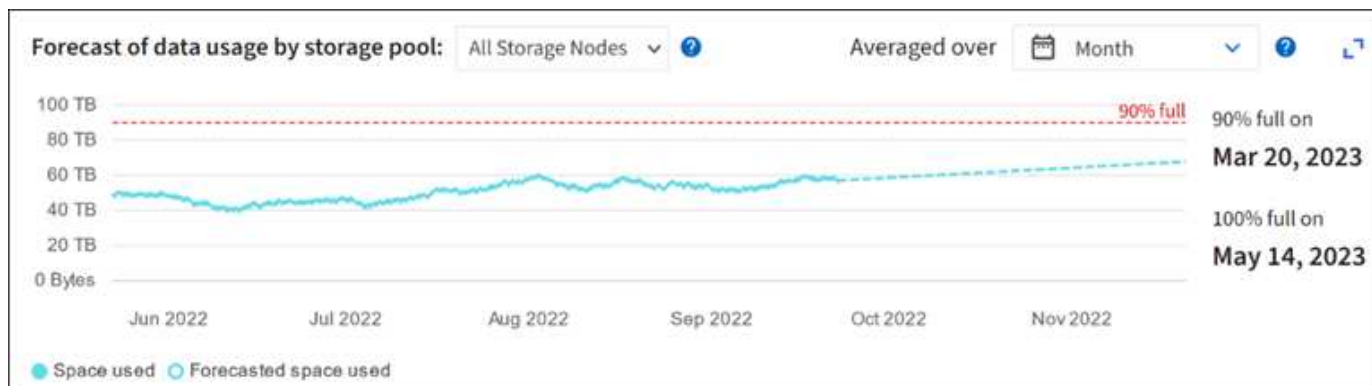
Si observa que la tasa de consumo cambia con el tiempo, seleccione un rango más corto en el menú desplegable **Promedio sobre** para reflejar solo los patrones de ingesta más recientes. Si observa patrones estacionales, seleccione un rango más largo.

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

Pasos

1. En el panel de control, seleccione **Almacenamiento**.
2. Vea las tarjetas del panel, el pronóstico del uso de datos por grupo de almacenamiento y el pronóstico del uso de metadatos por sitio.
3. Utilice estos valores para estimar cuándo necesitará agregar nuevos nodos de almacenamiento para el

almacenamiento de datos y metadatos.



Supervisar 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 la red. Debe supervisar las operaciones de ILM para comprender si la red puede soportar la carga actual o si se necesitan más recursos.

Acerca de esta tarea

El sistema StorageGRID administra objetos mediante la aplicación de las políticas ILM activas. Las políticas de ILM y las reglas de ILM asociadas determinan cuántas copias se realizan, el tipo de copias que se crean, dónde se colocan las copias y el tiempo que se conserva cada copia.

La ingesta de objetos y otras actividades relacionadas con objetos pueden exceder 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 pueden cumplir casi en tiempo real. Debe supervisar si StorageGRID se mantiene al día con las acciones del cliente.

Utilice la pestaña del panel de control de Grid Manager

Pasos

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

1. Sign in en el Administrador de cuadrícula.
2. Desde el panel de control, seleccione la pestaña ILM y anote los valores en la tarjeta de cola de ILM (Objetos) y la tarjeta de tarifa de evaluación de ILM.

Se esperan picos temporales en la tarjeta de cola ILM (Objetos) en el tablero. Pero si la cola continúa aumentando y nunca disminuye, la red necesita más recursos para funcionar de manera eficiente: más nodos de almacenamiento o, si la política ILM coloca objetos en ubicaciones remotas, más ancho de banda de red.

Utilice la página NODOS

Pasos

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



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

1. Seleccione **NODOS**.
2. Seleccione **nombre de la cuadrícula > ILM**.
3. Coloque el cursor sobre el gráfico de la cola ILM para ver el valor de los siguientes atributos en un momento determinado:
 - **Objetos en cola (de operaciones del cliente)**: la cantidad total de objetos que esperan la evaluación de ILM debido a operaciones del cliente (por ejemplo, ingesta).
 - **Objetos en cola (de todas las operaciones)**: la cantidad total de objetos que esperan la evaluación de ILM.
 - **Velocidad de escaneo (objetos/seg)**: la velocidad a la que se escanean los objetos de la cuadrícula y se ponen en cola para ILM.
 - **Tasa de evaluación (objetos/seg)**: La tasa actual a la que se evalúan los objetos en relación con la política ILM en la cuadrícula.
4. En la sección Cola ILM, observe los siguientes atributos.



La sección de cola ILM está incluida solo para la cuadrícula. Esta información no se muestra en la pestaña ILM de un sitio o nodo de almacenamiento.

- **Período de escaneo – estimado**: el tiempo estimado para completar un escaneo ILM completo de todos los objetos.



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

- **Reparaciones intentadas**: la cantidad total de operaciones de reparación de objetos para datos replicados que se han intentado. Este recuento aumenta cada vez que un nodo de almacenamiento intenta reparar un objeto de alto riesgo. Las reparaciones de ILM de alto riesgo se priorizan si la red se sobrecarga.



La misma reparación del objeto podría incrementarse nuevamente si la replicación falla después de la reparación.

Estos atributos pueden resultar útiles cuando supervisa el progreso de la recuperación del volumen del nodo de almacenamiento. Si el número de reparaciones intentadas ha dejado de aumentar y se ha completado un análisis completo, es probable que la reparación se haya completado.

Supervisar la red y los recursos del sistema

La integridad y el ancho de banda de la red entre nodos y sitios, y el uso de recursos por parte de los nodos individuales de la red, son fundamentales para operaciones eficientes.

Supervisar las conexiones y el rendimiento de la red

La conectividad de la red y el ancho de banda son especialmente importantes si su política de gestión del ciclo de vida de la información (ILM) copia objetos replicados entre sitios o almacena objetos con código de borrado utilizando un esquema que proporciona protección contra pérdida de sitios. 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 ILM no puedan colocar objetos donde se espera. Esto puede provocar fallas de ingesta (cuando se selecciona la opción Ingesta estricta para las reglas de ILM) o un rendimiento de ingesta deficiente y retrasos en ILM.

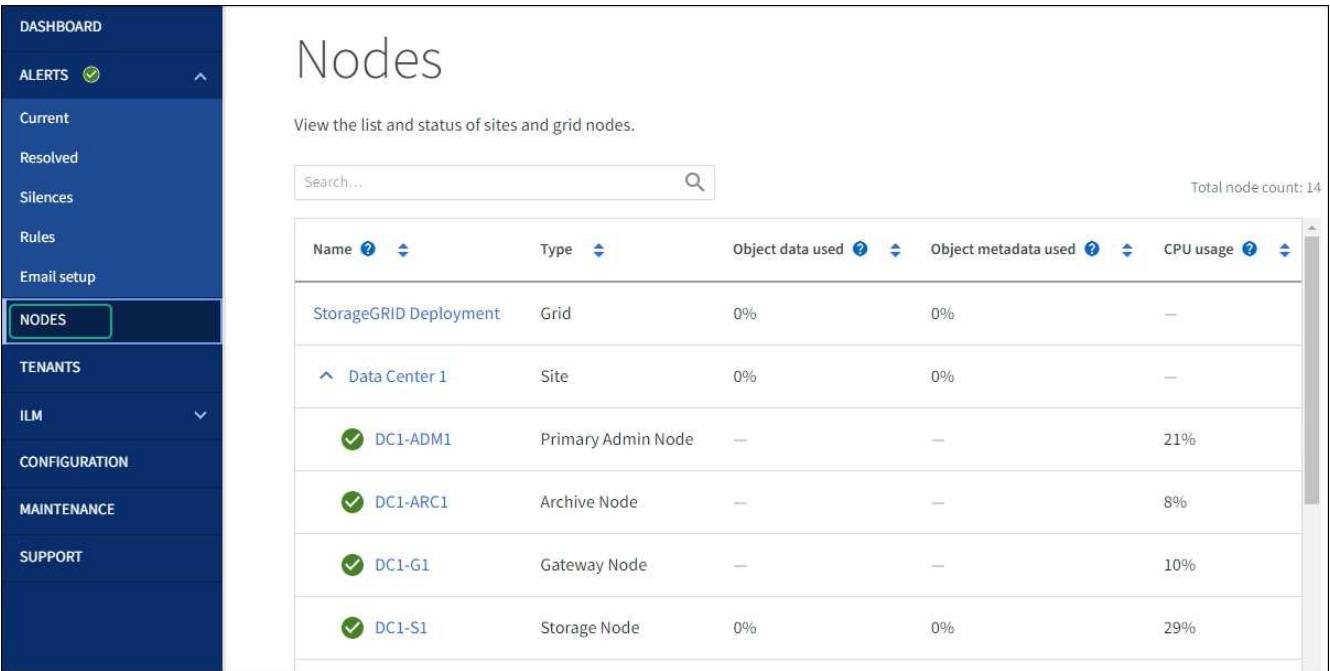
Utilice Grid Manager para supervisar la conectividad y el rendimiento de la red, de modo que pueda solucionar cualquier problema rápidamente.

Además, considere "Creación de políticas de clasificación del tráfico de red" para que pueda supervisar el tráfico relacionado con inquilinos, depósitos, subredes o puntos finales del balanceador de carga específicos. Puede establecer políticas de limitación de tráfico según sea necesario.

Pasos

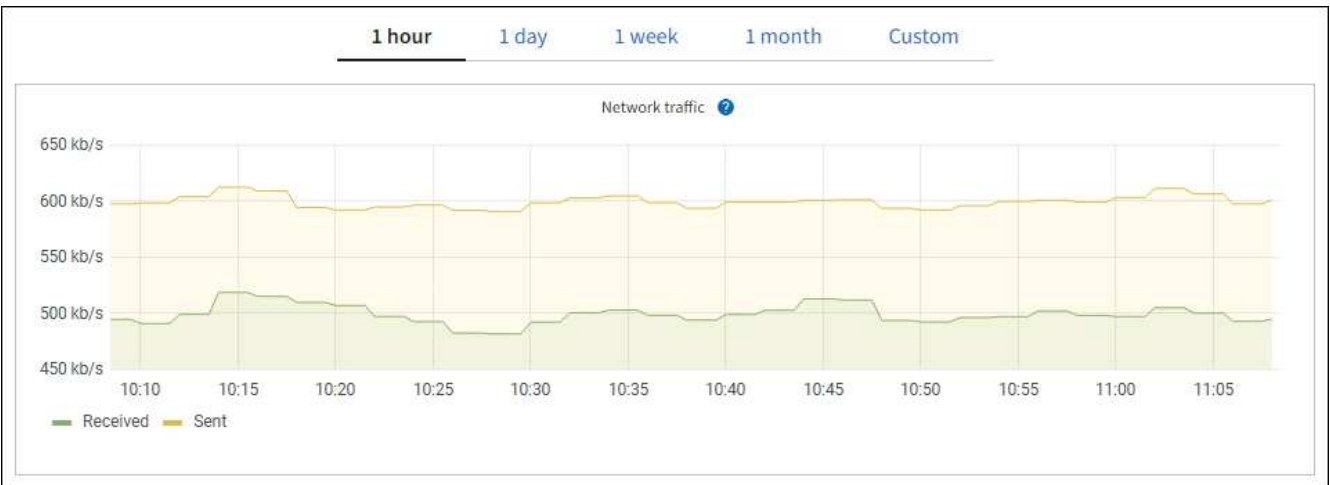
- 1. Seleccione **NODOS**.

Aparece la página Nodos. Cada nodo de la cuadrícula aparece enumerado en formato de tabla.



- 2. Seleccione el nombre de la red, un sitio de centro de datos específico o un nodo de la red y luego seleccione la pestaña **Red**.

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



- a. Si seleccionó 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 los nodos de la red, 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 sus políticas de clasificación de tráfico para monitorear el tráfico de red.

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

Aparece la página Políticas de clasificación de tráfico y las políticas existentes se enumeran 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. Para ver gráficos que muestran las métricas de red asociadas con una política, seleccione el botón de opción a la izquierda de la política y luego haga clic en **Métricas**.
- b. Revise los gráficos para comprender el tráfico de red asociado con la política.

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

Información relacionada

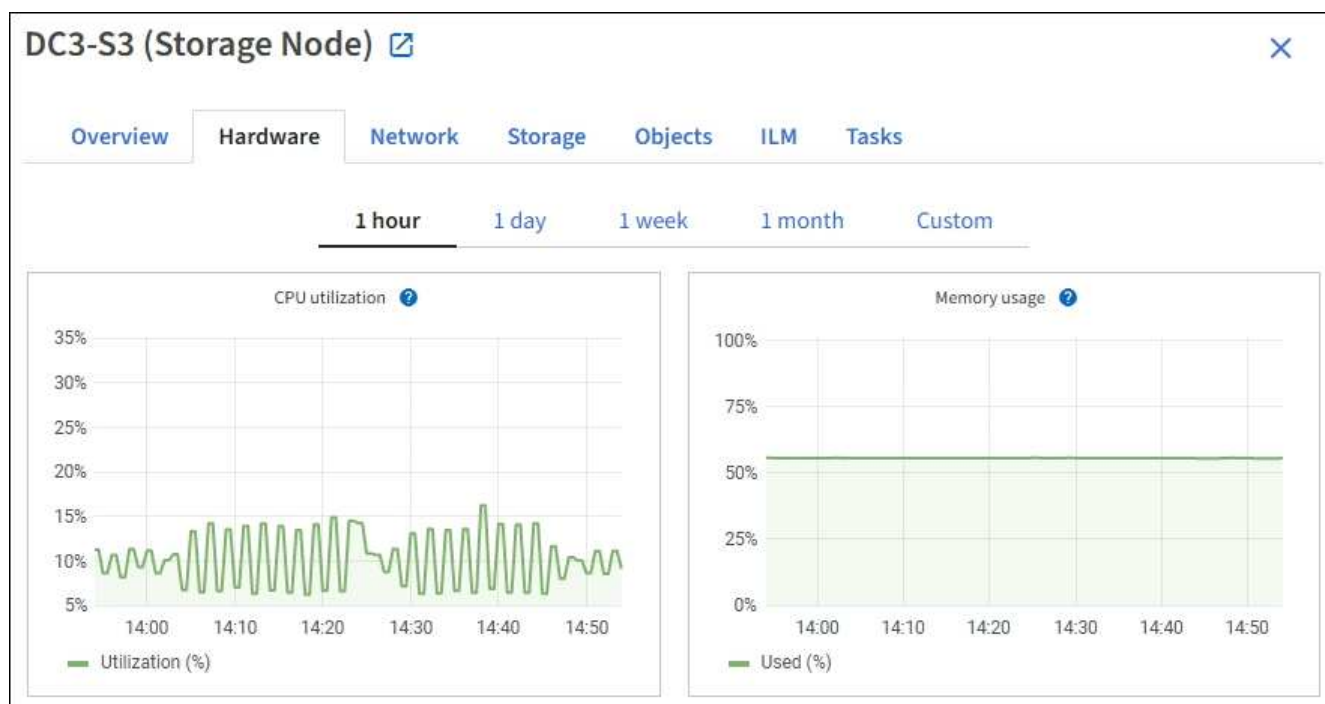
- ["Ver la pestaña Red"](#)
- ["Supervisar los estados de conexión de los nodos"](#)

Supervisar los recursos a nivel de nodo

Supervise los nodos individuales de la red para verificar sus niveles de uso de recursos. Si los nodos están constantemente sobrecargados, podrían requerirse más nodos para realizar operaciones eficientes.

Pasos

1. Desde la página **NODOS**, seleccione el nodo.
2. Seleccione la pestaña **Hardware** para mostrar gráficos de utilización de CPU y uso de memoria.



3. Para mostrar un intervalo de tiempo diferente, seleccione uno de los controles sobre el gráfico. Puede mostrar 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 rangos de fecha y hora.
4. Si el nodo está alojado en un dispositivo de almacenamiento o un dispositivo de servicios, desplácese hacia abajo para ver las tablas de componentes. El estado de todos los componentes debe ser "Nominal". Investigar componentes que tengan cualquier otro estado.

Información relacionada

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

Supervisar la actividad de los inquilinos

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"Permiso de acceso de root o de cuentas de inquilino" .

Ver todos los inquilinos

La página Inquilinos muestra información básica de todas las cuentas de inquilinos actuales.

Pasos

1. Seleccione **INQUILINOS**.
2. Revise la información que se muestra en las páginas de Inquilinos.

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



Los valores de espacio utilizados son estimaciones. Estas estimaciones se ven afectadas por el momento de la ingesta, la conectividad de la red y el estado del nodo.

Tenants

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

CreateExport to CSVActions

Search tenants by name or ID

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

3. Opcionalmente, inicie sesión en una cuenta de inquilino seleccionando el enlace de inicio de sesión→ en la columna * Sign in/Copiar URL*.
4. Opcionalmente, copie la URL de la página de inicio de sesión de un inquilino seleccionando el enlace copiar URL📄 en la columna * Sign in/Copiar URL*.

- Opcionalmente, seleccione **Exportar a CSV** para ver y exportar un .csv archivo que contiene los valores de uso para todos los inquilinos.

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

El contenido de la .csv El archivo se parece al siguiente ejemplo:

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	110000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	4750000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

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

- Si no se enumeran objetos, opcionalmente, seleccione **Acciones > Eliminar** para eliminar uno o más inquilinos. Ver ["Eliminar cuenta de inquilino"](#).

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

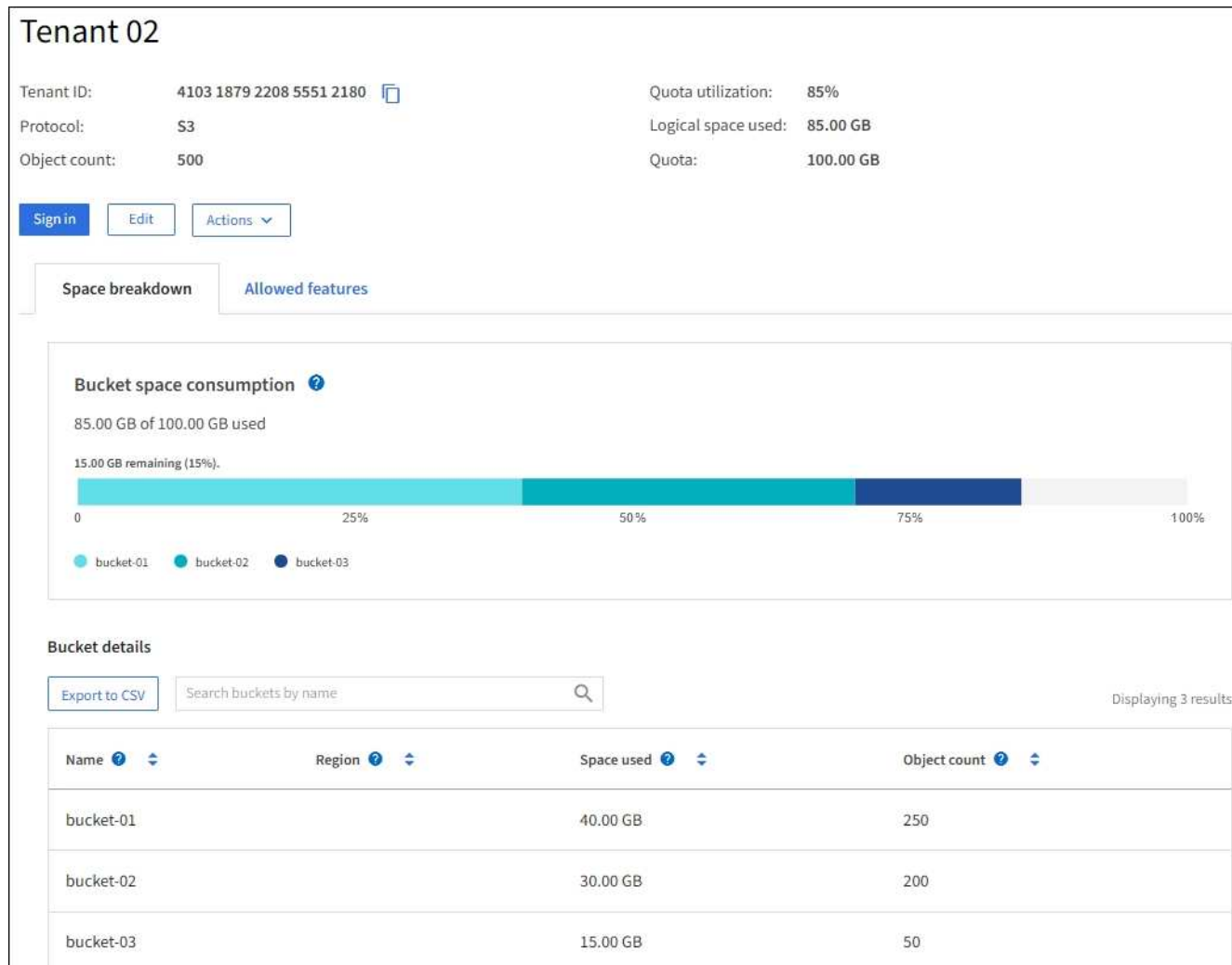
Ver un inquilino específico

Puede ver los detalles de un inquilino específico.

Pasos

- Seleccione el nombre del inquilino en la página Inquilinos.

Aparece la página de detalles del inquilino.



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

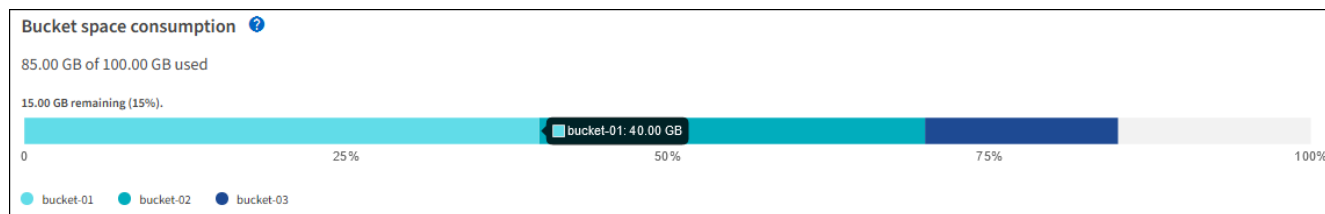
Esta sección de la página de detalles proporciona información resumida del inquilino, incluido el recuento de objetos del inquilino, el uso de cuota, el espacio lógico utilizado y la configuración de cuota.

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

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

Si se estableció una cuota para este inquilino, la cantidad de cuota utilizada y restante se muestra en texto (por ejemplo, 85.00 GB of 100 GB used). Si no se estableció ninguna cuota, el inquilino tiene una cuota ilimitada y el texto incluye solo una cantidad de espacio utilizado (por ejemplo, 85.00 GB used). El gráfico de barras muestra el porcentaje de cuota en cada contenedor o depósito. Si el inquilino ha excedido la cuota de almacenamiento en más del 1% y en al menos 1 GB, el gráfico muestra la cuota total y la cantidad excedente.

Puede colocar el cursor sobre el gráfico de barras para ver el almacenamiento utilizado por cada depósito o contenedor. Puede colocar el cursor sobre el segmento de espacio libre para ver la cantidad de cuota de almacenamiento restante.



El uso de la cuota se basa en estimaciones internas y podría superarse en algunos casos. Por ejemplo, StorageGRID verifica la cuota cuando un inquilino comienza a cargar objetos y rechaza nuevas ingestas si el inquilino ha excedido la cuota. Sin embargo, StorageGRID no tiene en cuenta el tamaño de la carga actual al determinar si se ha excedido la cuota. Si se eliminan objetos, es posible que a un inquilino se le impida temporalmente cargar nuevos objetos hasta que se vuelva a calcular el uso de la cuota. Los cálculos de uso de cuota pueden tardar 10 minutos o más.



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



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

4. Desde la pestaña **Desglose de espacio**, revise los **Detalles del depósito**.

Esta tabla enumera los depósitos S3 para el inquilino. El espacio utilizado es la cantidad total de datos del objeto en el depósito o contenedor. Este valor no representa el espacio de almacenamiento necesario para las copias ILM y los metadatos de los objetos.

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

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

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

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

6. Opcionalmente, seleccione la pestaña **Funciones permitidas** para ver una lista de los permisos y funciones que están habilitados para el inquilino. Ver ["Editar cuenta de inquilino"](#) Si necesita cambiar alguna de estas configuraciones.

7. Si el inquilino tiene el permiso **Usar conexión de federación de red**, seleccione opcionalmente la pestaña **Federación de red** para obtener más información sobre la conexión.

Ver ["¿Qué es la federación de red?"](#) y ["Gestionar los inquilinos permitidos para la federación de red"](#).

Ver el tráfico de la red

Si existen políticas de clasificación de tráfico para un inquilino, revise el tráfico de red de ese inquilino.

Pasos

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

Aparece la página Políticas de clasificación de tráfico y las políticas existentes se enumeran en la tabla.

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

Ver ["Administrar políticas de clasificación de tráfico"](#) Para más información.

Utilice el registro de auditoría

Opcionalmente, puede utilizar el registro de auditoría para realizar un seguimiento más granular de las actividades de un inquilino.

Por ejemplo, puede supervisar los siguientes tipos de información:

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

Los registros de auditoría se escriben en archivos de texto que puede analizar utilizando la herramienta de análisis de registros de su elección. Esto le permite comprender mejor las actividades de los clientes o implementar modelos sofisticados de facturación y devolución de cargos.

Ver ["Revisar los registros de auditoría"](#) Para más información.

Utilice las métricas de Prometheus

Opcionalmente, utilice las métricas de Prometheus para informar sobre la actividad de los inquilinos.

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



Las herramientas disponibles en la página Métricas están destinadas principalmente para ser utilizadas por el soporte técnico. Algunas funciones y elementos del menú de estas herramientas no son funcionales intencionalmente.

- Desde la parte superior del Administrador de cuadrícula, seleccione el ícono de ayuda y seleccione **Documentación de API**. Puede utilizar las métricas en la sección Métricas de la API de administración de cuadrícula para crear reglas de alerta y paneles personalizados para la actividad de los inquilinos.

Ver ["Revisar las métricas de soporte"](#) Para más información.

Supervisar las operaciones del cliente S3

Puede supervisar las tasas de ingesta y recuperación de objetos, así como las métricas de recuento de objetos, consultas y verificación. Puede ver la cantidad de intentos exitosos y fallidos de las aplicaciones cliente para leer, escribir y modificar objetos en el sistema StorageGRID .

Antes de empezar

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

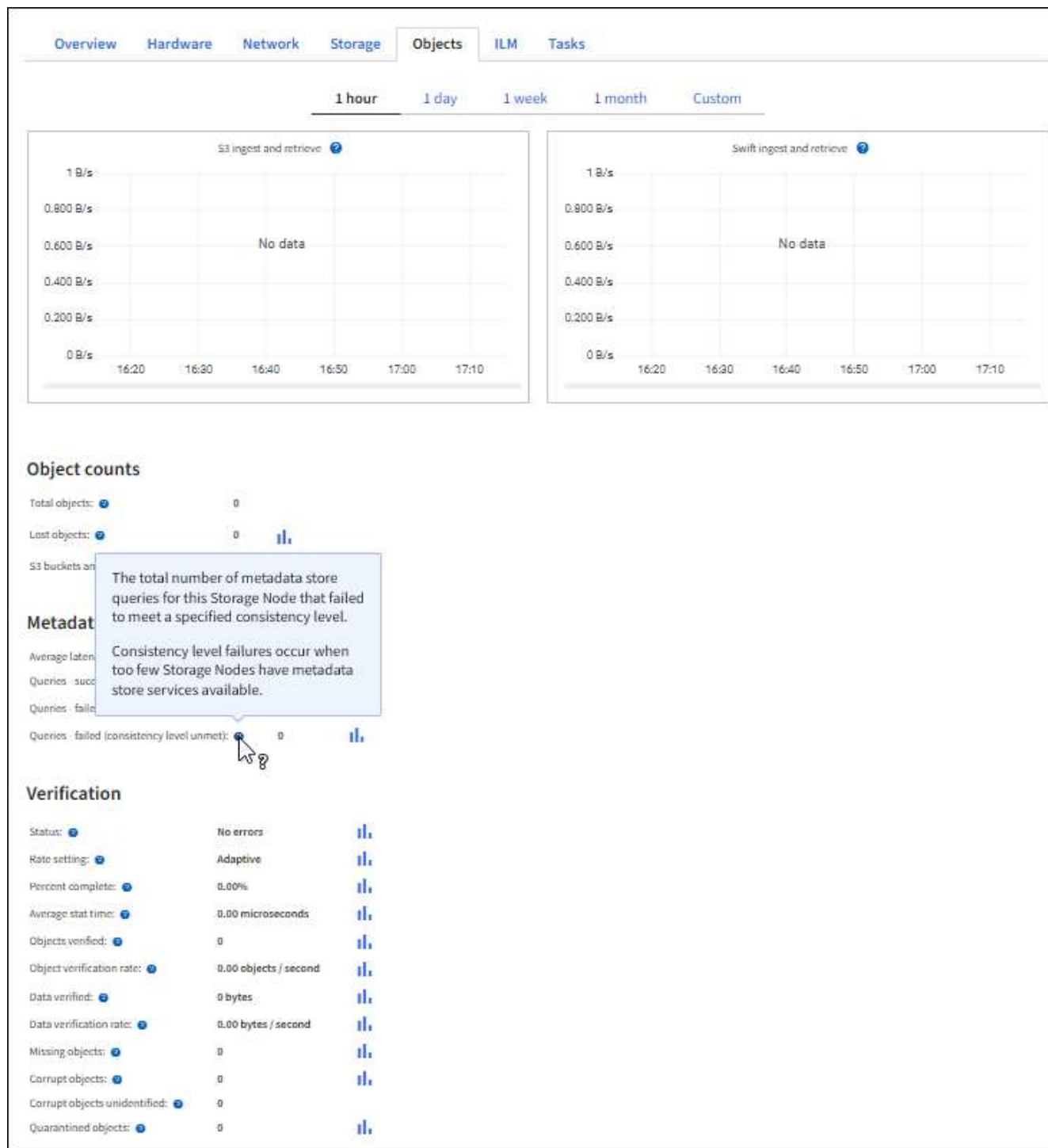
Pasos

1. Desde el panel de control, seleccione la pestaña **Rendimiento**.
2. Consulte los gráficos de S3, que resumen la cantidad de operaciones de cliente realizadas por los nodos de almacenamiento y la cantidad de solicitudes de API recibidas por los nodos de almacenamiento durante el período de tiempo seleccionado.
3. Seleccione **NODOS** para acceder a la página Nodos.
4. Desde la página de inicio de Nodos (nivel de cuadrícula), seleccione la pestaña **Objetos**.

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

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

El gráfico muestra las tasas de ingesta y recuperación del nodo. La pestaña también incluye métricas para recuentos de objetos, consultas de metadatos y operaciones de verificación.



Supervisar las operaciones de equilibrio de carga

Si está utilizando un equilibrador de carga para administrar las conexiones de clientes 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 realizar una expansión.

Acerca de esta tarea

Puede utilizar el servicio Load Balancer en nodos de administración o nodos de puerta de enlace o un balanceador de carga externo de terceros para distribuir solicitudes de clientes entre múltiples nodos de

almacenamiento.

Después de configurar el equilibrio de carga, debe confirmar que las operaciones de ingesta y recuperación de objetos se distribuyan de manera uniforme entre los nodos de almacenamiento. Las solicitudes distribuidas uniformemente garantizan que StorageGRID siga 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 (HA) de nodos de puerta de enlace o nodos de administración en modo de respaldo activo, solo un nodo del grupo distribuye activamente las solicitudes de los clientes.

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

Pasos

1. Si los clientes S3 se conectan mediante el servicio Load Balancer, verifique que los nodos de administración o los nodos de puerta de enlace estén distribuyendo el tráfico de forma activa como espera:

- a. Seleccione **NODOS**.
- b. Seleccione un nodo de puerta de enlace o un nodo de administración.
- c. En la pestaña **Descripción general**, verifique si una interfaz de nodo está en un grupo de alta disponibilidad y si la interfaz de nodo tiene el rol de Principal.

Los nodos con el rol de principal y los nodos que no están en un grupo de alta disponibilidad deben distribuir activamente solicitudes a los clientes.

- d. Para cada nodo que debería estar distribuyendo activamente solicitudes de clientes, seleccione el ["Pestaña Balanceador de carga"](#).
- e. Revise el gráfico del tráfico de solicitudes del balanceador de carga de la última semana para asegurarse de que el nodo haya estado distribuyendo solicitudes de forma activa.

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

- f. Revise el gráfico de la tasa de solicitudes entrantes del balanceador de carga de la última semana para revisar el rendimiento de objetos del nodo.
 - g. Repita estos pasos para cada nodo de administración o nodo de puerta de enlace en el sistema StorageGRID.
 - h. Opcionalmente, utilice políticas de clasificación de tráfico para ver un análisis más detallado del tráfico atendido por el servicio Load Balancer.
2. Verifique que estas solicitudes se distribuyan uniformemente entre los nodos de almacenamiento.
 - a. Seleccione **Nodo de almacenamiento > LDR > HTTP**.
 - b. Revise el número de **Sesiones entrantes establecidas actualmente**.
 - c. Repita este procedimiento para cada nodo de almacenamiento en la cuadrícula.

La cantidad de sesiones debe ser aproximadamente igual en todos los nodos de almacenamiento.

Supervisar las conexiones de la federación de red

Puede monitorear información básica sobre todos ["conexiones de federación de red"](#), información detallada sobre una conexión específica o métricas de Prometheus sobre

operaciones de replicación entre redes. Puedes monitorear una conexión desde cualquiera de las redes.

Antes de empezar

- Ha iniciado sesión en el Administrador de cuadrícula en cualquiera de las cuadrículas mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) para la red en la que ha iniciado sesión.

Ver todas las conexiones

La página de federación de red muestra información básica sobre todas las conexiones de federación de red y sobre todas las cuentas de inquilinos que tienen permiso para usar conexiones de federación de red.

Pasos

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

Aparece la página de federación de Grid.

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

Desde esta pestaña, puedes:

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

Grid federation

Learn more about grid federation

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

Connections

Permitted tenants

Add connectionUpload verification fileActions

Search...

Displaying 1 connection

Connection name	Remote hostname	Connection status
Grid 1 - Grid 2	10.96.130.76	Connected

3. Para ver información básica de todas las cuentas de inquilinos en esta red que tienen el permiso **Usar conexión de federación de red**, seleccione la pestaña **Inquilinos permitidos**.

Desde esta pestaña, puedes:

- ["Ver la página de detalles de cada inquilino permitido"](#) .
- Ver la página de detalles de cada conexión. Ver [Ver una conexión específica](#) .
- Seleccione un inquilino permitido y ["eliminar el permiso"](#) .
- Verifique si hay errores de replicación entre redes y borre el último error, si lo hay. Ver ["Solucionar errores de federación de red"](#) .

Grid federation [Learn more about grid federation](#)

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

[Connections](#)
[Permitted tenants](#)

[Remove permission](#)
[Clear error](#)

Displaying one result

Tenant name	Connection name	Connection status	Remote grid hostname	Last error
Tenant A	Grid 1 - Grid 2	Connected	10.96.130.76	Check for errors

Ver una conexión específica

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

Pasos

1. Seleccione cualquiera de las pestañas de la página de federación de Grid y luego seleccione el nombre de la conexión de la tabla.

Desde la página de detalles de la conexión, puedes:

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

2. Al ver una conexión específica, seleccione la pestaña **Inquilinos permitidos** para ver detalles sobre los inquilinos permitidos para la conexión.

Desde esta pestaña, puedes:

- ["Ver la página de detalles de cada inquilino permitido"](#) .
- ["Quitar el permiso de un inquilino"](#) para utilizar la conexión.
- Verifique si hay errores de replicación entre redes y borre el último error. Ver ["Solucionar errores de federación de red"](#) .

Grid 1 - Grid 2

Local hostname (this grid): 10.96.130.64

Port: 23000

Remote hostname (other grid): 10.96.130.76

Connection status: ✔ Connected

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

[Permitted tenants](#)
[Certificates](#)

[Remove permission](#)
[Clear error](#)

Displaying one result

Tenant name	Last error
☒ Tenant A Check for errors	

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

Desde esta pestaña, puedes:

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

Grid A-Grid B

Local hostname (this grid):10.96.106.230

Port:23000

Remote hostname (other grid):10.96.104.230

Connection status:

Connected

EditDownload fileTest connectionRemove

Permitted tenantsCertificates

Rotate certificates

ServerClient

Download certificateCopy certificate PEM

Metadata?

Subject DN:/C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=10.96.106.230

Serial number:30:81:B8:DD:AE:B2:86:0A

Issuer DN:/C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=GPT

Issued on:2022-10-04T02:21:18.000Z

Expires on:2024-10-03T19:05:13.000Z

SHA-1 fingerprint:92:7A:03:AF:6D:1C:94:8C:33:24:08:84:F9:2B:01:23:7D:BE:F2:DF

SHA-256 fingerprint:54:97:3E:77:EB:D3:6A:0F:8F:EE:72:83:D0:39:86:02:32:A5:60:9D:6F:C0:A2:3C:76:DA:3F:4D:FF:64:5D:60

Alternative names:IP Address:10.96.106.230

Certificate PEM?

-----BEGIN CERTIFICATE-----
MIIGdTCCBF2gAwIBAgIIHIG43a6yhgowDQYJKoZIhvcNAQENBQAwdzELMAkGA1UE
BhIMCVVMxEzARBgNVBAglMCKNhbg1mb3JuaWExejAQBgNVBAcMCVN1bm55dmFsZTEU
NDIwOjE1MDQyMjE1ODQyMTUzLTAuMC51PzAtBgkqhkiG9w0BCQEwAA==
-----END CERTIFICATE-----

Revisar las métricas de replicación entre redes

Puede utilizar el panel de replicación entre redes en Grafana para ver las métricas de Prometheus sobre las operaciones de replicación entre redes en su red.

Pasos

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



Las herramientas disponibles en la página Métricas están destinadas a ser utilizadas por el soporte técnico. Algunas funciones y elementos del menú de estas herramientas no son funcionales intencionalmente y están sujetos a cambios. Ver la lista de ["Métricas de Prometheus de uso común"](#) .

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

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

3. Para volver a intentar la replicación de objetos que no se pudieron replicar, consulte ["Identificar y reintentar operaciones de replicación fallidas"](#) .

Administrar alertas

Administrar alertas

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

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

- Se muestra un ícono de gravedad de alerta en el panel del Administrador de cuadrícula y se incrementa el recuento de alertas actuales.
- La alerta se muestra en la página de resumen **NODES** y en la pestaña **NODES > node > Overview**.
- Se envía una notificación por correo electrónico, asumiendo que ha configurado un servidor SMTP y proporcionado direcciones de correo electrónico para los destinatarios.
- Se envía una notificación de Protocolo simple de administración de red (SNMP), asumiendo que ha configurado el agente SNMP de StorageGRID .

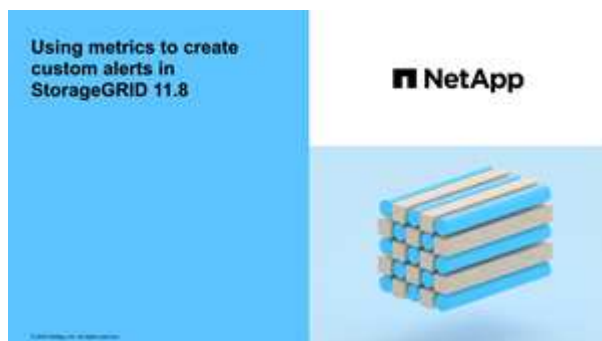
Puede crear alertas personalizadas, editarlas o deshabilitarlas y administrarlas.

Para saber más:

- Revisa el video: ["Vídeo: Descripción general de las alertas"](#)



- Revisa el video: ["Vídeo: Alertas personalizadas"](#)



- Ver el ["Referencia de alertas"](#) .

Ver reglas de alerta

Las reglas de alerta definen las condiciones que se activan "alertas específicas" . StorageGRID incluye un conjunto de reglas de alerta predeterminadas, que puede usar tal cual o modificar, o puede crear reglas de alerta personalizadas.

Puede ver la lista de todas las reglas de alerta predeterminadas y personalizadas para saber qué condiciones activarán cada alerta y ver si alguna alerta está deshabilitada.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "navegador web compatible" .
- Tú tienes el "Administrar alertas o permisos de acceso root" .
- Opcionalmente has visto el vídeo: "Vídeo: Descripción general de las alertas"



Pasos

1. Seleccione **ALERTAS > Reglas**.

Aparece 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 alerta:

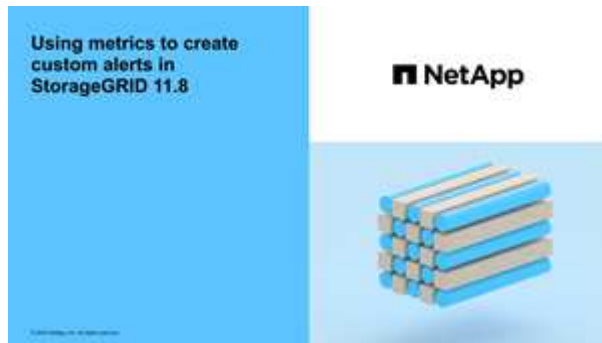
Encabezado de columna	Descripción
Nombre	El nombre único y la descripción de la regla de alerta. Las reglas de alerta personalizadas se enumeran primero, seguidas de las reglas de alerta predeterminadas. El nombre de la regla de alerta es el asunto de las notificaciones por correo electrónico.
Condiciones	Las expresiones de Prometeo que determinan cuándo se activa esta alerta. Se puede activar una alerta en uno o más de los siguientes niveles de gravedad, pero no se requiere una condición para cada nivel de gravedad. • *Crítico*  :Existe una condición anormal que ha detenido las operaciones normales de un nodo o servicio de StorageGRID . Debes abordar el problema subyacente inmediatamente. Si no se resuelve el problema podría producirse una interrupción del servicio y pérdida de datos. • *Importante*  :Existe una condición anormal que está afectando las operaciones actuales o acercándose al umbral de una alerta crítica. Debe investigar las alertas principales y abordar cualquier problema subyacente para garantizar que la condición anormal no detenga el funcionamiento normal de un nodo o servicio de StorageGRID . • *Menor*  :El sistema está funcionando normalmente, pero existe una condición anormal que podría afectar la capacidad del sistema para funcionar si continúa. Debes supervisar y resolver las alertas menores que no desaparecen por sí solas para garantizar que no provoquen un problema más grave.
Tipo	El tipo de regla de alerta: • Predeterminado: Una 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*: una 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: Una regla de alerta que usted creó. Puede deshabilitar, editar y eliminar reglas de alerta personalizadas.
Estado	Si esta regla de alerta está actualmente habilitada o deshabilitada. Las condiciones para las reglas de alerta deshabilitadas 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.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Administrar alertas o permisos de acceso root"](#) .
- Estás familiarizado con el ["Métricas de Prometheus de uso común"](#) .
- Tú entiendes el ["Sintaxis de las consultas de Prometheus"](#) .
- Opcionalmente has visto el vídeo: ["Vídeo: Alertas personalizadas"](#) .



Acerca de esta tarea

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

- Observe las condiciones de las reglas de alerta predeterminadas y utilícelas 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. Luego, cambie el valor del umbral para cada condición.
- Revise cuidadosamente cada condición para detectar errores tipográficos y lógicos.
- Utilice únicamente las métricas enumeradas en la API de administración de cuadrícula.
- Al probar una expresión utilizando la API de administración de cuadrícula, tenga en cuenta que una respuesta "exitosa" puede ser un cuerpo de respuesta vacío (sin que se active ninguna alerta). Para ver si la alerta realmente se activa, puede establecer temporalmente un umbral en un valor que espera que sea verdadero actualmente.

Por ejemplo, para probar la expresión `node_memory_MemTotal_bytes < 24000000000` , primero ejecutar `node_memory_MemTotal_bytes >= 0` y asegúrese de obtener los resultados esperados (todos los nodos devuelven un valor). Luego, cambie el operador y el umbral a los valores previstos y ejecute nuevamente. No hay resultados que indiquen que no hay alertas actuales para esta expresión.

- No asuma que una alerta personalizada está funcionando a menos que haya validado que la alerta se activa cuando se espera.

Pasos

1. Seleccione **ALERTAS > Reglas**.

Aparece la página Reglas de alerta.

2. Seleccione **Crear regla personalizada**.

Aparece el cuadro de diálogo Crear regla personalizada.

Create Custom Rule

Enabled

☒

Unique Name

Description

Recommended Actions
(optional)

Conditions

Minor

Major

Critical

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

Duration

5

minutes

Cancel

Save

3. Seleccione o desmarque la casilla de verificación **Habilitado** para determinar si esta regla de alerta está actualmente habilitada.

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 único	Un 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 está ocurriendo. La descripción es el mensaje de alerta que se muestra en la página de Alertas y en las notificaciones por correo electrónico. Las descripciones de las reglas de alerta pueden tener entre 1 y 128 caracteres.
Acciones recomendadas	Opcionalmente, las acciones recomendadas a tomar cuando se activa esta alerta. Introduzca las acciones recomendadas como texto simple (sin códigos de formato). Las acciones recomendadas para las reglas de alerta pueden tener entre 0 y 1024 caracteres.

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

Una expresión básica suele tener la forma:

```
[metric] [operator] [value]
```

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

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

```
node_memory_MemTotal_bytes < 24000000000
```

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

6. En el campo **Duración**, ingrese la cantidad de tiempo que una condición debe permanecer vigente continuamente antes de que se active la alerta y seleccione una unidad de tiempo.

Para activar una alerta inmediatamente cuando una condición se vuelve verdadera, ingrese **0**. Aumente este valor para evitar que condiciones temporales activen alertas.

El valor predeterminado es 5 minutos.

7. Seleccione **Guardar**.

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

Editar reglas de alerta

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

descripción y las acciones recomendadas.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Administrar alertas o permisos de acceso root"](#) .

Acerca de esta tarea

Al editar una regla de alerta predeterminada, puede cambiar las condiciones para alertas menores, mayores y críticas, así como la duración. Cuando edita 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 impida que se complete una operación crítica.

Pasos

1. Seleccione **ALERTAS > Reglas**.

Aparece la página Reglas de alerta.

2. Seleccione el botón de opción correspondiente a la regla de alerta que desea editar.
3. Seleccione **Editar regla**.

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

Edit Rule - Low installed node memory

Enabled ☒

Unique Name Low installed node memory

Description The amount of installed memory on a node is low.

Recommended Actions (optional)

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](#)

Conditions

Minor

Major

Critical

node_memory_MemTotal_bytes < 24000000000

node_memory_MemTotal_bytes <= 12000000000

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

Duration

2

minutes

Cancel

Save

4. Seleccione o desmarque la casilla de verificación **Habilitado** para determinar si esta regla de alerta está actualmente habilitada.

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 hasta que la alerta deje de aparecer como una alerta activa.



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

5. Para las reglas de alerta personalizadas, actualice la siguiente información según sea necesario.



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

Campo	Descripción
Nombre único	Un 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 está ocurriendo. La descripción es el mensaje de alerta que se muestra en la página de Alertas y en las notificaciones por correo electrónico. Las descripciones de las reglas de alerta pueden tener entre 1 y 128 caracteres.
Acciones recomendadas	Opcionalmente, las acciones recomendadas a tomar cuando se activa esta alerta. Introduzca las acciones recomendadas como texto simple (sin códigos de formato). Las acciones recomendadas para las reglas de alerta pueden tener entre 0 y 1024 caracteres.

- En la sección Condiciones, ingrese o actualice la expresión de Prometheus para uno o más de los niveles de gravedad de alerta.



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

Conditions ?

Minor	
Major	node_memory_MemTotal_bytes < 24000000000
Critical	node_memory_MemTotal_bytes <= 14000000000



Si actualiza las condiciones de 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 tener la forma:

```
[metric] [operator] [value]
```

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

Esta expresión hace 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
```

- En el campo **Duración**, ingrese la cantidad de tiempo que una condición debe permanecer vigente continuamente antes de que se active la alerta y seleccione la unidad de tiempo.

Para activar una alerta inmediatamente cuando una condición se vuelve verdadera, ingrese **0**. Aumente

este valor para evitar que condiciones temporales activen alertas.

El valor predeterminado es 5 minutos.

8. Seleccione **Guardar**.

Si editó una regla de alerta predeterminada, aparecerá **Predeterminado*** en la columna Tipo. Si deshabilitó una regla de alerta predeterminada o personalizada, aparecerá **Deshabilitado** en la columna **Estado**.

Deshabilitar reglas de alerta

Puede cambiar el estado habilitado/deshabilitado para una regla de alerta predeterminada o personalizada.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Administrar alertas o permisos de acceso root"](#).

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 detecte un problema subyacente hasta que impida que se complete una operación crítica.

Pasos

1. Seleccione **ALERTAS > Reglas**.

Aparece la página Reglas de alerta.

2. Seleccione el botón de opción correspondiente a la regla de alerta que desea deshabilitar o habilitar.

3. Seleccione **Editar regla**.

Aparece el cuadro de diálogo Editar regla.

4. Seleccione o desmarque la casilla de verificación **Habilitado** para determinar si esta regla de alerta está actualmente habilitada.

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 hasta que la alerta deje de mostrarse como una alerta activa.

5. Seleccione **Guardar**.

Deshabilitado aparece en la columna **Estado**.

Eliminar reglas de alerta personalizadas

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Administrar alertas o permisos de acceso root"](#) .

Pasos

1. Seleccione **ALERTAS > Reglas**.

Aparece la página Reglas de alerta.

2. Seleccione el botón de opción correspondiente a la regla de alerta personalizada que desea eliminar.

No se puede eliminar una regla de alerta predeterminada.

3. Seleccione **Eliminar regla personalizada**.

Aparece un cuadro de diálogo de confirmación.

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

Cualquier instancia activa de la alerta se resolverá en 10 minutos.

Administrar notificaciones de alerta

Configurar notificaciones SNMP para alertas

Si desea que StorageGRID envíe notificaciones SNMP cuando se producen alertas, debe habilitar el agente SNMP de StorageGRID y configurar uno o más destinos de captura.

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

Para aprender a configurar el agente SNMP, consulte ["Utilice la monitorización SNMP"](#) .

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

- Las trampas son notificaciones enviadas por el agente SNMP que no requieren reconocimiento por parte del sistema de administración. Las trampas sirven para notificar al sistema de administración que algo ha sucedido dentro de StorageGRID, como por ejemplo la activación de una alerta. Las trampas son compatibles con las tres versiones de SNMP.
- Los informes son similares a las trampas, pero requieren el reconocimiento del sistema de gestión. Si el agente SNMP no recibe un acuse de recibo dentro de un período de tiempo determinado, vuelve a enviar el informe hasta que recibe un acuse de recibo o se alcanza el valor máximo de reintentos. Los informes son compatibles con SNMPv2c y SNMPv3.

Las notificaciones de trampa e información 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. Ver ["Silenciar notificaciones de alerta"](#) .

Si su implementación de StorageGRID incluye varios nodos de administración, el nodo de administración principal es el remitente preferido para notificaciones de alerta, paquetes de AutoSupport y trampas e informes

SNMP. Si el nodo de administración principal deja de estar disponible, otros nodos de administración envían notificaciones temporalmente. Ver "[¿Qué es un nodo de administración?](#)".

Configurar notificaciones por correo electrónico para alertas

Si desea que se envíen notificaciones por correo electrónico cuando se produzcan alertas, debe proporcionar información sobre su servidor SMTP. También debe ingresar las direcciones de correo electrónico de los destinatarios de las notificaciones de alerta.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tú tienes el "[Administrar alertas o permisos de acceso root](#)".

Acerca de esta tarea

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

Si su implementación de StorageGRID incluye varios nodos de administración, el nodo de administración principal es el remitente preferido para notificaciones de alerta, paquetes de AutoSupport y trampas e informes SNMP. Si el nodo de administración principal deja de estar disponible, otros nodos de administración envían notificaciones temporalmente. Ver "[¿Qué es un nodo de administración?](#)".

Pasos

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

Aparece la página de configuración de correo electrónico.

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

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

3. En la sección Servidor de correo electrónico (SMTP), ingrese la información que StorageGRID necesita para acceder a su servidor SMTP.

Si su servidor SMTP requiere autenticación, deberá proporcionar un nombre de usuario y una contraseña.

Campo	Ingresar
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 su servidor SMTP requiere autenticación, ingrese el nombre de usuario para autenticarse.

Campo	Ingresar
Contraseña (opcional)	Si su servidor SMTP requiere autenticación, ingrese la contraseña para autenticarse.

4. En la sección Direcciones de correo electrónico, ingrese las direcciones de correo electrónico del remitente y de cada destinatario.

- a. Para la **Dirección de correo electrónico del remitente**, especifique una dirección de correo electrónico válida para usar como dirección de remitente para las notificaciones de alerta.

Por ejemplo: storagegrid-alerts@example.com

- b. En la sección Destinatarios, ingrese una dirección de correo electrónico para cada lista de correo electrónico o persona que debe recibir un correo electrónico cuando se produce una alerta.

Seleccione el icono más  para agregar destinatarios.

5. Si se requiere 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 CA que se utilizará para verificar la identidad del servidor SMTP.

Puede copiar y pegar el contenido en este campo o seleccionar **Explorar** y seleccionar el archivo.

Debe proporcionar un único archivo que contenga los certificados de cada autoridad de certificación (CA) emisora intermedia. El archivo debe contener cada uno de los archivos de certificado CA codificados en PEM, concatenados en el orden de la cadena de certificados.

- b. Seleccione la casilla de verificación **Enviar certificado de cliente** si su servidor de correo electrónico SMTP requiere que los remitentes de correo electrónico proporcionen certificados de cliente para la autenticación.

- c. En el campo **Certificado de cliente**, proporcione el certificado de cliente codificado en PEM para enviar al servidor SMTP.

Puede copiar y pegar el contenido en este campo o seleccionar **Explorar** y seleccionar el archivo.

- d. En el campo **Clave privada**, ingrese la clave privada para el certificado del cliente en codificación PEM sin cifrar.

Puede copiar y pegar el contenido en este campo o seleccionar **Explorar** y seleccionar el archivo.



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

6. En la sección Filtros, seleccione qué niveles de gravedad de alerta deben generar notificaciones por correo electrónico, a menos que se haya silenciado la regla para 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.

Gravedad	Descripción
Mayor, crítico	Se envía una notificación por correo electrónico cuando se cumple la condición principal o crítica de una regla de alerta. No se envían notificaciones para alertas menores.
Sólo crítico	Se envía una notificación por correo electrónico solo 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 su configuración de correo electrónico, realice estos pasos:

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

Aparece un mensaje de confirmación indicando que se envió un correo electrónico de prueba.

- b. Revise las bandejas de entrada de todos los destinatarios de correo electrónico y confirme que se recibió un correo electrónico de prueba.



Si no recibe el correo electrónico en unos minutos o si se activa la alerta **Error de notificación por correo electrónico**, verifique su configuración e inténtelo nuevamente.

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



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

8. Seleccione **Guardar**.

Enviar un correo electrónico de prueba no guarda su configuración. Debes seleccionar **Guardar**.

Se guardan las configuraciones de correo electrónico.

Información incluida en las notificaciones de alerta por correo electrónico

Después de configurar el servidor de correo electrónico SMTP, se envían notificaciones por correo electrónico a los destinatarios designados cuando se activa una alerta, a menos que la regla de alerta se suprima mediante un silencio. Ver "[Silenciar notificaciones de alerta](#)".

Las notificaciones por correo electrónico incluyen la siguiente información:

Low object data storage (6 alerts) 1

The space available for storing object data is low. 2

Recommended actions 3

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

DC1-S1-226

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

DC1-S2-227

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

Sent from: DC1-ADM1-225 5

Llamada	Descripción
1	El nombre de la alerta, seguido del número de instancias activas de esta alerta.
2	La descripción de la alerta.
3	¿Alguna acción recomendada 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 cuando se activó la regla de alerta y el nombre del trabajo y servicio afectados.
5	El nombre de host del nodo de administración que envió la notificación.

Cómo se agrupan las alertas

Para evitar que se envíe una cantidad excesiva de notificaciones por correo electrónico cuando se activan alertas, StorageGRID intenta agrupar varias alertas en la misma notificación.

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

Comportamiento	Ejemplo
Cada notificación de alerta se aplica solo a las alertas que tienen el mismo nombre. Si se activan dos alertas con nombres diferentes al mismo tiempo, 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 en un nodo específico, si se alcanzan los umbrales para más de un nivel de gravedad, se envía una notificación solo para la alerta más grave.	Se activa la alerta A y se alcanzan los umbrales de alerta menor, mayor y crítica. Se envía una notificación para la alerta crítica.
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.	- La alerta A se activa en el nodo 1 a las 08:00. No se envía ninguna notificación. - La alerta A se activa en el nodo 2 a las 08:01. No se envía ninguna notificación. - A las 08:02, se envía una notificación para informar 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 todas las alertas activas (alertas actuales que no han sido silenciadas), incluso si se informaron anteriormente.	- La alerta A se activa en el nodo 1 a las 08:00. Se envía una notificación a las 08:02. - La alerta A se activa en el nodo 2 a las 08:05. Se envía una segunda notificación a las 08:15 (10 minutos después). Se informan ambos nodos.
Si hay varias alertas actuales con el mismo nombre y una de esas alertas se resuelve, no se envía una nueva notificación si la alerta vuelve a ocurrir en el nodo para el cual se resolvió.	- La alerta A se activa para el nodo 1. Se envía una notificación. - La alerta A se activa para el nodo 2. Se envía una segunda notificación. - La alerta A se resuelve para el nodo 2, pero permanece activa para el nodo 1. - La alerta A se activa nuevamente para el nodo 2. No se envía ninguna notificación nueva porque la alerta todavía está activa para el nodo 1.
StorageGRID continúa enviando notificaciones por correo electrónico una vez cada 7 días hasta que se resuelvan todas las instancias de la alerta o se silencie la regla de alerta.	- La alerta A se activa para el nodo 1 el 8 de marzo. Se envía una notificación. - La alerta A no está resuelta o silenciada. Se envían notificaciones adicionales el 15 de marzo, el 22 de marzo, el 29 de marzo, etc.

Solucionar problemas de notificaciones de alerta por correo electrónico

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Administrar alertas o permisos de acceso root"](#) .

Pasos

1. Verifique su configuración.
 - a. Seleccione **ALERTAS > Configuración de correo electrónico**.
 - b. Verifique que la configuración del servidor de correo electrónico (SMTP) sea correcta.
 - c. Verifique que haya especificado direcciones de correo electrónico válidas para los destinatarios.
2. Revise su filtro de spam y asegúrese de que el correo electrónico no haya sido enviado a la carpeta de correo no deseado.
3. Pídale a su administrador de correo electrónico que confirme que los correos electrónicos de la dirección del remitente no estén siendo bloqueados.
4. Recopile un archivo de registro para el nodo de administración y luego comuníquese con el soporte técnico.

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

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

Silenciar notificaciones de alerta

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Administrar alertas o permisos de acceso root"](#) .

Acerca de esta tarea

Puede silenciar las reglas de alerta en toda la red, en un solo sitio o en un solo nodo y para uno o más niveles de gravedad. 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, los silencios también suprimen las trampas e informes SNMP.



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

Pasos

1. Seleccione **ALERTAS > Silencios**.

Aparece la página Silencios.

Silences

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

Create

Edit

Remove

Alert Rule	Description	Severity	Time Remaining	Nodes
No results found.				

2. Seleccione **Crear**.

Aparece el cuadro de diálogo Crear silencio.

Create Silence

Alert Rule

Description (optional)

Duration

Minutes

Severity

☐ Minor only

☐ Minor, major

☐ Minor, major, critical

Nodes

☐ StorageGRID Deployment

☐ Data Center 1

☐ DC1-ADM1

☐ DC1-G1

☐ DC1-S1

☐ DC1-S2

☐ DC1-S3

Cancel

Save

3. Seleccione o ingrese la siguiente información:

Campo	Descripción
Regla de alerta	El nombre de la regla de alerta que desea silenciar. Puede seleccionar cualquier regla de alerta predeterminada o personalizada, incluso si la regla de alerta está deshabilitada. 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, describe el propósito de este silencio.
Duración	¿Cuánto tiempo quieres que este silencio permanezca vigente, en minutos, horas o días? Un silencio puede durar desde 5 minutos hasta 1.825 días (5 años). Nota: No debes silenciar una regla de alerta durante un período prolongado. 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 necesite usar un silencio extendido si una alerta se activa mediante una configuración intencional específica, como podría ser el caso de las alertas Enlace del dispositivo de servicios inactivo y Enlace del dispositivo de almacenamiento inactivo.
Gravedad	¿Qué nivel o niveles de alerta se deben silenciar? Si la alerta se activa en uno de los niveles de gravedad seleccionados, no se envían notificaciones.
Nodos	¿A qué nodo o nodos quieres que se aplique este silencio? Puede suprimir una regla de alerta o todas las reglas en toda la red, un solo sitio o un solo nodo. Si selecciona toda la cuadrícula, el silencio se aplica a todos los sitios y todos los nodos. Si selecciona un sitio, el silencio se aplica solo a los nodos de ese sitio. Nota: No puedes seleccionar más de un nodo o más de un sitio para cada silencio. Debe crear silencios adicionales si desea suprimir la misma regla de alerta en más de un nodo o más de un sitio al mismo tiempo.

4. Seleccione **Guardar**.

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

Opción	Descripción
Editar un silencio	a. Seleccione ALERTAS > Silencios. b. Desde la tabla, seleccione el botón de opción correspondiente al silencio que desea editar. c. Seleccione Editar. d. Cambie la descripción, la cantidad de tiempo restante, las severidades seleccionadas o el nodo afectado. e. Seleccione Guardar.

Opción	Descripción
Eliminar un silencio	a. Seleccione ALERTAS > Silencios. b. Desde la tabla, seleccione el botón de opción correspondiente al silencio que desea eliminar. c. Seleccione Eliminar. d. Seleccione Aceptar para confirmar que desea eliminar este silencio. Nota: Ahora se enviarán notificaciones cuando se active esta alerta (a menos que se suprima mediante otro silencio). Si esta alerta está activada actualmente, es posible que pasen algunos minutos hasta que se envíen las notificaciones por correo electrónico o SNMP y hasta que se actualice la página de Alertas.

Información relacionada

["Configurar el agente SNMP"](#)

Referencia de alertas

Esta referencia enumera las alertas predeterminadas que aparecen en el Administrador de cuadrícula. Las acciones recomendadas están en el mensaje de alerta que recibe.

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

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

Alertas de electrodomésticos

Nombre de la alerta	Descripción
La batería del aparato está caducada	La batería del controlador de almacenamiento del aparato ha expirado.
La batería del aparato falló	La batería del controlador de almacenamiento del aparato ha fallado.
La batería del aparato tiene capacidad de aprendizaje insuficiente	La batería del controlador de almacenamiento del aparato no tiene suficiente capacidad de aprendizaje.
La batería del electrodoméstico está a punto de caducar	La batería del controlador de almacenamiento del aparato está próxima a agotarse.
Batería del aparato retirada	Falta la batería en el controlador de almacenamiento del aparato.
La batería del aparato está demasiado caliente	La batería del controlador de almacenamiento del aparato está sobrecalentada.

Nombre de la alerta	Descripción
Error de comunicación del BMC del dispositivo	Se ha perdido la comunicación con el controlador de administración de la placa base (BMC).
Se detectó un fallo en el dispositivo de arranque del dispositivo	Se detectó un problema con el dispositivo de arranque en el dispositivo.
Falló el dispositivo de copia de seguridad de caché del dispositivo	Ha fallado un dispositivo de copia de seguridad de caché persistente.
Capacidad insuficiente del dispositivo de copia de seguridad de caché del dispositivo	No hay suficiente capacidad en el dispositivo de copia de seguridad de caché.
Dispositivo de copia de seguridad de caché del dispositivo protegido contra escritura	Un dispositivo de copia de seguridad de caché está protegido contra escritura.
Desajuste del tamaño de la memoria caché del dispositivo	Los dos controladores del dispositivo tienen diferentes tamaños de caché.
Fallo de la batería CMOS del dispositivo	Se detectó un problema con la batería CMOS del dispositivo.
La temperatura del chasis del controlador de cómputo del dispositivo es demasiado alta	La temperatura del controlador de cómputo en un dispositivo StorageGRID ha superado un umbral nominal.
La temperatura de la CPU del controlador de cómputo del dispositivo es demasiado alta	La temperatura de la CPU en el controlador de cómputo de un dispositivo StorageGRID ha superado un umbral nominal.
El controlador de cómputo del dispositivo necesita atención	Se ha detectado una falla de hardware en el controlador de cómputo de un dispositivo StorageGRID .
La fuente de alimentación del controlador de cómputo del dispositivo A tiene un problema	La fuente de alimentación A en el controlador de cálculo tiene un problema.
La fuente de alimentación del controlador de cómputo del dispositivo B tiene un problema	La fuente de alimentación B en el controlador de cálculo tiene un problema.
El servicio de monitorización del hardware de cómputo del dispositivo se ha detenido	El servicio que supervisa el estado del hardware de almacenamiento se ha estancado.

Nombre de la alerta	Descripción
La unidad DAS del dispositivo excede el límite de datos escritos por día	Se escribe una cantidad excesiva de datos en una unidad cada día, lo que podría anular su garantía.
Se detectó un fallo en la unidad DAS del dispositivo	Se detectó un problema con una unidad de almacenamiento conectada directamente (DAS) en el dispositivo.
Luz de localización de la unidad DAS del dispositivo encendida	La luz localizadora de unidad para una o más unidades de almacenamiento de conexión directa (DAS) en un nodo de almacenamiento del dispositivo está encendida.
Reconstrucción de la unidad DAS del dispositivo	Se está reconstruyendo una unidad de almacenamiento conectada directamente (DAS). Esto es lo esperado si fue reemplazado o quitado/reinsertado recientemente.
Se detectó una falla en el ventilador del aparato	Se detectó un problema con una unidad de ventilador en el aparato.
Se detectó un fallo en el canal de fibra del dispositivo	Se ha detectado un problema de enlace de canal de fibra entre el controlador de almacenamiento del dispositivo y el controlador de cómputo
Falla del puerto HBA del canal de fibra del dispositivo	Un puerto HBA de canal de fibra está fallando o ha fallado.
Las unidades de caché flash del dispositivo no son óptimas	Las unidades utilizadas para la caché SSD no son óptimas.
Interconexión del aparato/recipiente de batería retirado	Falta el recipiente de interconexión/batería.
Falta el puerto LACP del dispositivo	Un puerto en un dispositivo StorageGRID no participa en el enlace LACP.
Se detectó un fallo en la NIC del dispositivo	Se detectó un problema con una tarjeta de interfaz de red (NIC) en el dispositivo.
La fuente de alimentación general del aparato se degradó	La energía de un dispositivo StorageGRID se ha desviado del voltaje operativo recomendado.
Advertencia crítica del SSD del dispositivo	Un dispositivo SSD informa una advertencia crítica.
Fallo del controlador de almacenamiento del dispositivo A	El controlador de almacenamiento A en un dispositivo StorageGRID ha fallado.

Nombre de la alerta	Descripción
Fallo del controlador de almacenamiento del dispositivo B	El controlador de almacenamiento B en un dispositivo StorageGRID ha fallado.
Falla de la unidad del controlador de almacenamiento del dispositivo	Una o más unidades en un dispositivo StorageGRID han fallado o no están en condiciones óptimas.
Problema de hardware del controlador de almacenamiento del dispositivo	El software SANtricity informa "Requiere atención" para un componente en un dispositivo StorageGRID .
Falla en la fuente de alimentación del controlador de almacenamiento del dispositivo A	La fuente de alimentación A en un dispositivo StorageGRID se ha desviado del voltaje operativo recomendado.
Falla de la fuente de alimentación B del controlador de almacenamiento del dispositivo	La fuente de alimentación B en un dispositivo StorageGRID se ha desviado del voltaje operativo recomendado.
El servicio de monitorización del hardware de almacenamiento del dispositivo se ha estancado	El servicio que supervisa el estado del hardware de almacenamiento se ha estancado.
Estantes de almacenamiento de electrodomésticos degradados	El estado de uno de los componentes en el estante de almacenamiento de un dispositivo de almacenamiento está degradado.
Se excedió la temperatura del aparato	Se ha excedido la temperatura nominal o máxima del controlador de almacenamiento del aparato.
Sensor de temperatura del aparato retirado	Se ha quitado un sensor de temperatura.
Error de arranque seguro UEFI del dispositivo	Un dispositivo no se ha iniciado de forma segura.
La E/S del disco es muy lenta	Una entrada/salida de disco muy lenta podría estar afectando el rendimiento de la red.
Se detectó una falla en el ventilador del dispositivo de almacenamiento	Se detectó un problema con una unidad de ventilador en el controlador de almacenamiento de un dispositivo.
La conectividad del dispositivo de almacenamiento se ha degradado	Hay un problema con una o más conexiones entre el controlador de cómputo y el controlador de almacenamiento.
Dispositivo de almacenamiento inaccesible	No se puede acceder a un dispositivo de almacenamiento.

Alertas de auditoría y syslog

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

Alertas de cubo

Nombre de la alerta	Descripción
El depósito FabricPool tiene una configuración de consistencia de depósito no compatible	Un bucket de FabricPool utiliza el nivel de consistencia de sitio disponible o fuerte, que no es compatible.
El bucket FabricPool tiene una configuración de versiones no compatible	Un bucket de FabricPool tiene habilitado el control de versiones o el bloqueo de objetos S3, que no son compatibles.

Alertas de Cassandra

Nombre de la alerta	Descripción
Error del autocompactador Cassandra	El autocompactador Cassandra ha experimentado un error.
Las métricas del autocompactador Cassandra están desactualizadas	Las métricas que describen el autocompactador Cassandra están desactualizadas.
Error de comunicación de Cassandra	Los nodos que ejecutan el servicio Cassandra tienen problemas para comunicarse entre sí.
Compactaciones de Cassandra sobrecargadas	El proceso de compactación de Cassandra está sobrecargado.
Error de escritura de gran tamaño en Cassandra	Un proceso interno de StorageGRID envió una solicitud de escritura a Cassandra que era demasiado grande.

Nombre de la alerta	Descripción
Las métricas de reparación de Cassandra están desactualizadas	Las métricas que describen los trabajos de reparación de Cassandra están desactualizadas.
El progreso de la reparación de Cassandra es lento	El progreso de las reparaciones de la base de datos de Cassandra es lento.
Servicio de reparación de Cassandra no disponible	El servicio de reparación de Cassandra no está disponible.
Corrupción en la tabla de Cassandra	Cassandra ha detectado corrupción en la tabla. Cassandra se reinicia automáticamente si detecta corrupción en la tabla.

Alertas del grupo de almacenamiento en la nube

Nombre de la alerta	Descripción
Error de conectividad del grupo de almacenamiento en la nube	La comprobación del estado de los grupos de almacenamiento en la nube detectó uno o más errores nuevos.
Vencimiento de la certificación de entidad final de IAM Roles Anywhere	El certificado de entidad final de IAM Roles Anywhere está a punto de expirar.

Alertas de replicación entre redes

Nombre de la alerta	Descripción
Fallo permanente de replicación entre redes	Se produjo un error de replicación entre redes que requiere la intervención del usuario para resolverlo.
Recursos de replicación entre redes no disponibles	Las solicitudes de replicación entre redes están pendientes porque un recurso no está disponible.

alertas DHCP

Nombre de la alerta	Descripción
La concesión DHCP ha expirado	La concesión DHCP en una interfaz de red ha expirado.
La concesión de DHCP expirará pronto	La concesión DHCP en una interfaz de red expirará pronto.
Servidor DHCP no disponible	El servidor DHCP no está disponible.

Alertas de depuración y seguimiento

Nombre de la alerta	Descripción
Impacto en el rendimiento de la depuración	Cuando el modo de depuración está habilitado, el rendimiento del sistema podría verse afectado negativamente.
Configuración de seguimiento habilitada	Cuando la configuración de seguimiento está habilitada, el rendimiento del sistema podría verse afectado negativamente.

Alertas por correo electrónico y AutoSupport

Nombre de la alerta	Descripción
El mensaje de AutoSupport no se pudo enviar	No se pudo enviar el mensaje de AutoSupport más reciente.
Error en la resolución del nombre de dominio	El nodo StorageGRID no ha podido resolver los nombres de dominio.
Error en la notificación por correo electrónico	No se pudo enviar la notificación por correo electrónico para una alerta.
Errores de información de SNMP	Errores al enviar notificaciones de información SNMP a un destino de trampa.
Se detectó inicio de sesión SSH o de consola	En las últimas 24 horas, un usuario inició sesión con la consola web o SSH.

Alertas de codificación de borrado (EC)

Nombre de la alerta	Descripción
Fallo de reequilibrio de la CE	El procedimiento de reequilibrio de la CE ha fallado o se ha detenido.
Fallo de reparación de CE	Un trabajo de reparación de datos de EC ha fallado o se ha detenido.
Reparación de CE estancada	Un trabajo de reparación de datos de la CE se ha estancado.
Error de verificación del fragmento codificado por borrado	Los fragmentos codificados por borrado ya no se pueden verificar. Es posible que los fragmentos corruptos no puedan repararse.

Alertas de vencimiento de certificados

Nombre de la alerta	Descripción
Vencimiento del certificado de CA del proxy de administración	Uno o más certificados en el paquete CA del servidor proxy de administración están a punto de expirar.

Nombre de la alerta	Descripción
Caducidad del certificado de cliente	Uno o más certificados de cliente están a punto de caducar.
Vencimiento del certificado de servidor global para S3 y Swift	El certificado de servidor global para S3 y Swift está a punto de expirar.
Vencimiento del certificado del punto final del balanceador de carga	Uno o más certificados de punto final del equilibrador de carga están a punto de caducar.
Caducidad del certificado del servidor para la interfaz de administración	El certificado del servidor utilizado para la interfaz de administración está a punto de caducar.
Vencimiento del certificado de CA de syslog externo	El certificado de la autoridad de certificación (CA) utilizado para firmar el certificado del servidor syslog externo está a punto de caducar.
Caducidad del certificado del cliente de syslog externo	El certificado de cliente para un servidor syslog externo está a punto de caducar.
Caducidad del certificado del servidor syslog externo	El certificado de servidor presentado por el servidor syslog externo está a punto de expirar.

Alertas de red Grid

Nombre de la alerta	Descripción
Desajuste de MTU de la red de cuadrícula	La configuración de MTU para la interfaz de red de cuadrícula (eth0) difiere significativamente entre los nodos de la cuadrícula.

Alertas de federación de red

Nombre de la alerta	Descripción
Vencimiento del certificado de federación de red	Uno o más certificados de federación de red están a punto de expirar.
Error de conexión de la federación de red	La conexión de la federación de red entre la red local y la red remota no funciona.

Alertas de alto uso o alta latencia

Nombre de la alerta	Descripción
Alto uso del montón de Java	Se está utilizando un alto porcentaje del espacio del montón de Java.

Nombre de la alerta	Descripción
Alta latencia para consultas de metadatos	El tiempo promedio para las consultas de metadatos de Cassandra es demasiado largo.

Alertas de federación de identidad

Nombre de la alerta	Descripción
Error de sincronización de la federación de identidad	No se pueden sincronizar grupos y usuarios federados desde la fuente de identidad.
Error de sincronización de la federación de identidades para un inquilino	No se pueden sincronizar grupos y usuarios federados desde la fuente de identidad configurada por un inquilino.

Alertas de gestión del ciclo de vida de la información (ILM)

Nombre de la alerta	Descripción
La colocación del ILM es inalcanzable	No se puede lograr una instrucción de ubicación en una regla ILM para ciertos objetos.
Tasa de escaneo ILM baja	La velocidad de escaneo ILM está establecida en menos de 100 objetos/segundo.

Alertas del servidor de administración de claves (KMS)

Nombre de la alerta	Descripción
Vencimiento del certificado de CA de KMS	El certificado de la autoridad de certificación (CA) utilizado para firmar el certificado del servidor de administración de claves (KMS) está a punto de caducar.
Caducidad del certificado del cliente KMS	El certificado de cliente para un servidor de administración de claves está a punto de caducar
La configuración de KMS no se pudo cargar	La configuración del servidor de administración de claves existe, pero no se pudo cargar.
Error de conectividad KMS	Un nodo del dispositivo no pudo conectarse al servidor de administración de claves de su sitio.
No se encontró el nombre de la clave de cifrado KMS	El servidor de administración de claves configurado no tiene una clave de cifrado que coincida con el nombre proporcionado.
Error en la rotación de la clave de cifrado KMS	Todos los volúmenes del dispositivo se descifraron correctamente, pero uno o más volúmenes no pudieron rotar a la clave más reciente.

Nombre de la alerta	Descripción
KMS no está configurado	No existe ningún servidor de administración de claves para este sitio.
La clave KMS no pudo descifrar un volumen del dispositivo	No se pudieron descifrar uno o más volúmenes de un dispositivo con cifrado de nodo habilitado con la clave KMS actual.
Caducidad del certificado del servidor KMS	El certificado de servidor utilizado por el servidor de administración de claves (KMS) está a punto de caducar.
Fallo de conectividad del servidor KMS	Un nodo del dispositivo no pudo conectarse a uno o más servidores en el clúster de servidores de administración de claves de su sitio.

Alertas del balanceador de carga

Nombre de la alerta	Descripción
Conexiones elevadas de balanceador de carga de solicitud cero	Un porcentaje elevado de conexiones a puntos finales del balanceador de carga se desconectaron sin realizar solicitudes.

Alertas de desfase del reloj local

Nombre de la alerta	Descripción
Gran desplazamiento horario del reloj local	El desfase entre el reloj local y la hora del Protocolo de tiempo de red (NTP) es demasiado grande.

Alertas de poca memoria o poco espacio

Nombre de la alerta	Descripción
Baja capacidad del disco de registro de auditoría	El espacio disponible para los registros de auditoría es bajo. Si no se aborda esta condición, las operaciones de S3 o Swift podrían fallar.
Memoria de nodo baja disponible	La cantidad de RAM disponible en un nodo es baja.
Poco espacio libre para almacenamiento de piscina	El espacio disponible para almacenar datos de objetos en el nodo de almacenamiento es bajo.
Poca memoria de nodo instalada	La cantidad de memoria instalada en un nodo es baja.
Almacenamiento de metadatos bajo	El espacio disponible para almacenar metadatos de objetos es bajo.
Capacidad de disco de métricas bajas	El espacio disponible para la base de datos de métricas es bajo.

Nombre de la alerta	Descripción
Almacenamiento de datos de objetos reducido	El espacio disponible para almacenar datos de objetos es bajo.
Anulación de marca de agua de solo lectura baja	La anulación de la marca de agua de solo lectura suave del volumen de almacenamiento es menor que la marca de agua mínima optimizada para un nodo de almacenamiento.
Baja capacidad del disco raíz	El espacio disponible en el disco raíz es bajo.
Baja capacidad de datos del sistema	El espacio disponible para /var/local es bajo. Si no se aborda esta condición, las operaciones de S3 o Swift podrían fallar.
Poco espacio libre en el directorio temporal	El espacio disponible en el directorio /tmp es bajo.

Alertas de nodo o red de nodos

Nombre de la alerta	Descripción
Uso de recepción de red de administración	El uso de recepción en la red de administración es alto.
Uso de transmisión de la red de administración	El uso de transmisión en la red de administración es alto.
Error en la configuración del firewall	No se pudo aplicar la configuración del firewall.
Puntos finales de la interfaz de administración en modo de respaldo	Todos los puntos finales de la interfaz de administración han estado recurriendo a los puertos predeterminados durante demasiado tiempo.
Error de conectividad de red del nodo	Se han producido errores al transferir datos entre nodos.
Error de trama de recepción de red de nodo	Un alto porcentaje de los marcos de red recibidos por un nodo tenían errores.
El nodo no está sincronizado con el servidor NTP	El nodo no está sincronizado con el servidor de protocolo de tiempo de red (NTP).
Nodo no bloqueado con el servidor NTP	El nodo no está bloqueado a un servidor de protocolo de tiempo de red (NTP).
Red de nodos que no son dispositivos inactiva	Uno o más dispositivos de red están inactivos o desconectados.

Nombre de la alerta	Descripción
El enlace del dispositivo de servicios está inactivo en la red de administración	La interfaz del dispositivo a la red de administración (eth1) está inactiva o desconectada.
El enlace del dispositivo de servicios no funciona en el puerto 1 de la red de administración	El puerto de red de administración 1 del dispositivo está inactivo o desconectado.
El enlace del dispositivo de servicios está inactivo en la red del cliente	La interfaz del dispositivo a la red del cliente (eth2) está inactiva o desconectada.
Enlace del dispositivo de servicios inactivo en el puerto de red 1	El puerto de red 1 del dispositivo está inactivo o desconectado.
Enlace del dispositivo de servicios inactivo en el puerto de red 2	El puerto de red 2 del dispositivo está inactivo o desconectado.
Enlace del dispositivo de servicios inactivo en el puerto de red 3	El puerto de red 3 del dispositivo está inactivo o desconectado.
Enlace del dispositivo de servicios inactivo en el puerto de red 4	El puerto de red 4 del dispositivo está inactivo o desconectado.
El enlace del dispositivo de almacenamiento está inactivo en la red de administración	La interfaz del dispositivo a la red de administración (eth1) está inactiva o desconectada.
Enlace del dispositivo de almacenamiento inactivo en el puerto 1 de la red de administración	El puerto de red de administración 1 del dispositivo está inactivo o desconectado.
Enlace del dispositivo de almacenamiento inactivo en la red del cliente	La interfaz del dispositivo a la red del cliente (eth2) está inactiva o desconectada.
Enlace del dispositivo de almacenamiento inactivo en el puerto de red 1	El puerto de red 1 del dispositivo está inactivo o desconectado.
Enlace del dispositivo de almacenamiento inactivo en el puerto de red 2	El puerto de red 2 del dispositivo está inactivo o desconectado.

Nombre de la alerta	Descripción
Enlace del dispositivo de almacenamiento inactivo en el puerto de red 3	El puerto de red 3 del dispositivo está inactivo o desconectado.
Enlace del dispositivo de almacenamiento inactivo en el puerto de red 4	El puerto de red 4 del dispositivo está inactivo o desconectado.
El nodo de almacenamiento no se encuentra en el estado de almacenamiento deseado	El servicio LDR en un nodo de almacenamiento no puede pasar al estado deseado debido a un error interno o un problema relacionado con el volumen
Uso de la conexión TCP	La cantidad de conexiones TCP en este nodo se está acercando al número máximo que se puede rastrear.
No se puede comunicar con el nodo	Uno o más servicios no responden o no se puede acceder al nodo.
Reinicio inesperado del nodo	Un nodo se reinició inesperadamente en las últimas 24 horas.

Alertas de objetos

Nombre de la alerta	Descripción
Falló la comprobación de existencia del objeto	La tarea de verificación de existencia del objeto ha fallado.
La comprobación de existencia del objeto se ha estancado	El trabajo de verificación de existencia del objeto se ha estancado.
Objetos perdidos	Se han perdido uno o más objetos de la cuadrícula.
El tamaño del objeto S3 PUT es demasiado grande	Un cliente está intentando realizar una operación PUT de objeto que excede los límites de tamaño de S3.
Se detectó un objeto corrupto no identificado	Se encontró un archivo en el almacenamiento de objetos replicados que no se pudo identificar como un objeto replicado.

Alertas de servicios de la plataforma

Nombre de la alerta	Descripción
Servicios de la Plataforma con capacidad de solicitudes pendientes baja	El número de solicitudes pendientes de Servicios de Plataforma se está acercando a su capacidad.

Nombre de la alerta	Descripción
Servicios de plataforma no disponibles	Hay muy pocos nodos de almacenamiento con el servicio RSM en ejecución o disponibles en un sitio.

Alertas de volumen de almacenamiento

Nombre de la alerta	Descripción
El volumen de almacenamiento necesita atención	Un volumen de almacenamiento está fuera de línea y necesita atención.
Es necesario restaurar el volumen de almacenamiento	Se ha recuperado un volumen de almacenamiento y es necesario restaurarlo.
Volumen de almacenamiento sin conexión	Un volumen de almacenamiento ha estado fuera de línea durante más de 5 minutos.
Se intentó volver a montar el volumen de almacenamiento	Un volumen de almacenamiento estaba fuera de línea y activó un remontaje automático. Esto podría indicar un problema con la unidad o errores del sistema de archivos.
La restauración de volumen no pudo iniciar la reparación de datos replicados	No se pudo iniciar automáticamente la reparación de datos replicados para un volumen reparado.

Alertas de servicios de StorageGRID

Nombre de la alerta	Descripción
Servicio nginx que utiliza la configuración de respaldo	La configuración del servicio nginx no es válida. Ahora se utiliza la configuración anterior.
Servicio nginx-gw que utiliza la configuración de respaldo	La configuración del servicio nginx-gw no es válida. Ahora se utiliza la configuración anterior.
Es necesario reiniciar para deshabilitar FIPS	La política de seguridad no requiere el modo FIPS, pero el módulo de seguridad criptográfica de NetApp está habilitado.
Es necesario reiniciar para habilitar FIPS	La política de seguridad requiere el modo FIPS, pero el módulo de seguridad criptográfica de NetApp está deshabilitado.
Servicio SSH que utiliza la configuración de respaldo	La configuración del servicio SSH no es válida. Ahora se utiliza la configuración anterior.

Alertas para inquilinos

Nombre de la alerta	Descripción
Alto uso de la cuota de inquilinos	Se está utilizando un alto porcentaje del espacio de cuota. Esta regla está deshabilitada de forma predeterminada porque podría generar demasiadas notificaciones.

Métricas de Prometheus de uso común

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

También puedes [obtener una lista completa de todas las métricas](#) .

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

¿Qué son las métricas de Prometheus?

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

¿Dónde se utilizan las métricas de Prometheus?

Las métricas recopiladas por Prometheus se utilizan en varios lugares del Administrador de cuadrícula:

- **Página de Nodos:** Los gráficos y cuadros en las pestañas disponibles en la página de Nodos utilizan la herramienta de visualización Grafana para mostrar las métricas de series de tiempo recopiladas por Prometheus. Grafana muestra datos de series temporales en formatos de gráficos y diagramas, mientras que Prometheus sirve como fuente de datos de back-end.



- **Alertas:** Las alertas se activan en niveles de gravedad específicos cuando las condiciones de las reglas de alerta que utilizan métricas de Prometheus se evalúan como verdaderas.
- **API de administración de red:** puede usar las métricas de Prometheus en reglas de alerta personalizadas o con herramientas de automatización externas para monitorear su sistema StorageGRID . Una lista completa de las métricas de Prometheus está disponible en la API de administración de

cuadrícula. (Desde la parte superior del Administrador de cuadrícula, seleccione el ícono de ayuda y seleccione **Documentación de API > métricas**). Si bien hay más de mil métricas disponibles, solo se requiere una cantidad relativamente pequeña para monitorear las operaciones más críticas de StorageGRID .



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

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



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

Lista de métricas más comunes

La siguiente lista contiene las métricas de Prometheus más utilizadas.



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

total de notificaciones fallidas del administrador de alertas

El número total de notificaciones de alerta fallidas.

bytes disponibles del sistema de archivos del nodo

La cantidad de espacio del sistema de archivos disponible para usuarios no root en bytes.

memoria_del_nodo_bytes_de_memoria_disponibles

Campo de información de memoria MemAvailable_bytes.

operador de red de nodo

Valor portador de `/sys/class/net/iface`.

total de errores de recepción de red de nodos

Estadísticas del dispositivo de red `receive_errs`.

total de errores de transmisión de la red de nodos

Estadísticas del dispositivo de red `transmit_errs`.

storagegrid_administrativamente_inactivo

El nodo no está conectado a la red por una razón esperada. Por ejemplo, el nodo, o los servicios en el nodo, se han apagado correctamente, el nodo se está reiniciando o se está actualizando el software.

estado del hardware del controlador de cómputo del dispositivo de la red de almacenamiento

El estado del hardware del controlador de cómputo en un dispositivo.

discos fallidos del dispositivo storagegrid

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

estado del hardware del controlador de almacenamiento del dispositivo storagegrid

El estado general del hardware del controlador de almacenamiento en un dispositivo.

cubos y contenedores de contenido de la red de almacenamiento

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

objetos de contenido de la cuadrícula de almacenamiento

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

objetos de contenido de la red de almacenamiento 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_sesiones http_iniciadas_intentadas

El número total de sesiones HTTP que se han intentado en un nodo de almacenamiento.

storagegrid_http_sesiones_entrantes_actualmente_establecidas

La cantidad de sesiones HTTP que están actualmente activas (abiertas) en el nodo de almacenamiento.

storagegrid_http_sessions_incoming_failed

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

storagegrid_http_sesiones_entrantes_exitosas

El número total de sesiones HTTP que se han completado correctamente.

storagegrid_ilm_en espera de objetos de fondo

El número total de objetos en este nodo que esperan la evaluación ILM del escaneo.

storagegrid_ilm_en espera de objetos de evaluación del cliente por segundo

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

storagegrid_ilm_en espera de objetos de cliente

La cantidad total de objetos en este nodo que esperan la evaluación de ILM de las operaciones del cliente (por ejemplo, ingesta).

storagegrid_ilm_en espera del total de objetos

El número total de objetos en espera de evaluación ILM.

storagegrid_ilm_scan_objetos_por_segundo

La velocidad a la que los objetos propiedad de este nodo se escanean y se ponen en cola para ILM.

período de escaneo de película de la cuadrícula de almacenamiento, minutos estimados

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

Nota: Un escaneo completo no garantiza que ILM se haya aplicado a todos los objetos propiedad de este nodo.

tiempo de caducidad del certificado del punto final del equilibrador de carga de la red de almacenamiento

El tiempo de expiración del certificado del punto final del balanceador de carga en segundos desde la época.

consultas_de_metadatos_de_la_red_de_almacenamiento_latencia_promedio_milisegundos

El tiempo promedio necesario para ejecutar una consulta en el almacén de metadatos a través de este servicio.

red de almacenamiento_grid_bytes_recibidos

La cantidad total de datos recibidos desde la instalación.

bytes transmitidos por la red de almacenamiento

La cantidad total de datos enviados desde la instalación.

porcentaje de utilización de CPU del nodo de la red de almacenamiento

El porcentaje de tiempo de CPU disponible que actualmente utiliza este servicio. Indica qué tan ocupado está el servicio. La cantidad de tiempo de CPU disponible depende de la cantidad de CPU del servidor.

desplazamiento de origen de tiempo elegido por la red de almacenamiento ntp en milisegundos

Desplazamiento sistemático del tiempo proporcionado por una fuente de tiempo elegida. El desplazamiento se introduce cuando el retraso para llegar a una fuente de tiempo no es igual al tiempo requerido para que la fuente de tiempo llegue al cliente NTP.

red de almacenamiento_ntp_bloqueada

El nodo no está bloqueado a un servidor de Protocolo de tiempo de red (NTP).

storagegrid_s3_data_transfers_bytes_ingested

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

storagegrid_s3_data_transfers_bytes_retrieved

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

storagegrid_s3_operations_failed

El número total de operaciones S3 fallidas (códigos de estado HTTP 4xx y 5xx), excluidas aquellas causadas por fallas de autorización S3.

storagegrid_s3_operations_successful

El número total de operaciones S3 exitosas (código de estado HTTP 2xx).

storagegrid_s3_operations_unauthorized

El número total de operaciones S3 fallidas que son el resultado de una falla de autorización.

días de vencimiento del certificado de la interfaz de gestión de certificados del servidor de StorageGrid

El número de días antes de que caduque el certificado de la interfaz de administración.

días de vencimiento del certificado de los puntos finales de la API de almacenamiento del certificado de servidor de la red de almacenamiento

La cantidad de días antes de que caduque el certificado de la API de almacenamiento de objetos.

segundos de CPU del servicio de red de almacenamiento

La cantidad acumulada de tiempo que este servicio ha utilizado la CPU desde su instalación.

uso de memoria del servicio de red de almacenamiento en bytes

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

red de servicio de almacenamiento_red_bytes_recibidos

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

red de servicio de almacenamiento_red_bytes_transmitidos

La cantidad total de datos enviados por este servicio.

reinicios del servicio de storagegrid

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

segundos de tiempo de ejecución del servicio de la red de almacenamiento

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

tiempo de actividad del servicio de la red de almacenamiento en segundos

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

estado_de_almacenamiento_actual_de_la_red_de_almacenamiento

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

- 10 = Desconectado
- 15 = Mantenimiento
- 20 = Solo lectura
- 30 = En línea

estado de almacenamiento de la red de almacenamiento

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

- 0 = Sin errores
- 10 = En transición
- 20 = Espacio libre insuficiente
- 30 = Volumen(es) no disponible(s)
- 40 = Error

datos_de_utilización_de_almacenamiento_en_la_red_de_almacenamiento_en_bytes

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

metadatos de utilización de almacenamiento de la red de almacenamiento permitidos

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

metadatos_bytes_de_utilización_de_almacenamiento_en_la_red_de_almacenamiento

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

Utilización de almacenamiento en la red de almacenamiento, espacio total en bytes

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

Utilización de almacenamiento en la red de almacenamiento, espacio utilizable en bytes

La cantidad total de espacio de almacenamiento de objetos restante. Se calcula sumando la cantidad de espacio disponible para todos los almacenes de objetos en el nodo de almacenamiento.

transferencias de datos de storagegrid_swift_bytes_ingridos

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

transferencias de datos de storagegrid_swift_bytes_recuperados

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

operaciones de storagegrid_swift_fallidas

El número total de operaciones Swift fallidas (códigos de estado HTTP 4xx y 5xx), excluidas aquellas causadas por fallas de autorización Swift.

operaciones de storagegrid_swift_exitosas

El número total de operaciones Swift exitosas (código de estado HTTP 2xx).

operaciones de storagegrid_swift_no autorizadas

El número total de operaciones Swift fallidas que son el resultado de una falla de autorización (códigos de estado HTTP 401, 403, 405).

bytes de datos de uso del inquilino de la red de almacenamiento

El tamaño lógico de todos los objetos para el inquilino.

recuento de objetos de uso de inquilinos de la red de almacenamiento

El número de objetos para el inquilino.

cuota_de_bytes_de_uso_de_inquilinos_de_la_red_de_almacenamiento

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

Obtenga una lista de todas las métricas

Para obtener la lista completa de métricas, utilice la API de administración de cuadrícula.

1. Desde la parte superior del Administrador de cuadrícula, seleccione el ícono de ayuda y seleccione **Documentación de API**.
2. Localice las operaciones **métricas**.
3. Ejecutar el GET `/grid/metric-names` operación.
4. Descargar los resultados.

Referencia de archivos de registro

Referencia de archivos de registro

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

Los registros se clasifican de la siguiente manera:

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



Los detalles proporcionados para cada tipo de registro son sólo para referencia. Los registros están destinados a la resolución avanzada de problemas por parte del soporte técnico. Las técnicas avanzadas que implican la reconstrucción del historial de problemas utilizando los registros de auditoría y los archivos de registro de la aplicación están fuera del alcance de estas instrucciones.

Acceder a los registros

Para acceder a los registros, puede ["Recopilar archivos de registro y datos del sistema"](#) desde uno o más nodos como un único archivo de registro. O bien, si el nodo de administración principal no está disponible o no puede acceder a un nodo específico, puede acceder a archivos de registro individuales para cada nodo de la red de la siguiente manera:

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

Exportar registros al servidor syslog

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

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

Para exportar los registros, consulte ["Configurar mensajes de auditoría y destinos de registro"](#).

Categorías de archivos de registro

El archivo de registro de StorageGRID contiene los registros descritos para cada categoría y archivos

adicionales que contienen métricas y resultados de comandos de depuración.

Ubicación del archivo	Descripción
auditoría	Mensajes de auditoría generados durante el funcionamiento normal del sistema.
registros del sistema operativo base	Información del sistema operativo base, incluidas las versiones de imágenes de StorageGRID .
paquetes	Información de configuración global (paquetes).
Cassandra	Información de la base de datos de Cassandra y registros de reparación de Reaper.
CE	Información de VCS sobre el nodo actual e información del grupo EC por ID de perfil.
red	Registros generales de la red, incluida la depuración(<code>broadcast.log</code>) y <code>servermanager</code> registros.
cuadrícula.json	Archivo de configuración de cuadrícula compartido entre todos los nodos. Además, <code>node.json</code> es específico del nodo actual.
hagrupos	Métricas y registros de grupos de alta disponibilidad.
instalar	`Gdu-server` e instalar registros.
Árbitro lambda	Registros relacionados con la solicitud de proxy S3 Select.
leñador.log	Mensajes de depuración relacionados con la recopilación de registros.
Métrica	Registros de servicio para Grafana, Jaeger, exportador de nodos y Prometheus.
miscd	Registros de acceso y errores miscd.
MySQL	La configuración de la base de datos mariaDB y los registros relacionados.
neto	Registros generados por scripts relacionados con la red y el servicio Dynip.
nginx	Archivos de configuración y registros del balanceador de carga y de la federación de red. También incluye registros de tráfico de Grid Manager y Tenant Manager.

Ubicación del archivo	Descripción
nginx-gw	• <code>access.log</code>: Mensajes de registro de solicitudes de Grid Manager y Tenant Manager. ◦ Estos mensajes tienen como prefijo <code>mgmt</code>: cuando se exporta utilizando <code>syslog</code>. ◦ El formato de estos mensajes de registro es <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$request" "\$http_host" "\$http_user_agent" "\$http_referer"</code> • <code>cgr-access.log.gz</code>: Solicitudes de replicación entre redes entrantes. ◦ Estos mensajes tienen como prefijo <code>cgr</code>: cuando se exporta utilizando <code>syslog</code>. ◦ El formato de estos mensajes de registro es <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$upstream_addr" "\$request" "\$http_host"</code> • <code>endpoint-access.log.gz</code>: Solicitudes de S3 y Swift a puntos finales del balanceador de carga. ◦ Estos mensajes tienen como prefijo <code>endpoint</code>: cuando se exporta utilizando <code>syslog</code>. ◦ El formato de estos mensajes de registro es <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$upstream_addr" "\$request" "\$http_host"</code> • <code>nginx-gw-dns-check.log</code>: Relacionado con la nueva alerta de verificación de DNS.
ntp	Archivo de configuración y registros NTP.
Objetos huérfanos	Registros pertenecientes a objetos huérfanos.
sistema operativo	Archivo de estado de nodos y redes, incluidos los servicios <code>pid</code> .
otro	Archivos de registro en <code>/var/local/log</code> que no se recogen en otras carpetas.
Perf	Información de rendimiento de CPU, redes y E/S de disco.
datos de prometeo	Métricas actuales de Prometheus, si la recopilación de registros incluye datos de Prometheus.
aprovisionamiento	Registros relacionados con el proceso de aprovisionamiento de la red.
balsa	Registros del clúster Raft utilizados en los servicios de la plataforma.

Ubicación del archivo	Descripción
ssh	Registros relacionados con la configuración y el servicio SSH.
SNMP	Configuración del agente SNMP utilizada para enviar notificaciones SNMP.
datos de sockets	Datos de sockets para depuración de red.
comandos del sistema.txt	Salida de los comandos del contenedor StorageGRID . Contiene información del sistema, como la red y el uso del disco.
paquete de recuperación de sincronización	Relacionado con el mantenimiento de la coherencia del último paquete de recuperación en todos los nodos de administración y nodos de almacenamiento que alojan el servicio ADC.

Registros del software StorageGRID

Puede utilizar los registros de StorageGRID para solucionar problemas.



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

Registros generales de StorageGRID

Nombre del archivo	Notas	Encontrado en
/var/local/log/broadcast.log	El archivo principal de solución de problemas de StorageGRID . Seleccione SOPORTE > Herramientas > Topología de cuadrícula . Luego seleccione Sitio > Nodo > SSM > Eventos .	Todos los nodos
/var/local/log/broadcast-err.log	Contiene un subconjunto de <code>broadcast.log</code> (mensajes con severidad ERROR y CRÍTICO). Los mensajes CRÍTICOS también se muestran en el sistema. Seleccione SOPORTE > Herramientas > Topología de cuadrícula . Luego seleccione Sitio > Nodo > SSM > Eventos .	Todos los nodos

Nombre del archivo	Notas	Encontrado en
/var/local/núcleo/	Contiene todos los archivos de volcado de núcleo creados si el programa finaliza de manera anormal. Las posibles causas incluyen errores de afirmación, violaciones o tiempos de espera de subprocesos. Nota: El archivo <code>`/var/local/core/kexec_cmd`</code> Generalmente existe en los nodos del dispositivo y no indica un error.	Todos los nodos

Registros relacionados con el cifrado

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

Registros de la federación de red

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

Registros de NMS

Nombre del archivo	Notas	Encontrado en
/var/local/log/nms.log	• Captura notificaciones del Administrador de red y del Administrador de inquilinos. • Captura eventos relacionados con el funcionamiento del servicio NMS. Por ejemplo, notificaciones por correo electrónico y cambios de configuración. • Contiene actualizaciones de paquetes XML resultantes de cambios de configuración realizados en el sistema. • Contiene mensajes de error relacionados con el muestreo descendente de atributos realizado 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 MySQL. Contiene el flujo de error estándar (stderr) de los servicios correspondientes. Hay un archivo de registro por servicio. Estos archivos generalmente están vacíos a menos que haya problemas con el servicio.	Nodos de administración
/var/local/log/nms.requestlog	Contiene información sobre las conexiones salientes desde la API de administración a los servicios internos de StorageGRID .	Nodos de administración

Registros del Administrador del servidor

Nombre del archivo	Notas	Encontrado en
/var/local/log/servermanager.log	Archivo de registro de la aplicación Administrador de servidor que se ejecuta en el servidor.	Todos los nodos

Nombre del archivo	Notas	Encontrado en
/var/local/log/GridstatBackend.errlog	Archivo de registro de la aplicación backend GUI del Administrador del servidor.	Todos los nodos
/var/local/log/gridstat.errlog	Archivo de registro de la GUI del Administrador de servidor.	Todos los nodos

Registros de servicios de StorageGRID

Nombre del archivo	Notas	Encontrado en
/var/local/log/acct.errlog		Nodos de almacenamiento que ejecutan el servicio ADC
/var/local/log/adcd.errlog	Contiene el flujo de error estándar (stderr) de los servicios correspondientes. Hay un archivo de registro por servicio. Estos archivos generalmente están 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/cassandra/system.log	Información para el almacén de metadatos (base de datos de Cassandra) que se puede utilizar si ocurren problemas al agregar nuevos nodos de almacenamiento o si la tarea de reparación de nodetool se detiene.	Nodos de almacenamiento
/var/local/log/cassandra-reaper.log	Información para el servicio Cassandra Reaper, que realiza reparaciones de los datos en la base de datos de Cassandra.	Nodos de almacenamiento
/var/local/log/cassandra-reaper.errlog	Información de error para el servicio Cassandra Reaper.	Nodos de almacenamiento
/var/local/log/chunk.errlog		Nodos de almacenamiento
/var/local/log/cmn.errlog		Nodos de administración

Nombre del archivo	Notas	Encontrado en
/var/local/log/cms.errlog	Este archivo de registro puede estar presente en sistemas que se han actualizado desde una versión anterior de StorageGRID. Contiene información heredada.	Nodos de almacenamiento
/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 monitorea la red en busca de cambios dinámicos de IP y actualiza la configuración local.	Todos los nodos
/var/local/log/grafana.log	El registro asociado con el servicio Grafana, que se utiliza para la visualización de métricas en Grid Manager.	Nodos de administración
/var/local/log/hagroups.log	El registro asociado con los grupos de alta disponibilidad.	Nodos de administración y nodos de puerta de enlace
/var/local/log/hagroups_events.log	Realiza un seguimiento de los cambios de estado, como la transición de BACKUP a MASTER o FAULT.	Nodos de administración y nodos de puerta de enlace
/var/local/log/idnt.errlog		Nodos de almacenamiento que ejecutan el servicio ADC
/var/local/log/jaeger.log	El registro asociado con el servicio Jaeger, que se utiliza para la recopilación de seguimiento.	Todos los nodos
/var/local/log/kstn.errlog		Nodos de almacenamiento que ejecutan el servicio ADC

Nombre del archivo	Notas	Encontrado en
/var/local/log/lambd*	Contiene registros del servicio S3 Select.	Nodos de administración y de puerta de enlace Sólo ciertos nodos de administración y de puerta de enlace contienen este registro. Ver el "Requisitos y limitaciones de S3 Select para nodos de administración y de 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), que proporciona una interfaz para consultar y administrar servicios en otros nodos y para administrar configuraciones ambientales en el nodo, como por ejemplo consultar el estado de los servicios que se ejecutan en otros nodos.	Todos los nodos
/var/local/log/nginx/*.log	Contiene registros del servicio nginx, que actúa como un mecanismo de autenticación y comunicación segura para varios servicios de red (como Prometheus y Dynip) para poder comunicarse con servicios en otros nodos a través de API HTTPS.	Todos los nodos
/var/local/log/nginx-gw/*.log	Contiene registros generales relacionados con el servicio nginx-gw, incluidos registros de errores y registros de los puertos de administración restringidos en los nodos de administración.	Nodos de administración y nodos de puerta de enlace
/var/local/log/nginx-gw/cgr-access.log.gz	Contiene registros de acceso relacionados con el tráfico de replicación entre redes.	Nodos de administración, nodos de puerta de enlace o ambos, según la configuración de la federación de la red. Sólo se encuentra en la red de destino para la replicación entre redes.

Nombre del archivo	Notas	Encontrado en
/var/local/log/nginx-gw/endpoint-access.log.gz	Contiene registros de acceso para el servicio Load Balancer, que proporciona equilibrio de carga del tráfico S3 desde los clientes a los nodos de almacenamiento.	Nodos de administración y nodos de puerta de enlace
/var/local/log/persistencia*	Contiene registros del servicio de persistencia, que administra los archivos en el disco raíz que deben persistir después de un reinicio.	Todos los nodos
/var/local/log/prometheus.log	Para todos los nodos, contiene el registro del servicio exportador de nodos y el registro del servicio de métricas del exportador ade. Para los nodos de administración, 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 del servicio de máquina de estado replicada (RSM), que se utiliza para los servicios de la 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 virtuales alojados en S3. Consulte las instrucciones para implementar aplicaciones cliente S3.	Nodos de administración y de puerta de enlace
/var/local/log/actualizar-snmp-firewall.*	Contiene registros relacionados con los puertos de firewall que se administran para SNMP.	Todos los nodos
/var/local/log/update-sysl.log	Contiene registros relacionados con los cambios realizados en la configuración del syslog del sistema.	Todos los nodos

Nombre del archivo	Notas	Encontrado en
/var/local/log/actualizar-clases-de-trafico.log	Contiene registros relacionados con los cambios en la configuración de los clasificadores de tráfico.	Nodos de administración y de puerta de enlace
/var/local/log/update-utcn.log	Contiene registros relacionados con el modo de red de cliente no confiable en este nodo.	Todos los nodos

Información relacionada

- ["Acerca de bycast.log"](#)
- ["Utilice la API REST de S3"](#)

Registros de implementación y mantenimiento

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

Nombre del 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/progreso-de-expansión.log	Creado durante las operaciones de expansión. Contiene un registro de los eventos de expansión.	Nodos de almacenamiento
/var/local/log/pa-move.log	Creado mientras se ejecuta el <code>pa-move.sh</code> guion.	Nodo de administración principal
/var/local/log/pa-mover-nuevo_pa.log	Creado mientras se ejecuta el <code>pa-move.sh</code> guion.	Nodo de administración principal
/var/local/log/pa-move-old_pa.log	Creado mientras se ejecuta el <code>pa-move.sh</code> guion.	Nodo de administración principal
/var/local/log/gdu-server.log	Creado por el servicio GDU. Contiene eventos relacionados con los procedimientos de aprovisionamiento y mantenimiento administrados por el nodo de administración principal.	Nodo de administración 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

Nombre del archivo	Notas	Encontrado en
/var/local/log/upgrade.log	Creado durante la actualización del software. Contiene un registro de los eventos de actualización de software.	Todos los nodos

Acerca de bycast.log

El archivo `/var/local/log/bycast.log` Es el archivo de solución de problemas principal para el software StorageGRID . Hay una `bycast.log` archivo para cada nodo de la cuadrícula. El archivo contiene mensajes específicos para ese nodo de la cuadrícula.

El archivo `/var/local/log/bycast-err.log` es un subconjunto de `bycast.log` . Contiene mensajes de gravedad ERROR y CRÍTICO.

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

Rotación de archivos para bycast.log

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

El archivo guardado se renombra `bycast.log.1` , y el nuevo archivo se llama `bycast.log` . Cuando el nuevo `bycast.log` alcanza 1 GB, `bycast.log.1` se renombra y se comprime para convertirse en `bycast.log.2.gz` , y `bycast.log` se renombra `bycast.log.1` .

El límite de rotación para `bycast.log` son 21 archivos. Cuando se estrenó la versión 22 de la `bycast.log` Se crea el archivo y se elimina el archivo más antiguo.

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



Si se ha comprimido un archivo de registro, no debe descomprimirlo en la misma ubicación en la que fue escrito. Descomprimir el archivo en la misma ubicación puede interferir con los scripts de rotación de registros.

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

Información relacionada

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

Mensajes en bycast.log

Mensajes en `bycast.log` están escritos por ADE (Entorno distribuido asíncrono). ADE es el entorno de ejecución utilizado por los servicios de cada nodo de la red.

Ejemplo de mensaje ADE:

```
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 el ejemplo
Nodo ID	12455685
Identificación del proceso ADE	0357819531
Nombre del módulo	SVMR
Identificador del mensaje	EVHR
Hora del sistema UTC	2019-05-05T27T17:10:29.784677 (AAAA-MM-DDTHH:MM:SS.uuuuuu)
Nivel de gravedad	ERROR
Número de seguimiento interno	0906
Mensaje	SVMR: La comprobación de estado del volumen 3 ha fallado con el motivo 'TOUT'

Gravedad de los mensajes en bycast.log

Los mensajes en `bycast.log` se les asignan niveles de gravedad.

Por ejemplo:

- **AVISO** – Ha ocurrido un evento que debe ser registrado. La mayoría de los mensajes de registro están en este nivel.
- **ADVERTENCIA** – Se ha producido una condición inesperada.
- **ERROR** – Se ha producido un error importante que afectará las operaciones.
- **CRÍTICO** – Se ha producido una condición anormal que ha detenido las operaciones normales. Debe abordar la condición subyacente de inmediato.

Códigos de error en `bycast.log`

La mayoría de los mensajes de error en `bycast.log` Contienen 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
ÉXITO	Sin error
GERR	Desconocido
Cáncer	Cancelado
ABRT	Abortado
REVENDEDOR	Se acabó el tiempo
INVL	Inválido
NFND	Extraviado
VERS	Versión
CONF	Configuración
FALLAR	Con errores
ICPL	Incompleto
HECHO	Hecho
SUNV	Servicio No Disponible

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

Número de error	Código de error	Significado
001	EPERM	Operación no permitida
002	ENOENT	El fichero o directorio no existe
003	Investigación científica y tecnológica	No existe tal proceso
004	EINTR	Llamada al sistema interrumpida
005	EIO	Error de E/S
006	ENXIO	No existe tal dispositivo o dirección

Número de error	Código de error	Significado
007	E2BIG	La lista de argumentos es demasiado larga
008	ENOEXEC	Error de formato de ejecución
009	EBADF	Número de archivo incorrecto
010	ECHILD	Sin procesos secundarios
011	OTRA VEZ	Intentar otra vez
012	ENOMEM	Sin memoria
013	EACCES	Permiso denegado
014	EFAULT	Mala dirección
015	ENOTBLK	Se requiere dispositivo de bloqueo
016	OCUPADO	Dispositivo o recurso ocupado
017	EXISTE	El archivo existe
018	EXDEV	Enlace entre dispositivos
019	ENODEV	No existe tal dispositivo
020	ENOTDIR	No es un directorio
021	EISDIR	Es un directorio
022	EINVAL	Argumento inválido
023	ENFILE	Desbordamiento de la tabla de archivos
024	ARCHIVO EMFILE	Demasiados archivos abiertos
025	ENOTTY	No es una máquina de escribir
026	ETXTBSY	Archivo de texto ocupado
027	EFBIG	El archivo es demasiado grande

Número de error	Código de error	Significado
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	EPIPE	Tubería rota
033	EDOM	Argumento matemático fuera del dominio de la función
034	ERANGE	Resultado matemático no representable
035	EDEADLK	Se produciría un bloqueo de recursos
036	ESMALTE DE LARGO	El nombre del archivo es demasiado largo
037	ENOLCK	No hay bloqueos de registros disponibles
038	ENOSIS	Función no implementada
039	ENOTEMPTY	Directorio no vacío
040	ELOOP	Se encontraron demasiados enlaces simbólicos
041		
042	ENOMSG	No hay mensaje del tipo deseado
043	EIDRM	Identificador eliminado
044	ECHRNG	Número de canal fuera de rango
045	EL2NSYNC	Nivel 2 no sincronizado
046	EL3HLT	Nivel 3 detenido
047	EL3RST	Reinicio de nivel 3
048	ELNRNG	Número de enlace fuera de rango

Número de error	Código de error	Significado
049	EUNIQUE	Controlador de protocolo no adjunto
050	ENOCSI	No hay estructura CSI disponible
051	EL2HLT	Nivel 2 detenido
052	EBADE	Cambio no válido
053	EBADR	Descriptor de solicitud no válido
054	EXFULL	Intercambio completo
055	ENOANO	Sin ánodo
056	EBADRQC	Código de solicitud no válido
057	EBADSLT	Ranura no válida
058		
059	EBFONT	Formato de archivo de fuente incorrecto
060	ENOSTR	El dispositivo no es una transmisión
061	ENODATA	No hay datos disponibles
062	TIEMPO	El temporizador expiró
063	ENOSR	Recursos fuera de los flujos
064	ENONET	La máquina no está en la red
065	ENOPKG	Paquete no instalado
066	REMOTO	El objeto es remoto
067	ENOLINK	El enlace ha sido cortado
068	EADV	Error de publicidad
069	ESRMNT	Error de Srmount

Número de error	Código de error	Significado
070	Comercio electrónico	Error de comunicación al enviar
071	EPROTO	Error de protocolo
072	EMULTIHOP	Intento de multisalto
073	Departamento de Transporte de EE. UU.	Error específico de RFS
074	EBADMSG	No es un mensaje de datos
075	DESBORDAMIENTO	Valor demasiado grande para el tipo de datos definido
076	ENOTUNIQ	Nombre no único en la red
077	EBADFD	Descriptor de archivo en mal estado
078	EREMCHG	Dirección remota cambiada
079	ELIBACC	No se puede acceder a una biblioteca compartida necesaria
080	ELIBBAD	Cómo acceder 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 ilegal
085	ERESTART	La llamada al sistema interrumpida debe reiniciarse
086	ESTRPIPE	Error en la tubería de Streams
087	USUARIOS	Demasiados usuarios
088	ENOTSOCK	Operación de socket en no socket
089	EDESTADDRREQ	Dirección de destino requerida

Número de error	Código de error	Significado
090	TAMAÑO EMS	El mensaje es demasiado largo
091	EPROTOTIPO	Protocolo de tipo incorrecto para el socket
092	ENOPROTOOPT	Protocolo no disponible
093	SOPORTE DE EPROTONOS	Protocolo no compatible
094	SOPORTE DE ESOCKTNOSUPPORT	Tipo de socket no compatible
095	EOPNOTSUPP	Operación no compatible con el punto final de transporte
096	APOYO EPFNOSUPPORT	Familia de protocolos no compatible
097	APOYO EAFNOSUPPORT	Familia de direcciones no admitida por el protocolo
098	BEBER	Dirección ya en uso
099	EADDRNOTAVAIL	No se puede asignar la dirección solicitada
100	DESCARGA DE ENET	La red está caída
101	ENETUNREACH	La red no es accesible
102	REINICIO DE ENERGÍA	La conexión a la red se perdió debido al reinicio
103	ECONNABORTED	El software provocó la finalización de la conexión
104	ECONNRESET	Conexión restablecida por el par
105	ENOBUFS	No hay espacio de búfer disponible
106	EISCONN	El punto final de transporte ya está conectado
107	ENOTCONN	El punto final de transporte no está conectado
108	APAGADO	No se puede enviar después del apagado del punto final de transporte
109	ETOOMANYREFS	Demasiadas referencias: no se pueden unir

Número de error	Código de error	Significado
110	TIEMPO DE ESPERA	Se agotó el tiempo de conexión
111	ECONNREFUSED	Conexión rechazada
112	DESCONEXIÓN DE HOST	El host está caído
113	ALCANCE DE EHOST	No hay ruta al host
114	YA	Operación ya en curso
115	EN PROGRESO	Operación ya en curso
116		
117	EUCLEAN	La estructura necesita limpieza
118	ENOTNAM	No es un archivo de tipo nombrado XENIX
119	DISPONIBLE	No hay semáforos XENIX disponibles
120	EISNAM	Es un archivo de tipo nombrado
121	EREMOTEIO	Error de E/S remota
122	EDQUOT	Cuota excedida
123	ENOMEDIO	No se encontró ningún medio
124	TIPO MEDIO	Tipo de medio incorrecto
125	ECANCELADO	Operación cancelada
126	ENOKEY	La clave requerida no está disponible
127	LLAVE ELECTRÓNICA CADUCADA	La clave ha expirado
128	LLAVE ELECTRÓNICA REVOCADA	La clave ha sido revocada
129	LLAVE ELECTRÓNICA RECHAZADA	La clave fue rechazada por el servicio

Número de error	Código de error	Significado
130	PROPIETARIO MUERTO	Para mutex robustos: el propietario murió
131	NO RECUPERABLE	Para mutex robustos: Estado no recuperable

Configurar destinos de mensajes y registros de auditoría

Consideraciones para el uso de un servidor syslog externo

Un servidor syslog externo es un servidor fuera de StorageGRID que puede utilizar para recopilar información de auditoría del sistema en una única ubicación. El uso de un servidor syslog externo le permite reducir el tráfico de red en sus nodos de administración y administrar la información de manera más eficiente. Para StorageGRID, el formato del paquete de mensajes de syslog salientes cumple con RFC 3164.

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

- Registros de auditoría que contienen los mensajes de auditoría generados durante el funcionamiento normal del sistema
- Eventos relacionados con la seguridad, como inicios de sesión y escaladas a la raíz
- Registros de aplicaciones que podrían solicitarse si es necesario abrir un caso de soporte para solucionar un problema que haya encontrado

Cuándo utilizar un servidor syslog externo

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

- Recopile y administre información de auditoría, como mensajes de auditoría, registros de aplicaciones y eventos de seguridad, de manera más eficiente.
- Reduzca el tráfico de red en sus nodos de administración porque la información de auditoría se transfiere directamente desde los distintos nodos de almacenamiento al servidor syslog externo, sin tener que pasar por un nodo de administración.



Cuando se envían registros a un servidor syslog externo, los registros individuales de más de 8192 bytes se truncan al final del mensaje para cumplir con las limitaciones comunes en las implementaciones de servidores syslog externos.



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

Cómo configurar un servidor syslog externo

Para aprender a configurar un servidor syslog externo, consulte ["Configurar mensajes de auditoría y servidor syslog externo"](#).

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

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



Si utiliza un certificado de cliente, también debe utilizar una clave privada de cliente. Si proporciona una clave privada cifrada, también deberá proporcionar la frase de contraseña. No existe ningún beneficio de seguridad significativo al utilizar una clave privada cifrada porque la clave y la frase de contraseña deben almacenarse; se recomienda utilizar una clave privada no cifrada, si está disponible, para mayor simplicidad.

Cómo estimar el tamaño del servidor syslog externo

Normalmente, su red está dimensionada para lograr un rendimiento requerido, definido en términos de operaciones S3 por segundo o bytes por segundo. Por ejemplo, es posible que tenga un requisito de que su red gestione 1000 operaciones S3 por segundo, o 2000 MB por segundo, de ingestas y recuperaciones de objetos. Debe dimensionar su servidor syslog externo de acuerdo con los requisitos de datos de su red.

Esta sección proporciona algunas fórmulas heurísticas que le ayudan a estimar la velocidad y el tamaño promedio de los mensajes de registro de varios tipos que su servidor syslog externo debe ser capaz de manejar, expresados en términos de las características de rendimiento conocidas o deseadas de la red (operaciones S3 por segundo).

Utilice operaciones S3 por segundo en fórmulas de estimación

Si su red fue dimensionada para un rendimiento expresado en bytes por segundo, debe convertir este tamaño en operaciones S3 por segundo para usar las fórmulas de estimación. Para convertir el rendimiento de la red, primero debe determinar el tamaño promedio de su objeto, lo que puede hacer utilizando la información de los registros de auditoría y las métricas existentes (si las hay), o utilizando su conocimiento de las aplicaciones que usarán StorageGRID. Por ejemplo, si su cuadrícula fue dimensionada para lograr un rendimiento de 2000 MB/segundo y el tamaño promedio de su objeto es de 2 MB, entonces su cuadrícula fue dimensionada para poder manejar 1000 operaciones S3 por segundo (2000 MB/2 MB).



Las fórmulas para dimensionar el servidor syslog externo en las siguientes secciones proporcionan estimaciones de casos comunes (en lugar de estimaciones del peor de los casos). Dependiendo de su configuración y carga de trabajo, es posible que observe una tasa mayor o menor de mensajes de syslog o un volumen de datos de syslog de lo que predicen las fórmulas. Las fórmulas están pensadas únicamente para servir de guía.

Fórmulas de estimación para registros de auditoría

Si no tiene información sobre su carga de trabajo S3 aparte de la cantidad de operaciones S3 por segundo que se espera que admita su red, puede estimar el volumen de registros de auditoría que su servidor syslog externo necesitará manejar utilizando las siguientes fórmulas, suponiendo que deje los Niveles de auditoría configurados en los valores predeterminados (todas las categorías configuradas en Normal, excepto Almacenamiento, que está configurado en Error):

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

Por ejemplo, si su red está dimensionada para 1000 operaciones S3 por segundo, su servidor syslog externo debe tener un tamaño que admita 2000 mensajes syslog por segundo y debe poder recibir (y normalmente almacenar) datos de registro de auditoría a una velocidad de 1,6 MB por segundo.

Si conoce más sobre su carga de trabajo, será posible realizar estimaciones más precisas. Para los registros de auditoría, las variables adicionales más importantes son el porcentaje de operaciones S3 que son PUT (frente a GETS) y el tamaño promedio, en bytes, de los siguientes campos S3 (las abreviaturas de 4 caracteres utilizadas en la tabla son nombres de campos del registro de auditoría):

Código	Campo	Descripción
SACC	Nombre de la cuenta del inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de inquilino del usuario que envió la solicitud. Vacío para solicitudes anónimas.
SBAC	Nombre de la cuenta del inquilino de S3 (propietario del depósito)	El nombre de la cuenta del inquilino del propietario del depósito. Se utiliza para identificar acceso entre cuentas o anónimo.
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito. Las operaciones en depósitos no incluyen este campo.

Utilicemos P para representar el porcentaje de operaciones S3 que son PUT, donde $0 \leq P \leq 1$ (por lo tanto, para una carga de trabajo PUT del 100 %, $P = 1$, y para una carga de trabajo GET del 100 %, $P = 0$).

Utilicemos K para representar el tamaño promedio de la suma de los nombres de cuenta S3, el depósito S3 y la clave S3. Supongamos que el nombre de la cuenta S3 siempre es my-s3-account (13 bytes), los buckets 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). Entonces el valor de K es 90 (13+13+28+36).

Si puede determinar valores para P y K, puede estimar el volumen de registros de auditoría que su servidor syslog externo necesitará manejar utilizando las siguientes fórmulas, bajo 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 su red está dimensionada para 1000 operaciones S3 por segundo, su carga de trabajo es 50% PUT y sus nombres de cuenta S3, nombres de depósito y nombres de objeto tienen un promedio de 90 bytes,

su servidor syslog externo debe tener un tamaño que admita 1500 mensajes syslog por segundo y debe poder recibir (y normalmente almacenar) datos de registro de auditoría a una velocidad de aproximadamente 1 MB por segundo.

Fórmulas de estimación para niveles de auditoría no predeterminados

Las fórmulas proporcionadas para los registros de auditoría suponen el uso de configuraciones de nivel de auditoría predeterminadas (todas las categorías configuradas en Normal, excepto Almacenamiento, que está configurada en Error). No están disponibles fórmulas detalladas para estimar la tasa y el tamaño promedio de los mensajes de auditoría para configuraciones de nivel de auditoría no predeterminado. Sin embargo, la siguiente tabla se puede utilizar para hacer una estimación aproximada de la tasa; puede utilizar la fórmula de tamaño promedio proporcionada para los registros de auditoría, pero tenga en cuenta que es probable que resulte en una sobreestimación porque los mensajes de auditoría "adicionales" son, en promedio, más pequeños que los mensajes de auditoría predeterminados.

Condición	Fórmula
Replicación: niveles de auditoría configurados en Depuración o Normal	Tasa de registro de auditoría = 8 x Tasa de operaciones de S3
Codificación de borrado: niveles de auditoría configurados en Depuración 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 normalmente producen 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 sobre su carga de trabajo S3 excepto la cantidad de operaciones S3 por segundo que se espera que admita su red, puede estimar el volumen de registros de aplicaciones que su servidor syslog externo necesitará manejar utilizando las siguientes fórmulas:

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Entonces, por ejemplo, si su red está dimensionada para 1000 operaciones S3 por segundo, su servidor syslog externo debe tener un tamaño que admita 3300 registros de aplicaciones por segundo y pueda recibir (y almacenar) datos de registros de aplicaciones a una velocidad de aproximadamente 1,2 MB por segundo.

Si conoce más sobre su carga de trabajo, será posible realizar estimaciones más precisas. Para los registros de aplicaciones, las variables adicionales más importantes son la estrategia de protección de datos (replicación vs. codificación de borrado), el porcentaje de operaciones S3 que son PUT (vs. GET/otras) y el tamaño promedio, en bytes, de los siguientes campos S3 (las abreviaturas de 4 caracteres utilizadas en la tabla son nombres de campos del registro de auditoría):

Código	Campo	Descripción
SACC	Nombre de la cuenta del inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de inquilino del usuario que envió la solicitud. Vacío para solicitudes anónimas.
SBAC	Nombre de la cuenta del inquilino de S3 (propietario del depósito)	El nombre de la cuenta del inquilino del propietario del depósito. Se utiliza para identificar acceso entre cuentas o anónimo.
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito. Las operaciones en depósitos no incluyen este campo.

Estimaciones de tamaño de ejemplo

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

- Replicación
- Codificación de borrado

Si utiliza la replicación para la protección de datos

Sea P el porcentaje de operaciones S3 que son PUT, donde $0 \leq P \leq 1$ (por lo tanto, para una carga de trabajo PUT del 100 %, $P = 1$, y para una carga de trabajo GET del 100 %, $P = 0$).

Sea K el tamaño promedio de la suma de los nombres de cuenta S3, el depósito S3 y la clave S3. Supongamos que el nombre de la cuenta S3 siempre es my-s3-account (13 bytes), los buckets 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). Entonces K tiene un valor de 90 (13+13+28+36).

Si puede determinar valores para P y K , puede estimar el volumen de registros de aplicaciones que su servidor syslog externo deberá poder manejar utilizando 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
```

Entonces, por ejemplo, si su red tiene un tamaño adecuado para 1000 operaciones S3 por segundo, su carga de trabajo es 50 % PUT y sus nombres de cuenta S3, nombres de depósito y nombres de objeto tienen un promedio de 90 bytes, su servidor syslog externo debe tener un tamaño adecuado para admitir 1800 registros de aplicaciones por segundo y recibirá (y generalmente almacenará) datos de aplicaciones a una velocidad de 0,5 MB por segundo.

Si utiliza codificación de borrado para la protección de datos

Sea P el porcentaje de operaciones S3 que son PUT, donde $0 \leq P \leq 1$ (por lo tanto, para una carga de trabajo PUT del 100 %, $P = 1$, y para una carga de trabajo GET del 100 %, $P = 0$).

Sea K el tamaño promedio de la suma de los nombres de cuenta S3, el depósito S3 y la clave S3. Supongamos que el nombre de la cuenta S3 siempre es my-s3-account (13 bytes), los buckets 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). Entonces K tiene un valor de 90 (13+13+28+36).

Si puede determinar valores para P y K , puede estimar el volumen de registros de aplicaciones que su servidor syslog externo deberá poder manejar utilizando 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
```

Entonces, por ejemplo, si su red tiene un tamaño adecuado para 1000 operaciones S3 por segundo, su carga de trabajo es 50 % PUT y los nombres de sus cuentas S3, nombres de bucket y nombres de objeto tienen un promedio de 90 bytes, su servidor syslog externo debe tener un tamaño adecuado para admitir 2250 registros de aplicaciones por segundo y debe poder recibir (y normalmente almacenar) datos de aplicaciones a una velocidad de 0,6 MB por segundo.

Configurar mensajes de auditoría y servidor syslog externo

Puede configurar una serie de ajustes relacionados con los mensajes de auditoría. Puede ajustar la cantidad de mensajes de auditoría registrados; definir cualquier encabezado de solicitud HTTP que desee incluir en los mensajes de auditoría de lectura y escritura del cliente; configurar un servidor syslog externo; y especificar dónde se envían los registros de auditoría, los registros de eventos de seguridad y los registros del software StorageGRID .

Los mensajes y registros de auditoría registran las actividades del sistema y los eventos de seguridad, y son herramientas esenciales para la supervisión y la resolución de problemas. Todos los nodos de StorageGRID generan mensajes de auditoría y registros para rastrear la actividad y los eventos del sistema.

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de mantenimiento o acceso root"](#) .
- Si planea configurar un servidor syslog externo, ha revisado la ["Consideraciones para el uso de un servidor syslog externo"](#) y se aseguró de que el servidor tenga suficiente capacidad para recibir y almacenar los archivos de registro.

- Si planea configurar un servidor syslog externo usando el protocolo TLS o RELP/TLS, debe tener los certificados de cliente y CA del servidor necesarios y la clave privada del cliente.

Cambiar los niveles de los mensajes de auditoría

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

Categoría de auditoría	Configuración predeterminada	Más información
Sistema	Normal	"Mensajes de auditoría del sistema"
Almacenamiento	Error	"Mensajes de auditoría de almacenamiento de objetos"
Gestión	Normal	"Mensaje de auditoría de gestión"
El cliente lee	Normal	"El cliente lee mensajes de auditoría"
El cliente escribe	Normal	"El cliente escribe mensajes de auditoría"
ILM	Normal	"Mensajes de auditoría de ILM"
Replicación entre redes	Error	"CGRR: Solicitud de replicación entre redes"



Estos valores predeterminados se aplican si instaló inicialmente StorageGRID usando la versión 10.3 o posterior. Si utilizó inicialmente una versión anterior de StorageGRID, el valor predeterminado para todas las categorías se establece en Normal.



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

Pasos

1. Seleccione **CONFIGURACIÓN > Monitoreo > 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: mensajes de auditoría para los cuales el código de resultado no fue "exitoso" (SUCCS).

Nivel de auditoría	Descripción
Normal	Se registran los mensajes transaccionales estándar (los mensajes enumerados en estas instrucciones para la categoría).
Depurar	Obsoleto. Este nivel se comporta igual que el nivel de auditoría Normal.

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



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

3. Seleccione **Guardar**.

Un banner verde indica que su configuración ha sido guardada.

Definir encabezados de solicitud HTTP

Opcionalmente, puede definir cualquier encabezado de solicitud HTTP que desee incluir en los mensajes de auditoría de lectura y escritura del cliente. Estos encabezados de protocolo se aplican únicamente a solicitudes S3.

Pasos

1. En la sección **Encabezados de protocolo de auditoría**, defina los encabezados de solicitud HTTP que desea incluir en los mensajes de auditoría de lectura y escritura del cliente.

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

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

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



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

3. Seleccione **Guardar**

Un banner verde indica que su configuración ha sido guardada.

Utilice un servidor syslog externo

Opcionalmente, puede configurar un servidor syslog externo para guardar registros de auditoría, registros de aplicaciones y registros de eventos de seguridad en una ubicación fuera de su red.



Si no desea utilizar un servidor syslog externo, omita este paso y vaya a [Seleccionar destinos de información de auditoría](#).



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

Ingresar información de syslog

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

Pasos

1. Desde la página Servidor de auditoría y syslog, seleccione **Configurar servidor syslog externo**. O bien, si ha configurado previamente un servidor syslog externo, seleccione **Editar servidor syslog externo**.

Aparece el asistente para configurar el servidor syslog externo.

2. Para el paso **Ingresar información de syslog** del asistente, ingrese un nombre de dominio completo válido o una dirección IPv4 o IPv6 para el servidor syslog externo en el campo **Host**.
3. Introduzca el puerto de destino en el servidor syslog externo (debe ser un número entero entre 1 y 65535). El puerto predeterminado es 514.
4. Seleccione el protocolo utilizado para enviar información de auditoría al servidor syslog externo.

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

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



El Protocolo de registro de eventos confiable (RELPL) extiende la funcionalidad del protocolo syslog para proporcionar una entrega confiable de mensajes de eventos. El uso de RELPL puede ayudar a evitar la pérdida de información de auditoría si su servidor syslog externo tiene que reiniciarse.

5. Seleccione **Continuar**.
6. Si seleccionó **TLS** o **RELPL/TLS**, cargue los certificados de CA del servidor, el certificado del cliente y la clave privada del cliente.
 - a. Seleccione **Explorar** para el certificado o la clave que desea utilizar.
 - b. Seleccione el certificado o el archivo de clave.
 - c. Seleccione **Abrir** para cargar el archivo.

Aparece una marca de verificación verde junto al nombre del certificado o del archivo de clave para notificarle que se ha cargado correctamente.

7. Seleccione **Continuar**.

Administrar el contenido de syslog

Puede seleccionar qué información enviar al servidor syslog externo.

Pasos

1. Para el paso **Administrar contenido de syslog** del asistente, seleccione cada tipo de información de auditoría que desee enviar al servidor syslog externo.
 - **Enviar registros de auditoría:** envía eventos de StorageGRID y actividades del sistema
 - **Enviar eventos de seguridad:** Envía eventos de seguridad, como cuando un usuario no autorizado intenta iniciar sesión o un usuario inicia sesión como root.
 - **Enviar registros de la aplicación:** Envía "[Archivos de registro del software StorageGRID](#)" Útil para la resolución de problemas, incluidos:
 - `broadcast-err.log`
 - `broadcast.log`
 - `jaeger.log`
 - `nms.log` (Solo nodos de administración)
 - `prometheus.log`
 - `raft.log`
 - `hagroups.log`
 - **Enviar registros de acceso:** envía registros de acceso HTTP para solicitudes externas a Grid Manager, Tenant Manager, puntos finales de balanceador de carga configurados y solicitudes de federación de red desde sistemas remotos.
2. Utilice los menús desplegables para seleccionar la gravedad y la facilidad (tipo de mensaje) para cada categoría de información de auditoría que desee enviar.

Establecer los valores de gravedad y de facilidad puede ayudarle a agregar los registros de formas personalizables para facilitar el análisis.

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

Si selecciona un valor, el valor seleccionado se aplicará a todos los mensajes de este tipo. Se perderá información sobre los diferentes niveles de gravedad si anula la gravedad con un valor fijo.

Gravedad	Descripción
Paso a través	Cada mensaje enviado al syslog externo debe tener el mismo valor de gravedad que cuando se registró localmente en el nodo: • Para los registros de auditoría, la gravedad es "info". • Para los eventos de seguridad, los valores de gravedad son generados por la distribución de Linux en los nodos. • Para los registros de aplicaciones, la gravedad varía entre "información" y "aviso", dependiendo de cuál sea el problema. Por ejemplo, agregar un servidor NTP y configurar un grupo HA proporciona un valor de "información", mientras que detener intencionalmente el servicio SSM o RSM proporciona un valor de "aviso". • Para los registros de acceso, la gravedad es "info".
0	Emergencia: El sistema no se puede utilizar

Gravedad	Descripción
1	Alerta: Se deben tomar medidas de inmediato
2	Crítico: Condiciones críticas
3	Error: Condiciones de error
4	Advertencia: Condiciones de advertencia
5	Aviso: Estado normal pero significativo.
6	Informativo: Mensajes informativos
7	Depuración: mensajes de nivel de depuración

b. Para **Instalación**, seleccione **Paso a través**, o seleccione un valor de instalación entre 0 y 23.

Si selecciona un valor, se aplicará a todos los mensajes de este tipo. Se perderá información sobre diferentes instalaciones si anula una instalación con un valor fijo.

Instalación	Descripción
Paso a través	Cada mensaje enviado al syslog externo debe tener el mismo valor de facilidad que cuando se registró localmente en el nodo: • Para los registros de auditoría, la función enviada al servidor syslog externo es "local7". • Para los eventos de seguridad, los valores de las instalaciones son generados por la distribución de Linux en los nodos. • Para los registros de aplicaciones, los registros de aplicaciones enviados al servidor syslog externo tienen los siguientes valores de instalación: ◦ <code>broadcast.log</code>: usuario o demonio ◦ <code>broadcast-err.log</code>: usuario, demonio, local3 o local4 ◦ <code>jaeger.log</code>: local2 ◦ <code>nms.log</code>: local3 ◦ <code>prometheus.log</code>: local4 ◦ <code>raft.log</code>: local5 ◦ <code>hagroups.log</code>: local6 • Para los registros de acceso, la función enviada al servidor syslog externo es "local0".
0	kern (mensajes del kernel)

Instalación	Descripción
1	usuario (mensajes a nivel de usuario)
2	correo
3	daemon (demonios del sistema)
4	auth (mensajes de seguridad/autorización)
5	syslog (mensajes generados internamente por syslogd)
6	lpr (subsistema de impresora de línea)
7	noticias (subsistema de noticias de la red)
8	UUCP
9	cron (demonio de reloj)
10	seguridad (mensajes de seguridad/autorización)
11	FTP
12	NTP
13	logaudit (auditoría de registros)
14	logalert (alerta de registro)
15	reloj (demonio del reloj)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6

Instalación	Descripción
23	local7

3. Seleccione **Continuar**.

Enviar mensajes de prueba

Antes de comenzar a utilizar un servidor syslog externo, debe solicitar que todos los nodos de su red envíen mensajes de prueba al servidor syslog externo. Debe utilizar estos mensajes de prueba para ayudarlo a validar toda su infraestructura de recopilación de registros antes de comprometerse a enviar datos al servidor syslog externo.



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

Pasos

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

Un banner verde indica que la configuración se ha guardado.

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

Los resultados de la prueba aparecen continuamente en la página hasta que usted detiene la prueba. Mientras la prueba está en curso, sus mensajes de auditoría continúan enviándose a los destinos previamente configurados.

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

Ver "[Solucionar problemas de un servidor syslog externo](#)" para ayudarlo a resolver cualquier error.

4. Espere hasta que vea un banner verde que indique que todos los nodos han pasado la prueba.
5. Verifique su servidor syslog para determinar si los mensajes de prueba se están recibiendo y procesando como se espera.



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

6. Seleccione **Detener y finalizar**.

Regresará a la página **Servidor de auditoría y syslog**. Un banner verde indica que se ha guardado la configuración del servidor syslog.



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

Seleccionar destinos de información de auditoría

Puede especificar dónde se guardan los registros de auditoría, los registros de eventos de seguridad y "Registros del software StorageGRID" se envían.



StorageGRID tiene como valor predeterminado los destinos de auditoría del nodo local y almacena la información de auditoría en `/var/local/log/localaudit.log`.

Al utilizar `/var/local/log/localaudit.log` Las entradas del registro de auditoría de Grid Manager y Tenant Manager podrían enviarse a un nodo de almacenamiento. Puede encontrar qué nodo tiene las entradas más recientes utilizando el `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail" dominio`.

Algunos destinos solo están disponibles si ha configurado un servidor syslog externo.

Pasos

1. En la página Servidor de auditoría y syslog, seleccione el destino de la información de auditoría.



Solo los nodos locales y los **servidores syslog externos** generalmente brindan un mejor rendimiento.

Opción	Descripción
Solo nodos locales (predeterminado)	Los mensajes de auditoría, los registros de eventos de seguridad y los registros de aplicaciones no se envían a los nodos de administración. En cambio, se guardan únicamente en los nodos que los generaron ("el nodo local"). La información de auditoría generada en cada nodo local se almacena en <code>/var/local/log/localaudit.log</code>. Nota: StorageGRID elimina periódicamente los registros locales en una rotación para liberar espacio. Cuando el archivo de registro de un nodo alcanza 1 GB, se guarda el archivo existente y se inicia un nuevo archivo de registro. El límite de rotación del registro es de 21 archivos. Cuando se crea la versión 22 del archivo de registro, se elimina el archivo de registro más antiguo. En promedio, se almacenan alrededor de 20 GB de datos de registro en cada nodo.
Nodos de administración/nodos locales	Los mensajes de auditoría se envían al registro de auditoría en los nodos de administración, y los registros de eventos de seguridad y los registros de aplicaciones se almacenan en los nodos que los generaron. La información de auditoría se almacena en los siguientes archivos: • Nodos de administración (principales y no principales): <code>/var/local/audit/export/audit.log</code> • Todos los nodos: El <code>/var/local/log/localaudit.log</code> El archivo normalmente está vacío o falta. Podría contener información secundaria, como una copia adicional de algunos mensajes.

Opción	Descripción
Servidor syslog externo	La información de auditoría se envía a un servidor syslog externo y se guarda en los nodos locales(<code>/var/local/log/localaudit.log</code>). El tipo de información enviada depende de cómo haya configurado el servidor syslog externo. Esta opción se habilita solo después de haber configurado un servidor syslog externo.
Nodo de administración y servidor syslog externo	Los mensajes de auditoría se envían al registro de auditoría(<code>/var/local/audit/export/audit.log</code>) en los nodos de administración y la información de auditoría se envía al servidor syslog externo y se guarda en el nodo local(<code>/var/local/log/localaudit.log</code>). El tipo de información enviada depende de cómo haya configurado el servidor syslog externo. Esta opción se habilita solo después de haber configurado un servidor syslog externo.

2. Seleccione **Guardar**.

Aparece un mensaje de advertencia.

3. Seleccione **Aceptar** para confirmar que desea cambiar el destino de la información de auditoría.

Un banner verde indica que se ha guardado la configuración de auditoría.

Los nuevos registros se envían a los destinos que usted seleccionó. Los registros existentes permanecen en su ubicación actual.

Utilice la monitorización SNMP

Utilice la monitorización SNMP

Si desea supervisar StorageGRID mediante el Protocolo simple de administración de red (SNMP), debe configurar el agente SNMP que se incluye con StorageGRID.

- ["Configurar el agente SNMP"](#)
- ["Actualizar el agente SNMP"](#)

Capacidades

Cada nodo StorageGRID ejecuta un agente SNMP, o demonio, que proporciona una MIB. La MIB de StorageGRID contiene definiciones de tablas y notificaciones para alertas. La 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.



Ver ["Acceder a archivos MIB"](#) Si desea descargar los archivos MIB en los nodos de su red.

Inicialmente, SNMP está deshabilitado en todos los nodos. Cuando configura 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 basadas en eventos a un sistema de administración:

Trampas

Las trampas son notificaciones enviadas por el agente SNMP que no requieren reconocimiento por parte del sistema de administración. Las trampas sirven para notificar al sistema de administración que algo ha sucedido dentro de StorageGRID, como por ejemplo la activación de una alerta.

Las trampas son compatibles con las tres versiones de SNMP.

Informa

Los informes son similares a las trampas, pero requieren el reconocimiento del sistema de gestión. Si el agente SNMP no recibe un acuse de recibo dentro de un período de tiempo determinado, vuelve a enviar el informe hasta que recibe un acuse de recibo o se alcanza el valor máximo de reintentos.

Los informes son compatibles con SNMPv2c y SNMPv3.

Las notificaciones de trampa e información se envían en los siguientes casos:

- 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. Las notificaciones de alerta son enviadas por el [Nodo de administración del remitente preferido](#).

Cada alerta se asigna a uno de tres tipos de trampa según el nivel de gravedad de la alerta: activeMinorAlert, activeMajorAlert y activeCriticalAlert. Para obtener una lista de las alertas que pueden activar estas trampas, consulte la [Referencia de alertas](#).

Compatibilidad con versiones SNMP

La tabla proporciona un resumen de alto nivel de lo que se admite para cada versión de SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Consultas (GET y GETNEXT)	Consultas MIB de solo lectura	Consultas MIB de solo lectura	Consultas MIB de solo lectura
Autenticación de consultas	Cadena comunitaria	Cadena comunitaria	Modelo de seguridad basado en el usuario (USM)
Notificaciones (TRAMPA e INFORME)	Solo trampas	Atrapa e informa	Atrapa e informa
Autenticación de notificaciones	Comunidad de trampa predeterminada o una cadena de comunidad personalizada para cada destino de trampa	Comunidad de trampa predeterminada o una cadena de comunidad personalizada para cada destino de trampa	Usuario USM para cada destino de trampa

Limitaciones

- StorageGRID admite acceso MIB de solo lectura. No se admite el acceso de lectura y escritura.
- Todos los nodos de la red reciben la misma configuración.
- SNMPv3: StorageGRID no admite el modo de soporte de transporte (TSM).
- SNMPv3: el único protocolo de autenticación admitido es SHA (HMAC-SHA-96).
- SNMPv3: el único protocolo de privacidad admitido es AES.

Configurar el agente SNMP

Puede configurar el agente SNMP de StorageGRID para utilizar un sistema de administración SNMP de terceros para acceso y notificaciones de MIB de solo lectura.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root"](#) .

Acerca de esta tarea

El agente SNMP de StorageGRID admite SNMPv1, SNMPv2c y SNMPv3. Puede configurar el agente para una o más versiones. Para SNMPv3, solo se admite la autenticación del modelo de seguridad de usuario (USM).

Todos los nodos de la red utilizan la misma configuración SNMP.

Especificar la configuración básica

Como primer paso, habilite el agente SMNP de StorageGRID y proporcione información básica.

Pasos

1. Seleccione **CONFIGURACIÓN > Monitoreo > Agente SNMP**.

Aparece la página del agente SNMP.

2. Para habilitar el agente SNMP en todos los nodos de la red, seleccione la casilla de verificación **Habilitar SNMP**.
3. Introduzca la siguiente información en la sección Configuración básica.

Campo	Descripción
Contacto del sistema	Opcional. El contacto principal del sistema StorageGRID , que se devuelve en los mensajes SNMP como sysContact. El contacto del sistema normalmente es una dirección de correo electrónico. Este valor se aplica a todos los nodos del sistema StorageGRID . Contacto del sistema puede tener un máximo de 255 caracteres.

Campo	Descripción
Ubicación del sistema	Opcional. La ubicación del sistema StorageGRID , que se devuelve en los mensajes SNMP como sysLocation. La ubicación del sistema puede ser cualquier información que sea útil para identificar dónde se encuentra su sistema StorageGRID . Por ejemplo, puede utilizar la dirección de una instalación. Este valor se aplica a todos los nodos del sistema StorageGRID . Ubicación del sistema puede tener un máximo de 255 caracteres.
Habilitar notificaciones del agente SNMP	• Si se selecciona, el agente SNMP de StorageGRID envía notificaciones de captura e información. • Si no se selecciona, el agente SNMP admite acceso MIB de solo lectura, pero no envía ninguna notificación SNMP.
Habilitar trampas de autenticación	Si se selecciona, el agente SNMP de StorageGRID envía trampas de autenticación si recibe mensajes de protocolo autenticados incorrectamente.

Introduzca cadenas de la comunidad

Si utiliza SNMPv1 o SNMPv2c, complete la sección Cadenas de comunidad.

Cuando el sistema de administración consulta la MIB de StorageGRID , envía una cadena de comunidad. Si la cadena de comunidad coincide con uno de los valores especificados aquí, el agente SNMP envía una respuesta al sistema de administración.

Pasos

1. Para **Comunidad de solo lectura**, ingrese opcionalmente una cadena de comunidad para permitir el acceso MIB de solo lectura en direcciones de agente IPv4 e IPv6.



Para garantizar la seguridad de su sistema StorageGRID , no utilice "público" como cadena de comunidad. Si deja este campo en blanco, el agente SNMP utiliza la ID de red de su sistema StorageGRID como cadena de comunidad.

Cada cadena de comunidad puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

2. Seleccione **Agregar otra cadena de comunidad** para agregar cadenas adicionales.

Se permiten hasta cinco cuerdas.

Crear destinos de trampa

Utilice la pestaña Destinos de trampa en la sección Otras configuraciones para definir uno o más destinos para las notificaciones de trampa o información de StorageGRID . Cuando habilita el agente SNMP y selecciona **Guardar**, StorageGRID envía notificaciones a cada destino definido cuando se activan alertas. También se envían notificaciones estándar para las entidades MIB-II compatibles (por ejemplo, ifDown y coldStart).

Pasos

1. Para el campo **Comunidad de trampa predeterminada**, ingrese opcionalmente la cadena de comunidad predeterminada que desea utilizar para los destinos de trampa SNMPv1 o SNMPv2.

Según sea necesario, puede proporcionar una cadena de comunidad diferente ("personalizada") cuando defina un destino de trampa específico.

La comunidad de trampa predeterminada puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

2. Para agregar un destino de trampa, seleccione **Crear**.
3. Seleccione qué versión de SNMP se utilizará para este destino de trampa.
4. Complete el formulario Crear destino de trampa para la versión que seleccionó.

SNMPv1

Si seleccionó SNMPv1 como versión, complete estos campos.

Campo	Descripción
Tipo	Debe ser una trampa para SNMPv1.
Host	Una dirección IPv4 o IPv6 o un nombre de dominio completo (FQDN) para recibir la trampa.
Puerto	Utilice 162, que es el puerto estándar para trampas SNMP, a menos que deba utilizar otro valor.
Protocolo	Utilice UDP, que es el protocolo de trampa SNMP estándar, a menos que necesite utilizar TCP.
Cadena comunitaria	Utilice la comunidad de trampa predeterminada, si se especificó una, o ingrese una cadena de comunidad personalizada para este destino de trampa. La cadena de comunidad personalizada puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

SNMPv2c

Si seleccionó SNMPv2c como versión, complete estos campos.

Campo	Descripción
Tipo	Si el destino se utilizará para trampas o informes.
Host	Una dirección IPv4 o IPv6 o FQDN para recibir la trampa.
Puerto	Utilice 162, que es el puerto estándar para trampas SNMP a menos que deba utilizar otro valor.
Protocolo	Utilice UDP, que es el protocolo de trampa SNMP estándar, a menos que necesite utilizar TCP.
Cadena comunitaria	Utilice la comunidad de trampa predeterminada, si se especificó una, o ingrese una cadena de comunidad personalizada para este destino de trampa. La cadena de comunidad personalizada puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

SNMPv3

Si seleccionó SNMPv3 como versión, complete estos campos.

Campo	Descripción
Tipo	Si el destino se utilizará para trampas o informes.
Host	Una dirección IPv4 o IPv6 o FQDN para recibir la trampa.
Puerto	Utilice 162, que es el puerto estándar para trampas SNMP a menos que deba utilizar otro valor.
Protocolo	Utilice UDP, que es el protocolo de trampa SNMP estándar, a menos que necesite utilizar TCP.
Usuario de USM	El usuario USM que se utilizará para la autenticación. • Si seleccionó Trampa, solo se mostrarán los usuarios de USM sin identificaciones de motor autorizadas. • Si seleccionó Informar, solo se mostrarán los usuarios de USM con ID de motor autorizados. • Si no se muestran usuarios: i. Crea y guarda el destino de la trampa. ii. Ir a Crear usuarios de USM y crear el usuario. iii. Regrese a la pestaña Destinos de trampa, seleccione el destino guardado de la tabla y seleccione Editar. iv. Seleccione el usuario.

5. Seleccione **Crear**.

Se crea el destino de la trampa y se agrega a la tabla.

Crear direcciones de agentes

Opcionalmente, utilice la pestaña Direcciones del agente en la sección Otras configuraciones para especificar una o más "direcciones de escucha". Estas son las direcciones StorageGRID en las que el agente SNMP puede recibir consultas.

Si no configura una dirección de agente, la dirección de escucha predeterminada es el puerto UDP 161 en todas las redes StorageGRID .

Pasos

1. Seleccione **Crear**.
2. Introduzca la siguiente información.

Campo	Descripción
Protocolo de Internet	Si esta dirección utilizará IPv4 o IPv6. De forma predeterminada, SNMP utiliza IPv4.
Protocolo de transporte	Si esta dirección utilizará UDP o TCP. De forma predeterminada, SNMP utiliza UDP.
Red StorageGRID	En qué red StorageGRID escuchará el agente. • Redes de cuadrícula, administración y cliente: el agente SNMP escuchará consultas en las tres redes. • Red de cuadrícula • Red de administración • Red de clientes Nota: Si utiliza la red del cliente para datos no seguros y crea una dirección de agente para la red del cliente, tenga en cuenta que el tráfico SNMP también será inseguro.
Puerto	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 ingresar cualquier número de puerto no utilizado. Nota: Cuando guarda el agente SNMP, StorageGRID abre automáticamente los puertos de dirección del agente en el firewall interno. Debe asegurarse de que todos los firewalls externos permitan el acceso a estos puertos.

3. Seleccione **Crear**.

Se crea la dirección del agente y se agrega a la tabla.

Crear usuarios USM

Si está utilizando SNMPv3, utilice la pestaña Usuarios USM en la sección Otras configuraciones para definir los usuarios USM que están autorizados a consultar la MIB o a recibir trampas e informes.



Los destinos *inform* de SNMPv3 deben tener usuarios con ID de motor. El destino *trap* de SNMPv3 no puede tener usuarios con ID de motor.

Estos pasos no se aplican si solo utiliza SNMPv1 o SNMPv2c.

Pasos

1. Seleccione **Crear**.

2. Introduzca la siguiente información.

Campo	Descripción
Nombre de usuario	Un nombre único para este usuario de USM. Los nombres de usuario pueden tener un máximo de 32 caracteres y no pueden contener espacios en blanco. El nombre de usuario no se puede cambiar una vez creado el usuario.
Acceso MIB de solo lectura	Si se selecciona, este usuario debe tener acceso de solo lectura a la MIB.
Identificación de motor autorizada	Si este usuario se utilizará en un destino de información, el ID del motor autorizado para este usuario. Ingrese de 10 a 64 caracteres hexadecimales (de 5 a 32 bytes) sin espacios. Este valor es necesario para los usuarios de USM que se seleccionarán en los destinos de trampa para los informes. Este valor no está permitido para los usuarios de USM que se seleccionarán en destinos de trampas. Nota: Este campo no se muestra si seleccionó Acceso MIB de solo lectura porque los usuarios de USM que tienen acceso MIB de solo lectura no pueden tener ID de motor.
Nivel de seguridad	El nivel de seguridad para el usuario USM: • authPriv: Este usuario se comunica con autenticación y privacidad (cifrado). Debe especificar un protocolo de autenticación y una contraseña y un protocolo de privacidad y una contraseña. • authNoPriv: Este usuario se comunica con autenticación y sin privacidad (sin cifrado). Debe especificar un protocolo de autenticación y una contraseña.
Protocolo de autenticación	Siempre configúrelo en SHA, que es el único protocolo compatible (HMAC-SHA-96).
Password	La contraseña que este usuario utilizará para la autenticación.
Protocolo de privacidad	Solo se muestra si seleccionó authPriv y siempre se configura en AES, que es el único protocolo de privacidad compatible.
Password	Sólo se muestra si seleccionó authPriv. La contraseña que este usuario utilizará para su privacidad.

3. Seleccione **Crear**.

Se crea el usuario USM y se agrega a la tabla.

4. Cuando haya completado la configuración del agente SNMP, seleccione **Guardar**.

La nueva configuración del agente SNMP se vuelve activa.

Actualizar el agente SNMP

Puede deshabilitar las notificaciones SNMP, actualizar cadenas de comunidad o agregar o eliminar direcciones de agentes, usuarios USM y destinos de trampa.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de acceso root"](#).

Acerca de esta tarea

Ver ["Configurar el agente SNMP"](#) para obtener detalles sobre cada campo en la página del agente SNMP. Debes seleccionar **Guardar** en la parte inferior de la página para confirmar cualquier cambio que realices en cada pestaña.

Pasos

1. Seleccione **CONFIGURACIÓN > Monitoreo > Agente SNMP**.

Aparece la página del agente SNMP.

2. Para deshabilitar el agente SNMP en todos los nodos de la red, desmarque la casilla **Habilitar SNMP** y seleccione **Guardar**.

Si vuelve a habilitar el agente SNMP, se conservarán todas las configuraciones de SNMP anteriores.

3. Opcionalmente, actualice la información en la sección Configuración básica:
 - a. Según sea necesario, actualice el **Contacto del sistema** y la **Ubicación del sistema**.
 - b. De manera opcional, seleccione o desmarque la casilla de verificación **Habilitar notificaciones del agente SNMP** para controlar si el agente SNMP de StorageGRID envía notificaciones de captura e información.

Cuando esta casilla de verificación no está marcada, el agente SNMP admite acceso MIB de solo lectura, pero no envía notificaciones SNMP.

- c. De manera opcional, seleccione o desmarque la casilla de verificación **Habilitar trampas de autenticación** para controlar si el agente SNMP de StorageGRID envía trampas de autenticación cuando recibe mensajes de protocolo autenticados incorrectamente.
4. Si usa SNMPv1 o SNMPv2c, opcionalmente actualice o agregue una **Comunidad de solo lectura** en la sección Cadenas de la comunidad.
 5. Para actualizar los destinos de trampa, seleccione la pestaña Destinos de trampa en la sección Otras configuraciones.

Utilice esta pestaña para definir uno o más destinos para las notificaciones de captura o información de StorageGRID. Cuando habilita el agente SNMP y selecciona **Guardar**, StorageGRID envía notificaciones a cada destino definido cuando se activan alertas. También se envían notificaciones estándar para las entidades MIB-II compatibles (por ejemplo, ifDown y coldStart).

Para obtener detalles sobre qué ingresar, consulte ["Crear destinos de trampa"](#).

- Opcionalmente, actualice o elimine la comunidad de trampas predeterminada.

Si elimina la comunidad de trampa predeterminada, primero debe asegurarse de que todos los destinos de trampa existentes utilicen una cadena de comunidad personalizada.

- Para agregar un destino de trampa, seleccione **Crear**.
- Para editar un destino de trampa, seleccione el botón de opción y seleccione **Editar**.
- Para eliminar un destino de trampa, seleccione el botón de opción y seleccione **Eliminar**.
- Para confirmar los cambios, seleccione **Guardar** en la parte inferior de la página.

6. Para actualizar las direcciones del agente, seleccione la pestaña Direcciones del agente en la sección Otras configuraciones.

Utilice esta pestaña para especificar una o más "direcciones de escucha". Estas son las direcciones StorageGRID en las que el agente SNMP puede recibir consultas.

Para obtener detalles sobre qué ingresar, consulte ["Crear direcciones de agentes"](#).

- Para agregar una dirección de agente, seleccione **Crear**.
- Para editar la dirección de un agente, seleccione el botón de opción y seleccione **Editar**.
- Para eliminar una dirección de agente, seleccione el botón de opción y seleccione **Eliminar**.
- Para confirmar los cambios, seleccione **Guardar** en la parte inferior de la página.

7. Para actualizar los usuarios de USM, seleccione la pestaña Usuarios de USM en la sección Otras configuraciones.

Utilice esta pestaña para definir los usuarios de USM que están autorizados a consultar la MIB o a recibir trampas e informes.

Para obtener detalles sobre qué ingresar, consulte ["Crear usuarios de USM"](#).

- Para agregar un usuario USM, seleccione **Crear**.
- Para editar un usuario USM, seleccione el botón de opción y seleccione **Editar**.

No se puede cambiar el nombre de usuario de un usuario USM existente. Si necesita cambiar un nombre de usuario, debe eliminar el usuario y crear uno nuevo.



Si agrega o elimina el ID de motor autorizado de un usuario y ese usuario está actualmente seleccionado para un destino, debe editar o eliminar el destino. De lo contrario, se produce un error de validación al guardar la configuración del agente SNMP.

- Para eliminar un usuario de USM, seleccione el botón de opción y seleccione **Eliminar**.



Si el usuario que eliminó está actualmente seleccionado para un destino de trampa, debe editar o eliminar el destino. De lo contrario, se produce un error de validación al guardar la configuración del agente SNMP.

- Para confirmar los cambios, seleccione **Guardar** en la parte inferior de la página.

8. Cuando haya actualizado la configuración del agente SNMP, seleccione **Guardar**.

Acceder a archivos MIB

Los archivos MIB contienen definiciones e información sobre las propiedades de los recursos y servicios administrados para los nodos de su red. Puede acceder a los archivos MIB que definen los objetos y las notificaciones para StorageGRID. Estos archivos pueden ser útiles para monitorear su red.

Ver ["Utilice la monitorización SNMP"](#) para obtener más información sobre los archivos SNMP y MIB.

Acceder a archivos MIB

Siga estos pasos para acceder a los archivos MIB.

Pasos

1. Seleccione **CONFIGURACIÓN > Monitoreo > Agente SNMP**.
2. En la página del agente SNMP, seleccione el archivo que desea descargar:
 - **NETAPP-STORAGEGRID-MIB.txt**: Define la tabla de alertas y las notificaciones (trampas) accesibles en todos los nodos de administración.
 - **ES-NETAPP-06-MIB.mib**: Define objetos y notificaciones para dispositivos basados en E-Series.
 - **MIB_1_10.zip**: Define objetos y notificaciones para dispositivos con una interfaz BMC .



También puede acceder a los archivos MIB en la siguiente ubicación en cualquier nodo StorageGRID : `/usr/share/snmp/mibs`

3. Para extraer los OID de StorageGRID del archivo MIB:

- a. Obtenga el OID de la raíz del MIB de StorageGRID :

```
root@user-adm1:~ # snmptranslate -On -IR storagegrid
```

Resultado: `.1.3.6.1.4.1.789.28669` (28669 es siempre el OID para StorageGRID)

- a. Busque el OID de StorageGRID en todo el árbol (usando `paste` para unir líneas):

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



El `snmptranslate` El comando tiene muchas opciones que son útiles para explorar la MIB. Este comando está disponible en cualquier nodo StorageGRID .

Contenido del archivo MIB

Todos los objetos están bajo el OID StorageGRID .

Nombre del objeto	Identificador de objeto (OID)	Descripción
		El módulo MIB para entidades NetApp StorageGRID .

Objetos MIB

Nombre del objeto	Identificador de objeto (OID)	Descripción
recuento de alertas activas		El número de alertas activas en activeAlertTable.
tabla de alerta activa		Una tabla de alertas activas en StorageGRID.
ID de alerta activa		El ID de la alerta. Único en el conjunto actual de alertas activas.
nombreAlertaActiva		El nombre de la alerta.
instancia de alerta activa		El nombre de la entidad que generó la alerta, normalmente el nombre del nodo.
activeAlertSeverity		La gravedad de la alerta.
hora de inicio de alerta activa		La fecha y hora en que se activó la alerta.

Tipos de notificaciones (trampas)

Todas las notificaciones incluyen las siguientes variables como varbinds:

- ID de alerta activa
- nombreAlertaActiva
- instancia de alerta activa
- activeAlertSeverity
- hora de inicio de alerta activa

Tipo de notificación	Identificador de objeto (OID)	Descripción
alerta menor activa		Una alerta con gravedad menor
alerta mayor activa		Una alerta con mayor gravedad
alerta crítica activa		Una alerta con gravedad crítica

Recopilar datos adicionales de StorageGRID

Utilice tablas y gráficos

Puede utilizar gráficos e informes para supervisar el estado del sistema StorageGRID y

solucionar problemas.

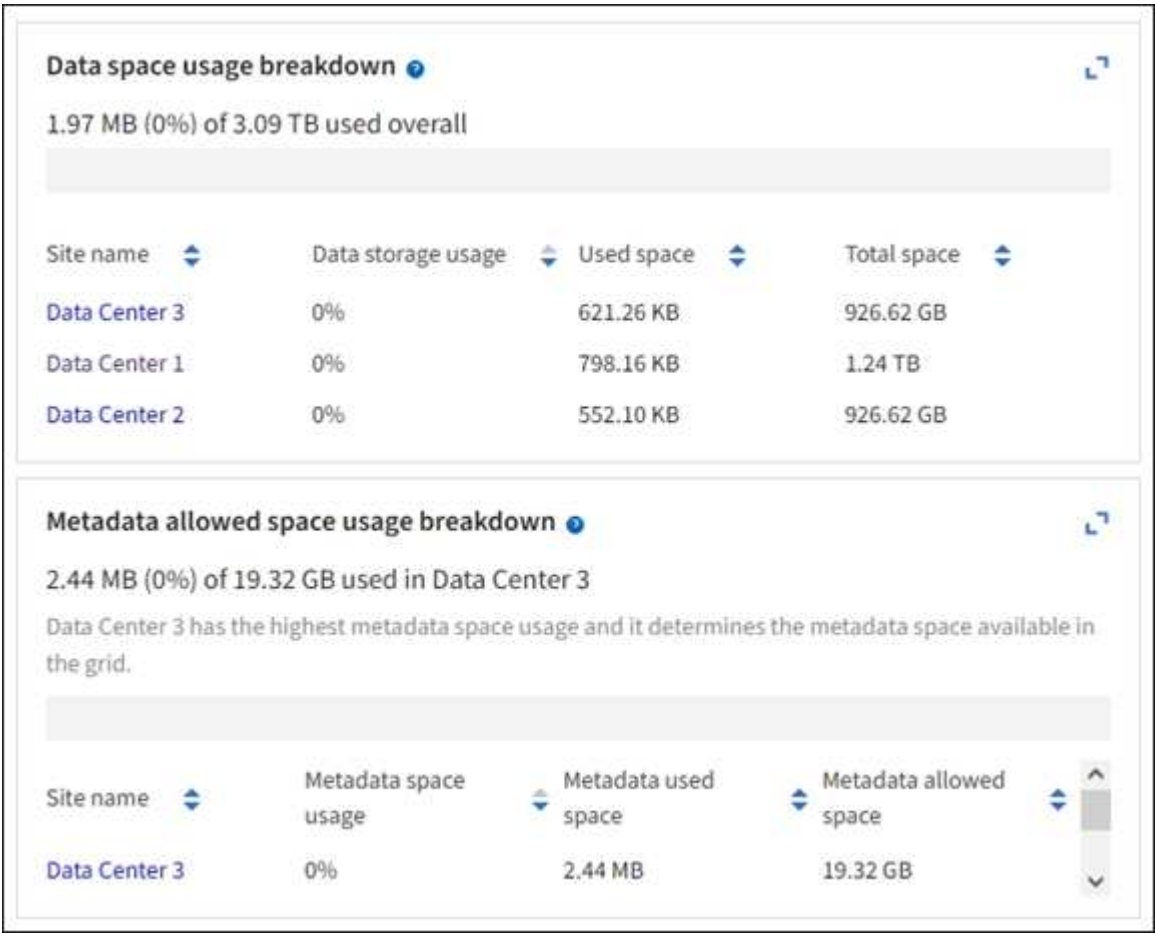


El Grid Manager se actualiza con cada versión y es posible que no coincida con las capturas de pantalla de ejemplo en esta página.

Tipos de gráficos

Los gráficos y tablas resumen los valores de métricas y atributos específicos de StorageGRID .

El panel de control de Grid Manager incluye tarjetas que resumen el almacenamiento disponible para la red y cada sitio.



El panel de uso de almacenamiento en el tablero del Administrador de inquilinos muestra lo siguiente:

- Una lista de los depósitos (S3) o contenedores (Swift) más grandes 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

Dashboard

16 Buckets
[View buckets](#)

2 Platform services
endpoints
[View endpoints](#)

0 Groups
[View groups](#)

1 User
[View users](#)

Storage usage ?

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Top buckets by capacity limit usage ?

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details ?

Name: Tenant02

ID: 3341 1240 0546 8283 2208

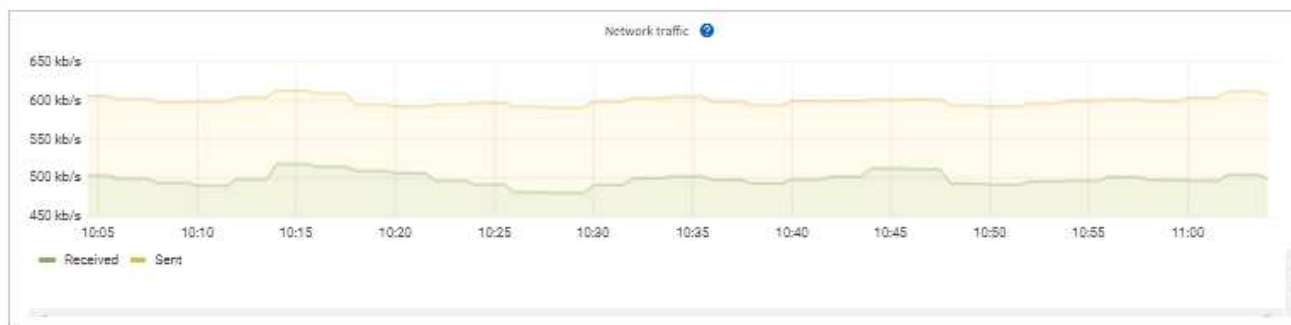
- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

Además, los gráficos que muestran cómo las métricas y los atributos de StorageGRID cambian con el tiempo están disponibles en la página **Nodos** y en la página **SOPORTE > Herramientas > Topología de cuadrícula**.

Hay cuatro tipos de gráficos:

- **Gráficos de Grafana:** Los gráficos de Grafana, que se muestran en la página **Nodos**, se utilizan para trazar los valores de las métricas de Prometheus a lo largo del tiempo. Por ejemplo, la pestaña **NODOS > Red** de un nodo de almacenamiento incluye un gráfico de Grafana para el tráfico de red.

DC1-S2 (Storage Node)

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

Network interfaces

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

Network communication

Receive

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

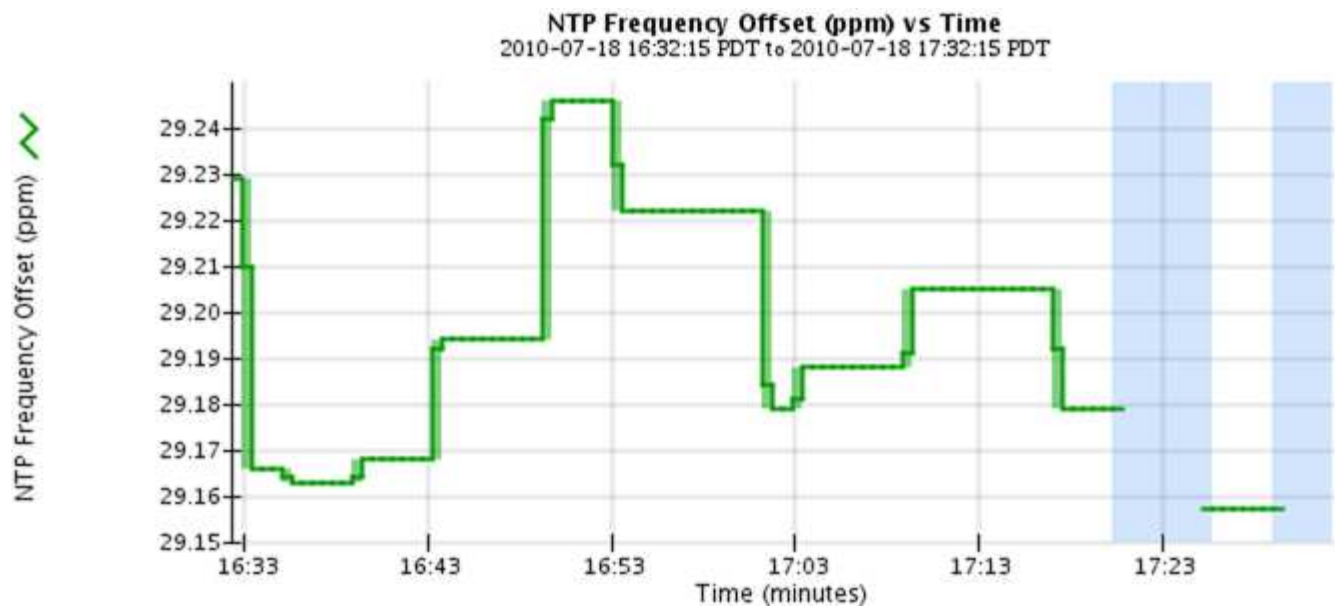
Transmit

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

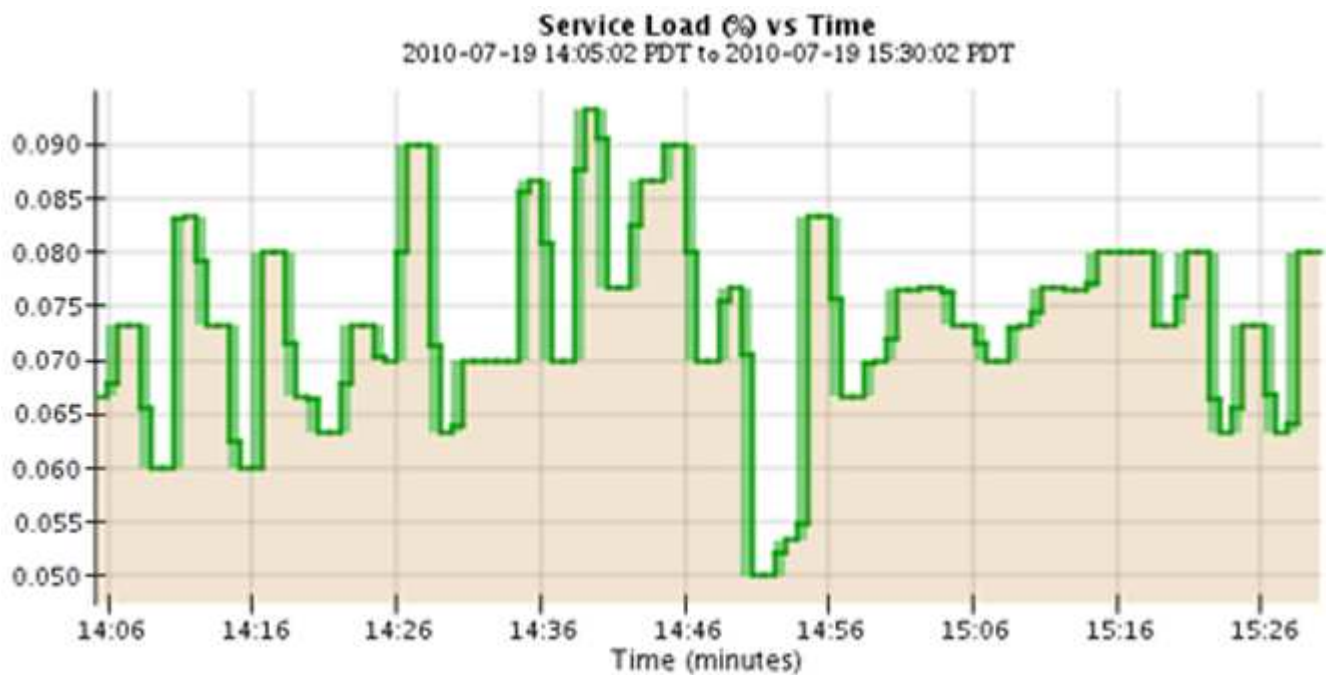


Los gráficos de Grafana también se incluyen en los paneles prediseñados disponibles en la página **SOPORTE > Herramientas > Métricas**.

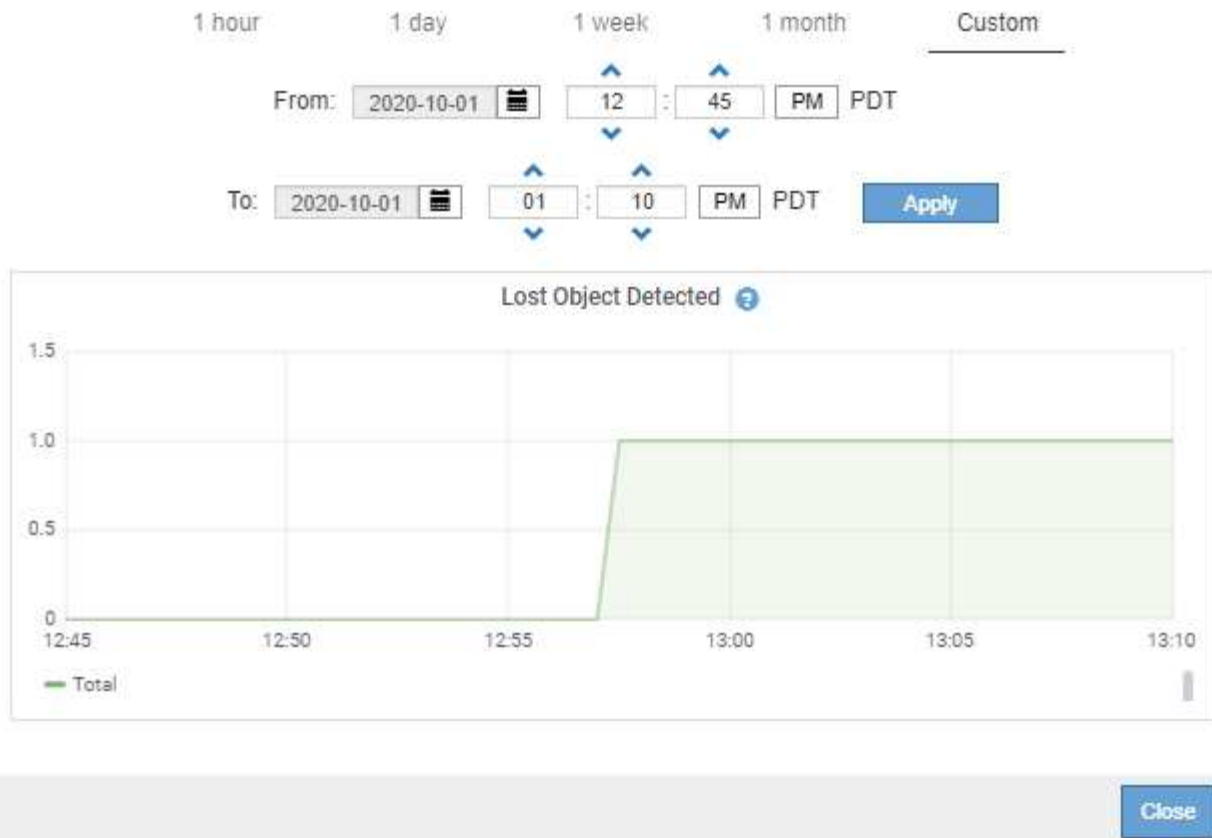
- **Gráficos de líneas:** Disponibles en la página Nodos y en la página **SOPORTE > Herramientas > Topología de cuadrícula** (seleccione el ícono del gráfico  después de un valor de datos), los gráficos de líneas se utilizan para trazar los valores de los atributos de StorageGRID que tienen un valor unitario (como el desplazamiento de frecuencia NTP, en ppm). Los cambios en el valor se grafican en intervalos de datos regulares (contenedores) a lo largo del tiempo.



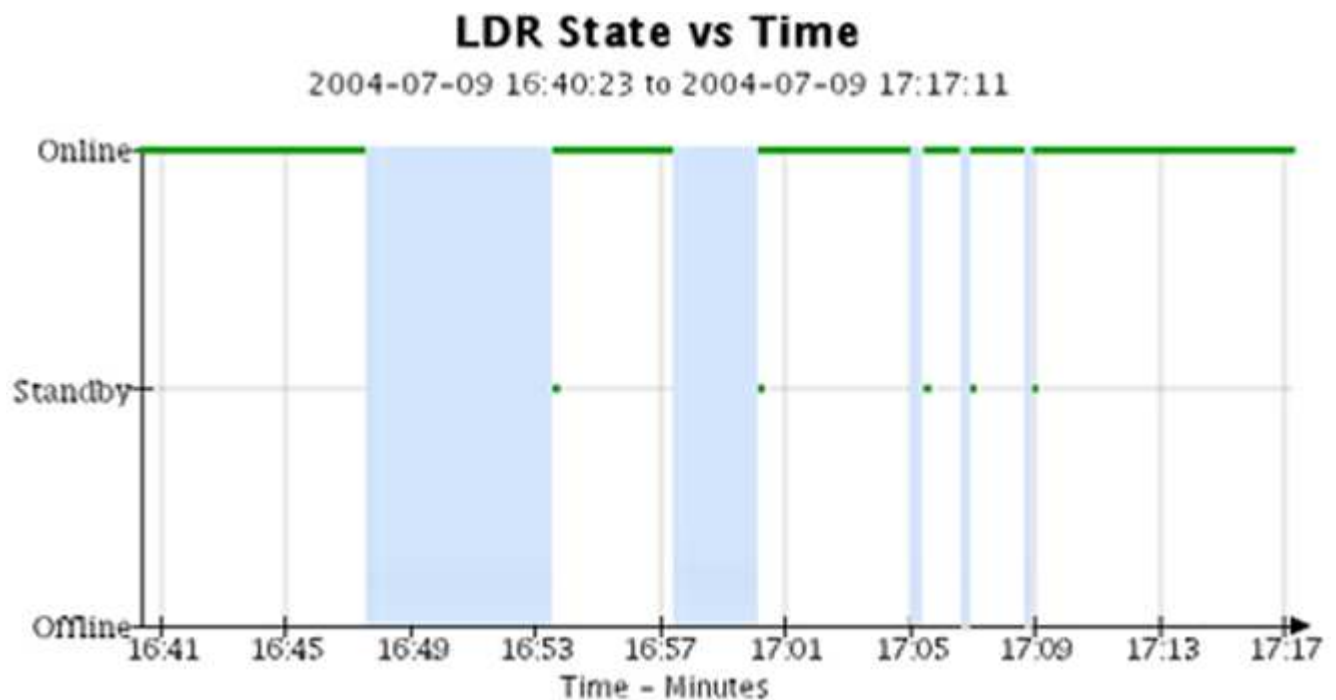
- **Gráficos de área:** Disponibles en la página Nodos y en la página **SOPORTE > Herramientas > Topología de cuadrícula** (seleccione el ícono del gráfico  después de un valor de datos), los gráficos de área se utilizan para trazar cantidades de atributos volumétricos, como recuentos de objetos o valores 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 grafican en intervalos de datos regulares (contenedores) a lo largo del tiempo.



- Algunos gráficos se indican con un tipo de ícono de gráfico diferente.  y tienen un formato diferente:



- **Gráfico de estado:** Disponible en la página **SOPORTE > Herramientas > Topología de cuadrícula** (seleccione el ícono del 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 ser en línea, en espera o fuera de línea. Los gráficos de estados 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

- ["Ver la página de Nodos"](#)
- ["Ver el árbol de topología de la cuadrícula"](#)
- ["Revisar las métricas de soporte"](#)

Leyenda del gráfico

Las líneas y colores utilizados para dibujar gráficos tienen un significado específico.

Ejemplo	Significado
	Los valores de los atributos informados se representan mediante líneas de color verde oscuro.
	El sombreado verde claro alrededor de las líneas verde oscuro indica que los valores reales en ese rango de tiempo varían y han sido agrupados para un trazado más rápido. La línea oscura representa el promedio ponderado. El rango en verde claro indica los valores máximo y mínimo dentro del contenedor. El sombreado marrón claro se utiliza en los gráficos de área para indicar datos volumétricos.
	Las áreas en blanco (sin datos representados) indican que los valores de los atributos no estaban disponibles. El fondo puede ser azul, gris o una mezcla de gris y azul, según el estado del servicio que informa el atributo.
	El sombreado azul claro indica que algunos o todos los valores de los atributos en ese momento eran indeterminados; el atributo no informaba valores porque el servicio estaba en un estado desconocido.
	El sombreado gris indica que algunos o todos los valores de los atributos en ese momento no se conocían porque el servicio que informaba los atributos no estaba disponible administrativamente.
	Una mezcla de sombreado gris y azul indica que algunos de los valores de los atributos en ese momento eran indeterminados (porque el servicio estaba en un estado desconocido), mientras que otros no se conocían porque el servicio que informaba los atributos estaba administrativamente inactivo.

Mostrar gráficos y tablas

La página Nodos contiene gráficos y tablas a los que debe acceder periódicamente para monitorear atributos como la capacidad de almacenamiento y el rendimiento. En algunos casos, especialmente cuando se trabaja con soporte técnico, puede utilizar la página **SOPORTE > Herramientas > Topología de cuadrícula** para acceder a gráficos adicionales.

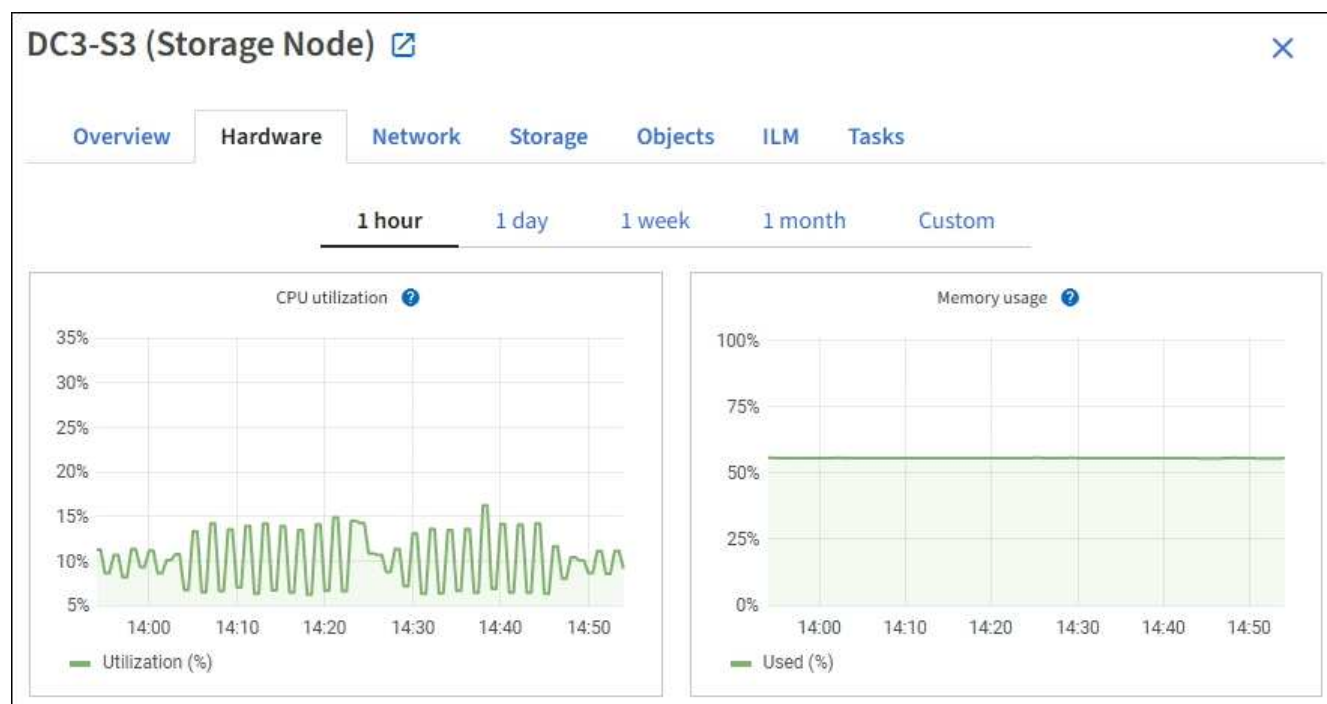
Antes de empezar

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

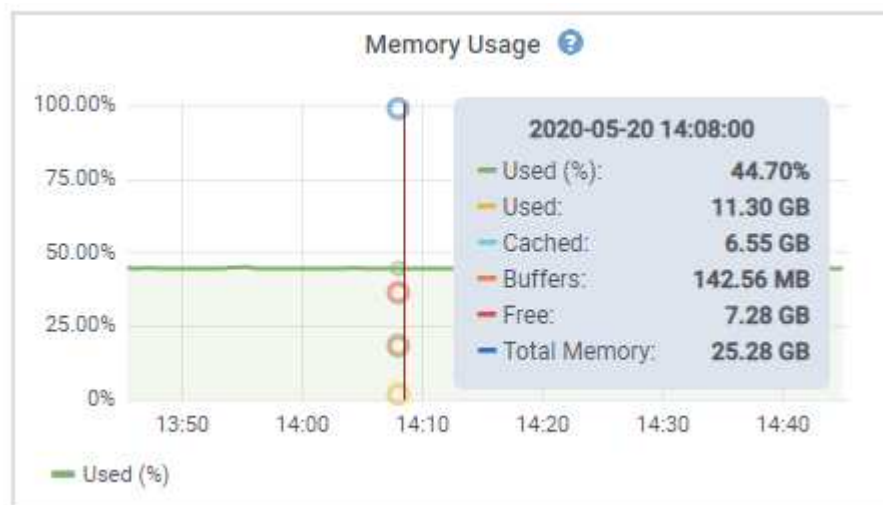
Pasos

1. Seleccione **NODOS**. Luego, seleccione un nodo, un sitio o toda la cuadrícula.
2. Seleccione la pestaña de la que desea ver información.

Algunas pestañas incluyen uno o más gráficos de Grafana, que se utilizan para trazar los valores de las métricas de Prometheus a lo largo del tiempo. Por ejemplo, la pestaña **NODOS > Hardware** de un nodo incluye dos gráficos de Grafana.



- Opcionalmente, coloque el cursor sobre el gráfico para ver valores más detallados para un punto particular en el tiempo.



- Según sea necesario, a menudo puede mostrar un gráfico para un atributo o métrica específicos. Desde la tabla en la página Nodos, seleccione el ícono del gráfico  a la derecha del nombre del atributo.



Los gráficos no están disponibles para todas las métricas y atributos.

Ejemplo 1: Desde la pestaña Objetos de un nodo de almacenamiento, puede seleccionar el ícono del gráfico  para ver el número total de consultas exitosas al almacén de metadatos para el nodo de almacenamiento.



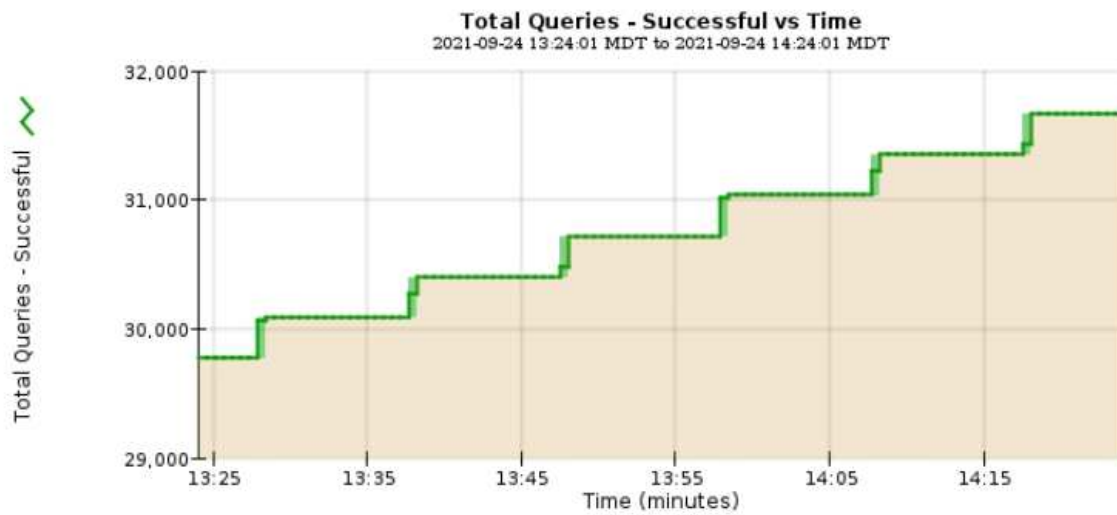
Reports (Charts): DDS (DC1-S1) - Data Store



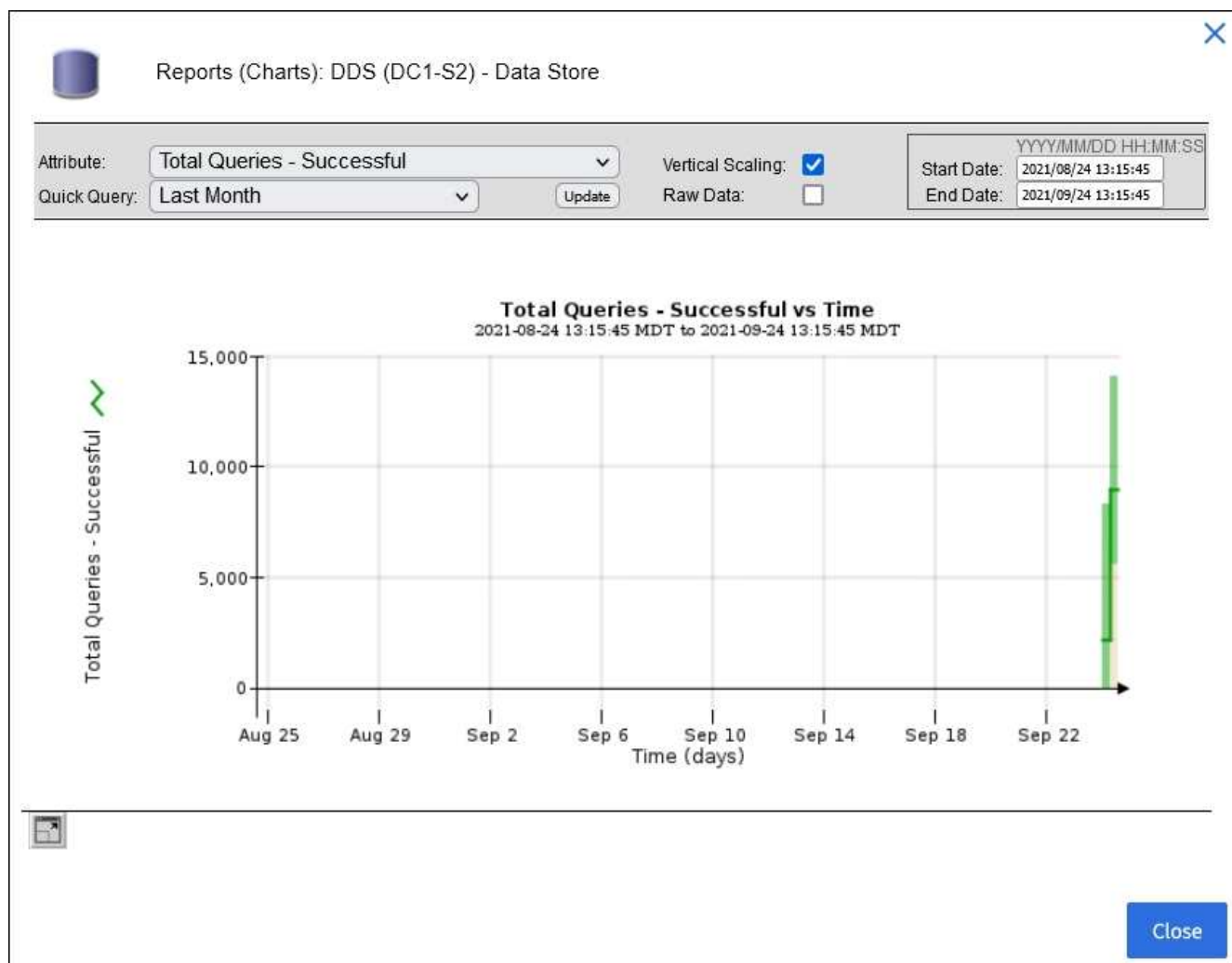
Attribute: Total Queries - Successful
Quick Query: Last Hour Update

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

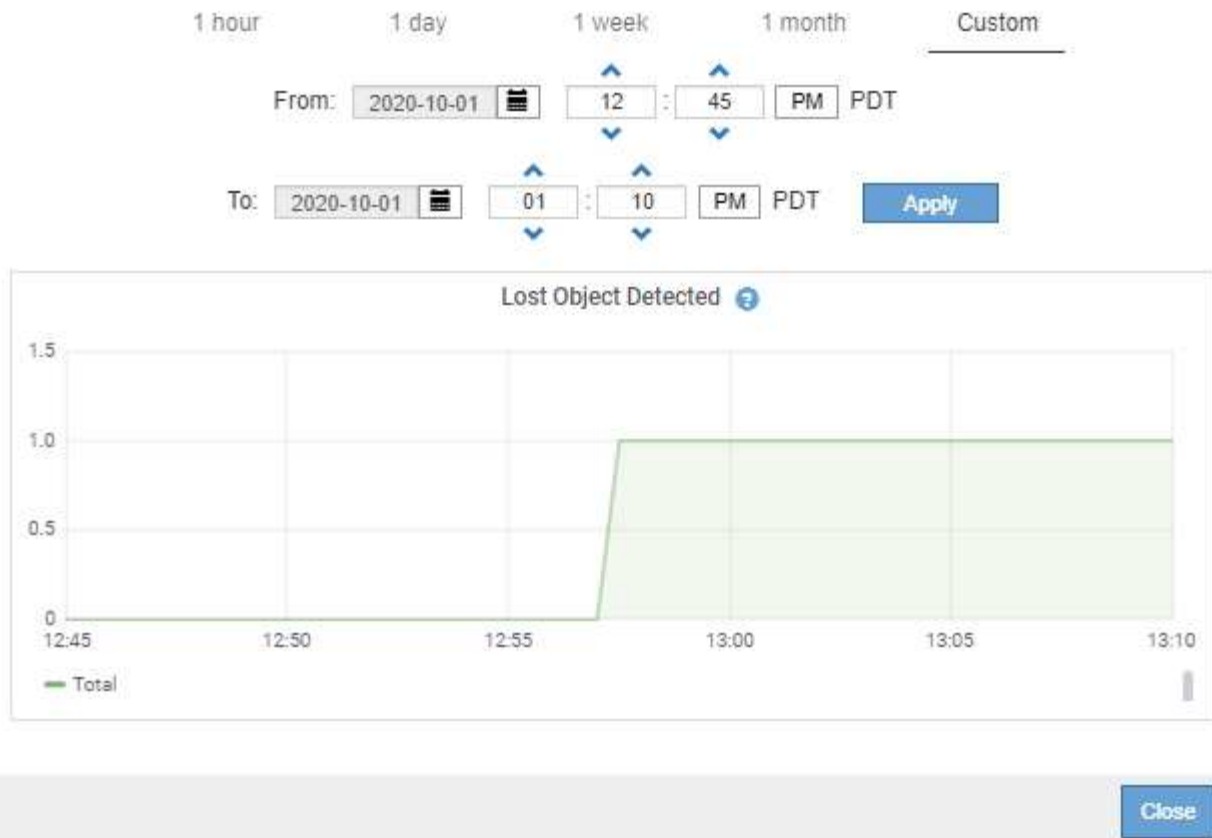


Close



Ejemplo 2: Desde la pestaña Objetos de un nodo de almacenamiento, puede seleccionar el ícono del gráfico  para ver el gráfico de Grafana del recuento de objetos perdidos detectados a lo largo del tiempo.

Object Counts		
Total Objects	1	
Lost Objects	1	
S3 Buckets and Swift Containers	1	



5. Para mostrar gráficos de atributos que no se muestran en la página Nodo, seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
6. Seleccione **nodo de cuadrícula > componente o servicio > Descripción general > Principal**.

Computational Resources

Service Restarts:	1	
Service Runtime:	6 days	
Service Uptime:	6 days	
Service CPU Seconds:	10666 s	
Service Load:	0.266 %	

Memory

Installed Memory:	8.38 GB	
Available Memory:	2.9 GB	

Processors

Processor Number	Vendor	Type	Cache
1	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
2	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
3	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
4	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
5	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
6	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
7	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
8	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB

7. Seleccione el icono del gráfico  junto al atributo.

La pantalla cambia automáticamente a la página **Informes > Gráficos**. El gráfico muestra los datos del atributo durante el último día.

Generar gráficos

Los gráficos muestran una representación gráfica de los valores de los datos de atributos. Puede informar sobre un sitio de centro de datos, un nodo de red, un componente o un servicio.

Antes de empezar

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

Pasos

1. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
2. Seleccione **nodo de cuadrícula > componente o servicio > Informes > Gráficos**.
3. Seleccione el atributo sobre el que desea informar de la lista desplegable **Atributo**.
4. Para forzar que el eje Y comience en cero, desmarque la casilla de verificación **Escala vertical**.
5. Para mostrar valores con total precisión, seleccione la casilla de verificación **Datos sin procesar**, o para

redondear los valores a un máximo de tres decimales (por ejemplo, para atributos informados como porcentajes), desmarque la casilla de verificación **Datos sin procesar**.

6. Seleccione el período de tiempo sobre el que desea informar en la lista desplegable **Consulta rápida**.

Seleccione la opción Consulta personalizada para seleccionar un rango de tiempo específico.

El gráfico aparece después de unos momentos. Deje pasar varios minutos para la tabulación de rangos de tiempo largos.

7. Si seleccionó Consulta personalizada, personalice el período de tiempo para el gráfico ingresando la **Fecha de inicio** y la **Fecha de finalización**.

Utilice el formato `YYYY/MM/DDHH:MM:SS` en hora local. Se requieren ceros a la izquierda para que coincida con el formato. Por ejemplo, 2017/4/6 7:30:00 no pasa la validación. El formato correcto es: 2017/04/06 07:30:00.

8. Seleccione **Actualizar**.

Se genera un gráfico después de unos segundos. Deje pasar varios minutos para la tabulación de rangos de tiempo largos. Dependiendo del período de tiempo establecido para la consulta, se muestra un informe de texto sin procesar o un informe de texto agregado.

Utilice informes de texto

Los informes de texto muestran una representación textual de los valores de datos de atributos que han sido procesados por el servicio NMS. Hay dos tipos de informes generados según el período de tiempo sobre el que esté informando: informes de texto sin procesar para períodos inferiores a una semana e informes de texto agregados para períodos superiores a una semana.

Informes de texto sin procesar

Un informe de texto sin formato muestra detalles sobre el atributo seleccionado:

- Hora de recepción: fecha y hora locales en que el servicio NMS procesó un valor de muestra de los datos de un atributo.
- Hora de muestra: fecha y hora locales en las que se muestreó o modificó un valor de atributo en la fuente.
- Valor: Valor del atributo en el momento 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 datos durante un período de tiempo más largo (normalmente una semana) que un informe de texto sin procesar. Cada entrada es el resultado de resumir múltiples valores de atributos (un agregado de valores de atributos) por parte del servicio NMS a lo largo del tiempo en una única entrada con valores promedio, máximos y mínimos que se derivan de la agregación.

Cada entrada muestra la siguiente información:

- Hora agregada: última fecha y hora local en que el servicio NMS agregó (recopiló) un conjunto de valores de atributos modificados.
- Valor promedio: el promedio del valor del atributo durante el período de tiempo agregado.
- Valor mínimo: el valor mínimo durante el período de tiempo agregado.
- Valor máximo: el 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 han sido procesados por el servicio NMS. Puede informar sobre un sitio de centro de datos, un nodo de red, un componente o un servicio.

Antes de empezar

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

Acerca de esta tarea

En el caso de los datos de atributos que se espera que cambien continuamente, el servicio NMS muestrea dichos datos (en la fuente) a intervalos regulares. Para los datos de atributos que cambian con poca frecuencia (por ejemplo, datos basados en eventos como cambios de estado o estatus), se envía un valor de atributo al servicio NMS cuando el valor cambia.

El tipo de informe que se muestra depende del período de tiempo configurado. De forma predeterminada, los informes de texto agregados se generan para períodos de tiempo superiores a una semana.

El texto gris indica que el servicio estuvo administrativamente inactivo durante el tiempo en que se muestreó. El texto azul indica que el servicio estaba en un estado desconocido.

Pasos

1. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
2. Seleccione **nodo de cuadrícula > componente o servicio > Informes > Texto**.
3. Seleccione el atributo sobre el que desea informar de la lista desplegable **Atributo**.
4. Seleccione el número de resultados por página de la lista desplegable **Resultados por página**.
5. Para redondear valores a un máximo de tres decimales (por ejemplo, para atributos informados como porcentajes), desmarque la casilla de verificación **Datos sin procesar**.
6. Seleccione el período de tiempo sobre el que desea informar en la lista desplegable **Consulta rápida**.

Seleccione la opción Consulta personalizada para seleccionar un rango de tiempo específico.

El informe aparece después de unos momentos. Deje pasar varios minutos para la tabulación de rangos de tiempo largos.

- Si seleccionó Consulta personalizada, debe personalizar el período de tiempo sobre el que se realizará el informe ingresando la **Fecha de inicio** y la **Fecha de finalización**.

Utilice el formato YYYY/MM/DDHH:MM:SS en hora local. Se requieren ceros a la izquierda para que coincida con el formato. Por ejemplo, 2017/4/6 7:30:00 no pasa la validación. El formato correcto es: 2017/04/06 07:30:00.

- Haga clic en **Actualizar**.

Se genera un informe de texto después de unos momentos. Deje pasar varios minutos para la tabulación de rangos de tiempo largos. Dependiendo del período de 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 le permite seleccionar y copiar los datos.

Acerca de esta tarea

Luego, los datos copiados se pueden guardar en un nuevo documento (por ejemplo, una hoja de cálculo) y utilizar para analizar el rendimiento del sistema StorageGRID .

Pasos

- Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
- Crear un informe de texto.
- Haga clic en *Exportar*.

OverviewAlarmsReportsConfiguration

ChartsText

**Reports (Text): SSM (170-176) - Events**

Attribute: Attribute Send to Relay RateResults Per Page: 5Quick Query: Custom QueryUpdateRaw Data: ☒

YYYY/MM/DD HH:MM:SSStart Date: 2010/07/19 08:42:09End Date: 2010/07/20 08:42:09

Text Results for Attribute Send to Relay Rate
2010-07-19 08:42:09 PDT To 2010-07-20 08:42:09 PDT

1 - 5 of 254

Time Received	Sample Time	Value
2010-07-20 08:40:46	2010-07-20 08:40:46	0.274981485 Messages/s
2010-07-20 08:38:46	2010-07-20 08:38:46	0.274989 Messages/s
2010-07-20 08:36:46	2010-07-20 08:36:46	0.283317543 Messages/s
2010-07-20 08:34:46	2010-07-20 08:34:46	0.274982493 Messages/s
2010-07-20 08:32:46	2010-07-20 08:32:46	0.291646426 Messages/s

Previous « 1 2 3 4 5 » Next

Se abre la ventana Exportar informe de texto mostrando 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 ahora se pueden pegar en un documento de terceros, como una hoja de cálculo.

Supervisar el rendimiento de PUT y GET

Puede supervisar el rendimiento de determinadas operaciones, como el almacenamiento y la recuperación de objetos, para ayudar a identificar cambios que podrían requerir una mayor investigación.

Acerca de esta tarea

Para supervisar el rendimiento de PUT y GET, puede ejecutar comandos S3 directamente desde una estación de trabajo o utilizando la aplicación de código abierto S3tester. El uso de estos métodos le 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 operaciones PUT y GET, utilice las siguientes pautas:

- Utilice tamaños de objetos comparables a los objetos que normalmente ingiere en su cuadrícula.
- Realizar operaciones contra sitios tanto locales como remotos.

Mensajes en el "[registro de auditoría](#)" Indica el tiempo total necesario para ejecutar determinadas operaciones. Por ejemplo, para determinar el tiempo total de procesamiento de una solicitud GET de S3, puede revisar el valor del atributo TIME en el mensaje de auditoría de SGET. También puede encontrar el atributo TIME en los mensajes de auditoría para las siguientes operaciones de S3: DELETE, GET, HEAD, Metadata Updated, POST, PUT

Al analizar los resultados, observe el tiempo promedio necesario para satisfacer una solicitud, así como el rendimiento general que puede lograr. Repita las mismas pruebas periódicamente y registre los resultados, para que pueda identificar tendencias que podrían requerir investigación.

- Puede ["Descargar S3tester desde GitHub"](#) .

Supervisar las operaciones de verificación de objetos

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

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de mantenimiento o acceso root"](#) .

Acerca de esta tarea

Dos ["procesos de verificación"](#) Trabajar juntos para garantizar la integridad de los datos:

- La **verificación de antecedentes** se ejecuta automáticamente y verifica continuamente la exactitud de los datos del objeto.

La verificación de antecedentes verifica de forma automática y continua todos los nodos de almacenamiento para determinar si hay copias corruptas de datos de objetos replicados y codificados para borrado. Si se encuentran problemas, el sistema StorageGRID intenta automáticamente reemplazar los datos de los objetos dañados desde copias almacenadas en otras partes del sistema. La verificación en segundo plano no se ejecuta en objetos de un grupo de almacenamiento en la nube.



La alerta **Objeto corrupto no identificado detectado** se activa si el sistema detecta un objeto corrupto que no se puede corregir automáticamente.

- Un usuario puede activar la **verificación de existencia de objeto** para verificar más rápidamente la existencia (aunque no la exactitud) de los datos del objeto.

La verificación de existencia de objetos verifica si todas las copias replicadas esperadas de objetos y fragmentos codificados de borrado existen en un nodo de almacenamiento. La verificación de existencia de objetos proporciona una manera de verificar la integridad de los dispositivos de almacenamiento, especialmente si un problema de hardware reciente pudo haber afectado la integridad de los datos.

Debe revisar periódicamente los resultados de las verificaciones de antecedentes y las comprobaciones de existencia de objetos. Investigue inmediatamente cualquier instancia de datos de objetos corruptos o faltantes para determinar la causa raíz.

Pasos

1. Revise los resultados de las verificaciones de antecedentes:
 - a. Seleccione **NODOS > Nodo de almacenamiento > Objetos**.
 - b. Compruebe los resultados de la verificación:
 - Para comprobar la verificación de datos de objetos replicados, mire los atributos en la sección Verificación.

Verification		
Status: ?	No errors	
Percent complete: ?	0.00%	
Average stat time: ?	0.00 microseconds	
Objects verified: ?	0	
Object verification rate: ?	0.00 objects / second	
Data verified: ?	0 bytes	
Data verification rate: ?	0.00 bytes / second	
Missing objects: ?	0	
Corrupt objects: ?	0	
Corrupt objects unidentified: ?	0	
Quarantined objects: ?	0	

- Para comprobar la verificación del fragmento codificado de borrado, seleccione **Storage Node > ILM** y observe los atributos en la sección Verificación de codificación de borrado.

Erasure coding verification		
Status: ?	Idle	
Next scheduled: ?	2021-10-08 10:45:19 MDT	
Fragments verified: ?	0	
Data verified: ?	0 bytes	
Corrupt copies: ?	0	
Corrupt fragments: ?	0	
Missing fragments: ?	0	

Seleccione el signo de interrogación ? junto al nombre de un atributo para mostrar el texto de ayuda.

- Revise los resultados de los trabajos de verificación de existencia de objetos:
 - Seleccione **MANTENIMIENTO > Verificación de existencia de objetos > Historial de trabajos**.
 - Escanee la columna Copias de objetos faltantes detectadas. Si alguno de los trabajos generó 100 o más copias de objetos faltantes y se activó la alerta **Objetos perdidos**, comuníquese con el soporte técnico.

Object existence check

Perform an object existence check if you suspect storage volumes have been damaged or are corrupt. You can verify that objects defined by your ILM policy, still exist on the volumes.

Active job

Job history

Delete

Search...

☐

Job ID ?

Status ?

Nodes (volumes) ?

Missing object copies detected ?

☐

15816859223101303015

Completed

DC2-S1 (3 volumes)

0

☐

12538643155010477372

Completed

DC1-S3 (1 volume)

0

☐

5490044849774982476

Completed

DC1-S2 (1 volume)

0

☐

3395284277055907678

Completed

DC1-S1 (3 volumes)
DC1-S2 (3 volumes)
DC1-S3 (3 volumes)
and 7 more

0

Monitorear eventos

Puede supervisar eventos detectados por un nodo de la red, incluidos eventos personalizados que haya creado para rastrear eventos que se registran en el servidor syslog. El mensaje Último evento que se muestra en el Administrador de cuadrícula proporciona más información sobre el evento más reciente.

Los mensajes de eventos también se enumeran en el `/var/local/log/bycast-err.log` archivo de registro. Ver el ["Referencia de archivos de registro"](#).

La alarma SMTT (Total de eventos) puede activarse repetidamente por problemas como problemas de red, cortes de energía o actualizaciones. Esta sección contiene información sobre cómo investigar eventos para que pueda comprender mejor por qué se produjeron estas alarmas. Si se produjo un evento debido a un problema conocido, es seguro restablecer los contadores de eventos.

Pasos

- Revise los eventos del sistema para cada nodo de la red:
 - Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
 - Seleccione **sitio > nodo de cuadrícula > SSM > Eventos > Descripción general > Principal**.
- Genere una lista de mensajes de eventos anteriores para ayudar a aislar problemas que ocurrieron en el pasado:

- Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
- Seleccione **sitio > nodo de cuadrícula > SSM > Eventos > Informes**.
- Seleccionar **Texto**.

El atributo **Último evento** no se muestra en el "vista de gráficos". Para verlo:

- Cambiar **Atributo** a **Último evento**.
- Opcionalmente, seleccione un período de tiempo para la **Consulta rápida**.
- Seleccione **Actualizar**.

Reports (Text): SSM (170-41) - Events

Attribute: Results Per Page: Start Date: End Date:

Quick Query: Raw Data: ☒

Text Results for Last Event
2009-04-15 15:19:53 PDT To 2009-04-15 15:24:53 PDT

1 - 2 of 2

Time Received	Sample Time	Value
2009-04-15 15:24:22	2009-04-15 15:24:22	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }
2009-04-15 15:24:11	2009-04-15 15:23:39	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }

Crear eventos de syslog personalizados

Los eventos personalizados le permiten rastrear todos los eventos de usuario de nivel crítico, error, daemon y kernel registrados en el servidor syslog. Un evento personalizado puede ser útil para monitorear la ocurrencia de mensajes de registro del sistema (y, por lo tanto, eventos de seguridad de red y fallas de hardware).

Acerca de esta tarea

Considere crear eventos personalizados para monitorear problemas recurrentes. Las siguientes consideraciones se aplican a los eventos personalizados.

- Después de crear un evento personalizado, se supervisa cada una de sus ocurrencias.
- Para crear un evento personalizado basado en palabras clave en el `/var/local/log/messages` archivos, los registros en esos archivos deben ser:
 - Generado por el kernel
 - Generado por el demonio o programa de usuario en el nivel de error o crítico

Nota: No todas las entradas en el `/var/local/log/messages` Los archivos se combinarán a menos que cumplan los requisitos establecidos anteriormente.

Pasos

- Seleccione **SOPORTE > Alarmas (heredadas) > Eventos personalizados**.
- Haga clic en ***Editar*** (o ***Insertar*** si este no es el primer evento).

3. Introduzca una cadena de evento personalizada, por ejemplo, apagado

Events
Updated: 2021-10-22 11:15:34 MDT

Custom Events (1 - 1 of 1)

Event	Actions
shutdown	

Show 10 Records Per Page Refresh Previous 1 Next

Apply Changes

4. Seleccione **Aplicar cambios**.

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

6. Seleccione **nodo de cuadrícula > SSM > Eventos**.

7. Localice la entrada de Eventos personalizados en la tabla Eventos y supervise el valor de **Count**.

Si el recuento aumenta, se activará un evento personalizado que estás monitoreando en ese nodo de la cuadrícula.

Overview
Alarms
Reports
Configuration

Main



Overview: SSM (DC1-ADM1) - Events
Updated: 2021-10-22 11:19:18 MDT

System Events

Log Monitor State: Connected
Total Events: 0
Last Event: No Events

Description	Count
Abnormal Software Events	0
Account Service Events	0
Cassandra Errors	0
Cassandra Heap Out Of Memory Errors	0
Chunk Service Events	0
Custom Events	0
Data-Mover Service Events	0
File System Errors	0
Forced Termination Events	0
Grid Node Errors	0
Hotfix Installation Failure Events	0
I/O Errors	0
IDE Errors	0
Identity Service Events	0
Kernel Errors	0
Kernel Memory Allocation Failure	0
Keystone Service Events	0
Network Receive Errors	0
Network Transmit Errors	0
Out Of Memory Errors	0
Replicated State Machine Service Events	0
SCSI Errors	0

Restablecer el recuento de eventos personalizados a cero

Si desea restablecer el contador solo para eventos personalizados, debe utilizar la página Topología de cuadrícula en el menú Soporte.

Al reiniciar un contador, la alarma se activará en el siguiente evento. Por el contrario, cuando se reconoce una alarma, dicha alarma solo se vuelve a activar si se alcanza el siguiente nivel de umbral.

Pasos

1. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
2. Seleccione **grid node > SSM > Eventos > Configuración > Principal**.
3. Seleccione la casilla de verificación **Restablecer** para Eventos personalizados.

Overview

Alarms

Reports

Configuration

Main

Alarms



Configuration: SSM (DC2-ADM1) - Events

Updated: 2018-04-11 10:35:44 MDT

Description	Count	Reset
Abnormal Software Events	0	☐
Account Service Events	0	☐
Cassandra Errors	0	☐
Cassandra Heap Out Of Memory Errors	0	☐
Custom Events	0	☒
File System Errors	0	☐
Forced Termination Events	0	☐

4. Seleccione **Aplicar cambios**.

Revisar los mensajes de auditoría

Los mensajes de auditoría pueden ayudarle a comprender mejor las operaciones detalladas de su sistema StorageGRID . Puede utilizar 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, como se indica a continuación:

- Los mensajes de auditoría del sistema están relacionados con el sistema de auditoría en sí, los estados de los nodos de la red, la actividad de las tareas de todo el sistema y las operaciones de respaldo del servicio.
- Los mensajes de auditoría de almacenamiento de objetos están relacionados con el almacenamiento y la administración de objetos dentro de StorageGRID, incluido el almacenamiento y la recuperación de objetos, las transferencias de nodo de red a nodo de red y las verificaciones.
- Los mensajes de auditoría de lectura y escritura del cliente se registran cuando una aplicación cliente S3 realiza una solicitud para crear, modificar o recuperar un objeto.
- Los mensajes de auditoría de administración registran las solicitudes de los usuarios a la API de administración.

Cada nodo de administración almacena mensajes de auditoría en archivos de texto. El recurso compartido de auditoría contiene el archivo activo (audit.log), así como registros de auditoría comprimidos de días anteriores. Cada nodo de la red también almacena una copia de la información de auditoría generada en el nodo.

Puede acceder a los archivos de registro de auditoría directamente desde la línea de comando del nodo de administración.

StorageGRID puede enviar información de auditoría de forma predeterminada, o puede cambiar el destino:

- StorageGRID tiene como valor predeterminado los destinos de auditoría de nodos locales.
- Las entradas del registro de auditoría de Grid Manager y Tenant Manager podrían enviarse a un nodo de almacenamiento.
- Opcionalmente, puede cambiar el destino de los registros de auditoría y enviar información de auditoría a un servidor syslog externo. Los registros locales de registros de auditoría continúan generándose y almacenándose cuando se configura un servidor syslog externo.
- ["Obtenga información sobre cómo configurar mensajes de auditoría y destinos de registro"](#) .

Para obtener detalles sobre el archivo de registro de auditoría, el formato de los mensajes de auditoría, los tipos de mensajes de auditoría y las herramientas disponibles para analizar los mensajes de auditoría, consulte ["Revisar los registros de auditoría"](#) .

Recopilar archivos de registro y datos del sistema

Puede utilizar Grid Manager para recuperar archivos de registro y datos del sistema (incluidos los datos de configuración) para su sistema StorageGRID .

Antes de empezar

- Debe iniciar sesión en el Administrador de cuadrícula en el nodo de administración principal mediante un ["navegador web compatible"](#) .
- Tienes ["permisos de acceso específicos"](#) .
- Debe tener la contraseña de aprovisionamiento.

Acerca de esta tarea

Puede utilizar el Administrador de cuadrícula para recopilar ["archivos de registro"](#) , datos del sistema y datos de configuración de cualquier nodo de la red durante el período de tiempo que seleccione. Los datos se recopilan y archivan en un archivo .tar.gz que luego puedes descargar a tu computadora local.

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

Pasos

1. Seleccione **SOPORTE > Herramientas > Registros**.

2. Seleccione los nodos de la cuadrícula para los que desea recopilar archivos de registro.

Según sea necesario, puede recopilar archivos de registro para toda la red o para todo el sitio del centro de datos.

3. Seleccione una **Hora de inicio** y una **Hora de finalización** para establecer el rango 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 en una cuadrícula grande, el archivo de registros podría volverse demasiado grande para almacenarse en un nodo o demasiado grande para recopilarse en el nodo de administración principal para su descarga. Si esto ocurre, deberá reiniciar la recopilación de registros con un conjunto de datos más pequeño.

4. Seleccione los tipos de registros que desea recopilar.

- **Registros de aplicaciones:** registros específicos de la aplicación que el soporte técnico utiliza con mayor frecuencia para solucionar problemas. Los registros recopilados son un subconjunto de los registros de aplicaciones disponibles.
- **Registros de auditoría:** Registros que contienen los mensajes de auditoría generados durante el funcionamiento normal del sistema.
- **Rastreo de red:** registros utilizados para la depuración de red.
- **Base de datos Prometheus:** métricas de series temporales de los servicios en todos los nodos.

5. Opcionalmente, ingrese notas sobre los archivos de registro que está recopilando en el cuadro de texto **Notas**.

Puede utilizar estas notas para brindar al soporte técnico información sobre el problema que le llevó a

recopilar los archivos de registro. Sus notas se agregan a un archivo llamado `info.txt`, junto con otra información sobre la recopilación de archivos de registro. El `info.txt` El archivo se guarda en el paquete de archivo de registro.

6. Ingrese la frase de contraseña de aprovisionamiento para su sistema StorageGRID en el cuadro de texto **Frase de contraseña de aprovisionamiento**.

7. Seleccione **Recopilar registros**.

Cuando envía una nueva solicitud, se elimina la colección anterior de archivos de registro.

Puede utilizar la página Registros para supervisar el progreso de la recopilación de archivos de registro para cada nodo de la cuadrícula.

Si recibe un mensaje de error sobre el tamaño del registro, intente recopilar registros durante un período de tiempo más corto o para menos nodos.

8. Seleccione **Descargar** cuando se complete la recopilación del archivo de registro.

El archivo `.tar.gz` contiene todos los archivos de registro de todos los nodos de la red donde la recopilación de registros fue exitosa. Dentro del archivo combinado `.tar.gz`, hay un archivo de registro para cada nodo de la red.

Después de terminar

Puede volver a descargar el paquete de almacenamiento de archivos de registro más tarde si lo necesita.

Opcionalmente, puede seleccionar **Eliminar** para eliminar el paquete de archivo de registro y liberar espacio en el disco. El paquete de archivo de registro actual se elimina automáticamente la próxima vez que se recopilan archivos de registro.

Activar manualmente un paquete de AutoSupport

Para ayudar al soporte técnico a solucionar problemas con su sistema StorageGRID, puede activar manualmente el envío de un paquete de AutoSupport.

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Debe tener acceso de root u otro permiso de configuración de red.

Pasos

1. Seleccione **SOPORTE > Herramientas > * AutoSupport***.
2. En la pestaña **Acciones**, seleccione **Enviar AutoSupport activado por el usuario**.

StorageGRID intenta enviar un paquete de AutoSupport al sitio de soporte de NetApp. Si el intento es exitoso, se actualizan los valores **Resultado más reciente** y **Última vez exitoso** en la pestaña **Resultados**. Si hay un problema, el valor **Resultado más reciente** se actualiza a "Error" y StorageGRID no intenta enviar el paquete AutoSupport nuevamente.

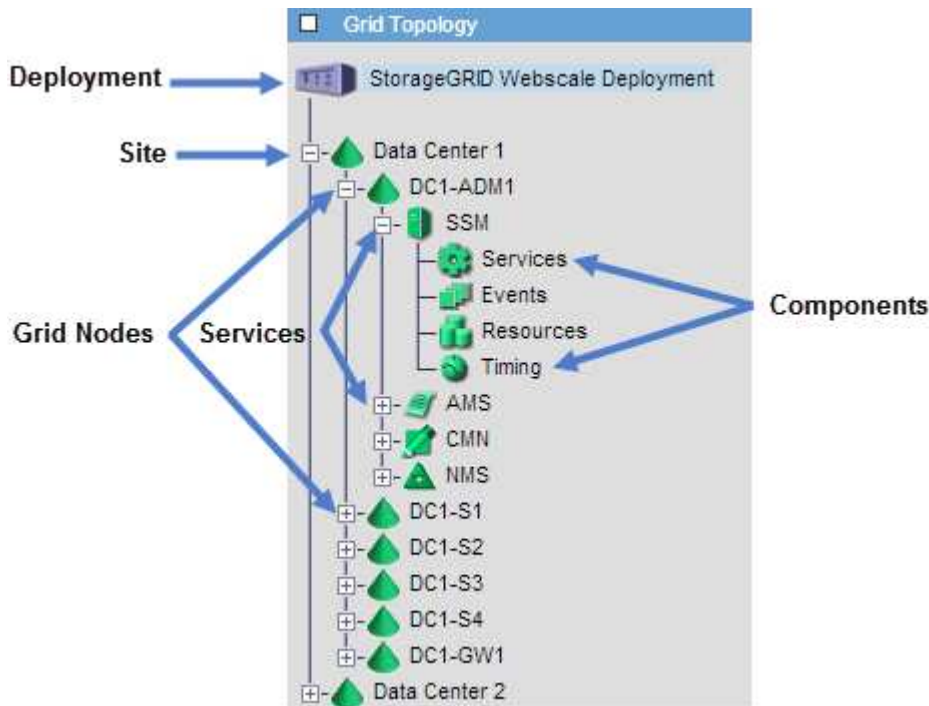


Después de enviar un paquete de AutoSupport activado por el usuario, actualice la página de AutoSupport en su navegador después de 1 minuto para acceder a los resultados más recientes.

Ver el árbol de topología de la cuadrícula

El árbol de topología de cuadrícula proporciona acceso a información detallada sobre los elementos del sistema StorageGRID , incluidos sitios, nodos de cuadrícula, servicios y componentes. En la mayoría de los casos, solo necesita acceder al árbol de topología de la cuadrícula cuando se lo indique la documentación o cuando trabaje con soporte técnico.

Para acceder al árbol de topología de cuadrícula, seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.



Para expandir o contraer el árbol de topología de cuadrícula, haga clic en **+** o **-** en el nivel de sitio, nodo o servicio. Para expandir o contraer todos los elementos en todo el sitio o en cada nodo, mantenga presionada la tecla **<Ctrl>** y haga clic.

Atributos de StorageGRID

Los atributos informan 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 Administrador de cuadrícula:

- **Página Nodos:** Muchos de los valores que se muestran en la página Nodos son atributos de StorageGRID . (Las métricas de Prometheus también se muestran en las páginas de Nodos).
- **Árbol de topología de cuadrícula:** los valores de los atributos se muestran en el árbol de topología de cuadrícula (**SOPORTE > Herramientas > Topología de cuadrícula**).
- **Eventos:** Los eventos del sistema ocurren cuando ciertos atributos registran un error o una condición de falla para un nodo, incluidos errores como errores de red.

Valores de los atributos

Los atributos se informan según el método del máximo esfuerzo y son aproximadamente correctos. Las actualizaciones de atributos se pueden perder en algunas circunstancias, como por ejemplo, si se produce un fallo de un servicio o si falla y se vuelve a crear un nodo de la red.

Además, los retrasos en la propagación podrían ralentizar la notificación de atributos. Los valores actualizados de la mayoría de los atributos se envían al sistema StorageGRID a intervalos fijos. Pueden pasar varios minutos antes de que una actualización sea visible en el sistema, y dos atributos que cambian más o menos simultáneamente pueden informarse en momentos ligeramente diferentes.

Revisar las métricas de soporte

Al solucionar un problema, puede trabajar con el soporte técnico para revisar métricas y gráficos detallados de su sistema StorageGRID .

Antes de empezar

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

Acerca de esta tarea

La página Métricas le permite acceder 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 a ser utilizadas por el soporte técnico. Algunas funciones y elementos del menú de estas herramientas no son funcionales intencionalmente y están sujetos a cambios. Ver la lista de ["Métricas de Prometheus de uso común"](#) .

Pasos

1. Según las indicaciones del soporte técnico, seleccione **SOPORTE > Herramientas > Métricas**.

Aquí se muestra un ejemplo de la página Métricas:

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://\[redacted\]](https://[redacted])

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	EC Overview	Replicated Read Path Overview
Account Service Overview	Grid	S3 - Node
Alertmanager	ILM	S3 Overview
Audit Overview	Identity Service Overview	S3 Select
Cassandra Cluster Overview	Ingests	Site
Cassandra Network Overview	Node	Support
Cassandra Node Overview	Node (Internal Use)	Traces
Cross Grid Replication	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	

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 en la sección Prometheus.

Aparece la interfaz de Prometheus. Puede utilizar esta interfaz para ejecutar consultas sobre las métricas de StorageGRID disponibles y para graficar las métricas de StorageGRID a lo largo del tiempo.



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

3. Para acceder a paneles prediseñados 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 que seleccionó.



Ejecutar diagnósticos

Al solucionar un problema, puede trabajar con el soporte técnico para ejecutar diagnósticos en su sistema StorageGRID y revisar los resultados.

- ["Revisar las métricas de soporte"](#)
- ["Métricas de Prometheus de uso común"](#)

Antes de empezar

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

Acerca de esta tarea

La página Diagnóstico realiza un conjunto de comprobaciones de diagnóstico sobre el estado actual de la red. Cada comprobación de diagnóstico puede tener uno de 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 red. Por ejemplo, una verificación de diagnóstico podría mostrar el estado de Precaución incluso si no se ha activado ninguna alerta.

Pasos

1. Seleccione **SOPORTE > Herramientas > Diagnóstico**.

Aparece la página Diagnóstico y enumera los resultados de cada verificación de diagnóstico. Los resultados se ordenan por gravedad (Precaución, Atención y Normal). Dentro de cada gravedad, los resultados se ordenan alfabéticamente.

En este 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 automatic restarts
- ✓ Cassandra blocked task queue too large
- ✓ Cassandra commit log latency
- ✓ Cassandra commit log queue depth

2. Para obtener más información sobre un diagnóstico específico, haga clic en cualquier parte 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 de Prometheus:** si se utiliza para el diagnóstico, la expresión de Prometheus que se utilizó para generar los valores de estado. (No se utiliza una expresión de Prometeo para todos los

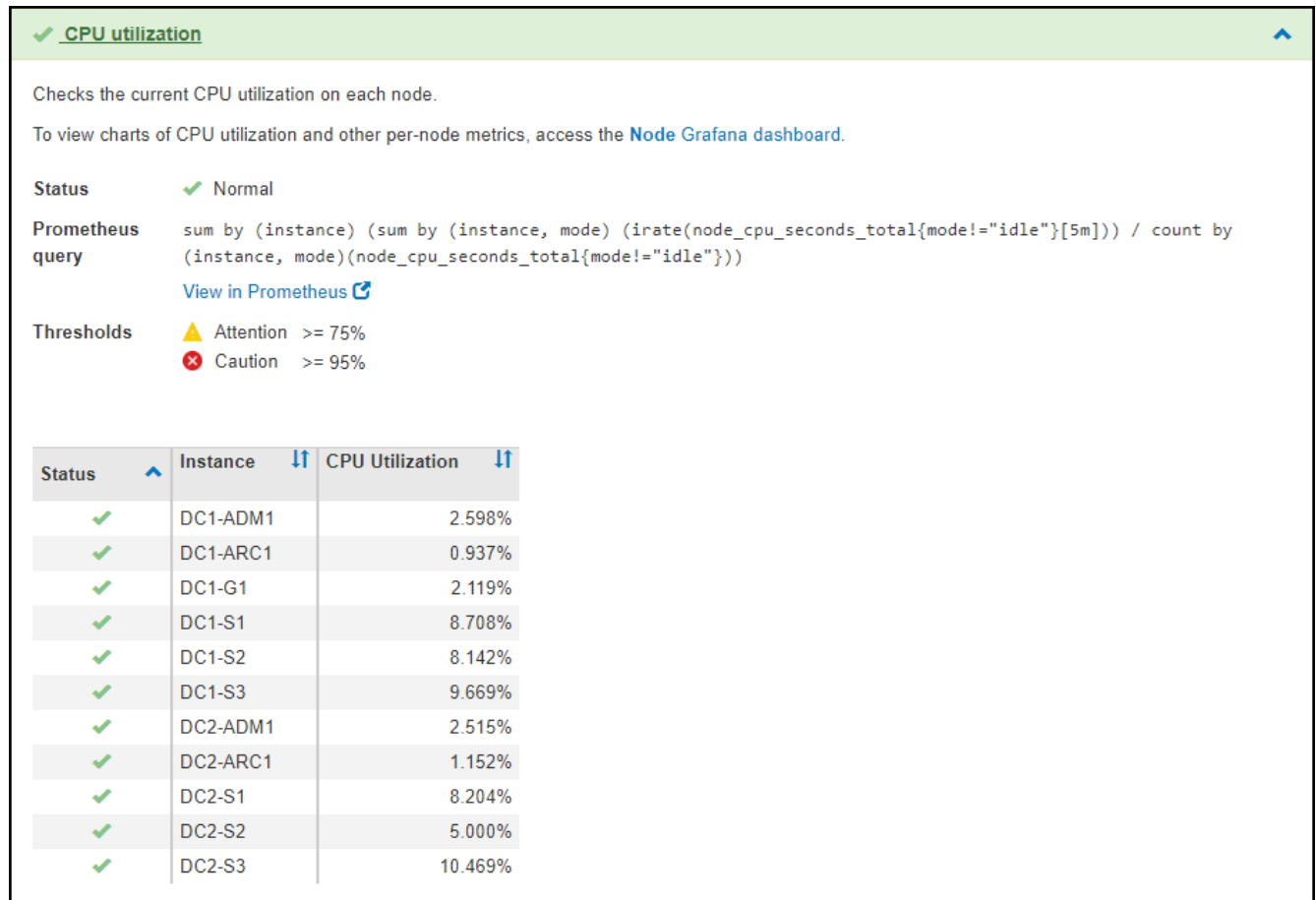
diagnósticos).

- **Umbrales:** Si están disponibles para el diagnóstico, los umbrales definidos por el sistema para cada estado de diagnóstico anormal. (Los valores de umbral no se utilizan para todos los diagnósticos).



No puedes cambiar estos umbrales.

- **Valores de estado:** una tabla que muestra el estado y el valor del diagnóstico en todo el sistema StorageGRID . En este ejemplo, se muestra la utilización actual de la CPU para cada nodo en un sistema StorageGRID . Todos los valores de los nodos están por debajo de los umbrales de Atención y Precaución, por lo que el estado general del diagnóstico es Normal.



3. **Opcional:** Para ver los gráficos de Grafana relacionados con este diagnóstico, haga clic en el enlace **Panel de Grafana**.

Este enlace no se muestra para todos los diagnósticos.

Aparece el panel de Grafana relacionado. En este ejemplo, el panel de nodo aparece mostrando la utilización de la CPU a lo largo del tiempo para este nodo, así como otros gráficos de Grafana para el nodo.



También puede acceder a los paneles de Grafana prediseñados desde la sección Grafana de la página **SOPORTE > Herramientas > Métricas**.



4. **Opcional:** Para ver un gráfico de la expresión de Prometheus a lo largo del tiempo, haga clic en **Ver en Prometheus**.

Aparece un gráfico de Prometeo de la expresión utilizada en el diagnóstico.

☐ Enable query history

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

Load time: 547ms
Resolution: 14s
Total time series: 13

Execute

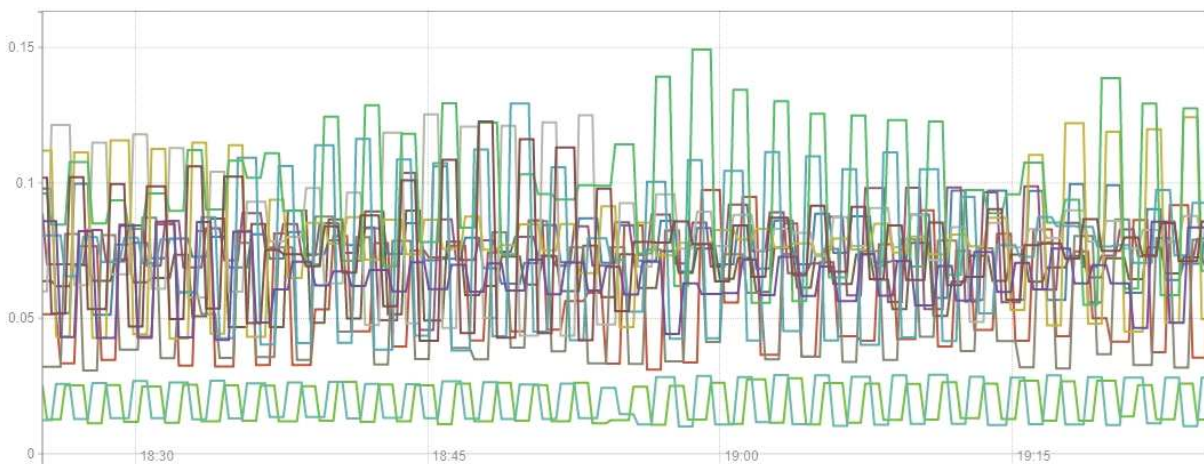
- insert metric at cursor - ▾

Graph Console

- 1h +

◀ Until ▶

Res. (s)

☐ stacked

- ✓ {instance="DC3-S3"}
- ✓ {instance="DC3-S2"}
- ✓ {instance="DC3-S1"}
- ✓ {instance="DC2-S3"}
- ✓ {instance="DC2-S2"}
- ✓ {instance="DC2-S1"}
- ✓ {instance="DC2-ADM1"}
- ✓ {instance="DC1-S3"}
- ✓ {instance="DC1-S2"}
- ✓ {instance="DC1-S1"}
- ✓ {instance="DC1-G1"}
- ✓ {instance="DC1-ARC1"}
- ✓ {instance="DC1-ADM1"}

Remove Graph

Add Graph

Cree aplicaciones de monitorización personalizadas

Puede crear aplicaciones y paneles de monitoreo personalizados utilizando las métricas StorageGRID disponibles en la API de administración 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 usar la API de administración de Grid para consultar las métricas de StorageGRID .

También puede acceder a las métricas de Prometheus directamente con una herramienta de monitoreo externa, como Grafana. Para usar una herramienta externa es necesario cargar o generar un certificado de cliente administrativo para permitir que StorageGRID autentique la herramienta por motivos de seguridad. Ver el ["Instrucciones para administrar StorageGRID"](#) .

Para ver las operaciones de la API de métricas, incluida la lista completa de las métricas disponibles, vaya al Administrador de cuadrícula. Desde la parte superior de la página, seleccione el ícono de ayuda y seleccione **Documentación de API > métricas**

GET

`/grid/metric-labels/{label}/values` Lists the values for a metric label

GET

`/grid/metric-names` Lists all available metric names

GET

`/grid/metric-query` Performs an instant metric query at a single point in time

GET

`/grid/metric-query-range` Performs a metric query over a range of time

Los detalles de cómo implementar una aplicación de monitoreo personalizada están más allá del alcance de esta documentación.

Solucionar problemas del sistema StorageGRID

Solucionar problemas de un sistema StorageGRID

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

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

Define el problema

El primer paso para resolver un problema es definirlo claramente.

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

Pregunta	Ejemplo de respuesta
¿Qué está haciendo o no haciendo el sistema StorageGRID ? ¿Cuales son sus síntomas?	Las aplicaciones cliente informan que los objetos no se pueden ingerir en StorageGRID.
¿Cuándo empezó el problema?	La ingesta de objetos se denegó por primera vez aproximadamente a las 14:50 del 8 de enero de 2020.
¿Cómo notó el problema por primera vez?	Notificado por la aplicación del cliente. También recibí notificaciones de alerta por correo electrónico.
¿El problema ocurre constantemente o sólo a veces?	El problema continúa.
Si el problema ocurre regularmente, ¿qué pasos se deben seguir para provocarlo?	El problema ocurre cada vez que un cliente intenta ingerir un objeto.

Pregunta	Ejemplo de respuesta
Si el problema ocurre de forma intermitente, ¿cuándo ocurre? Registre las horas de cada incidente del que tenga conocimiento.	El problema no es intermitente.
¿Has visto este problema antes? ¿Con qué frecuencia has tenido este problema en el pasado?	Esta es la primera vez que veo este problema.

Evaluar el riesgo y el impacto en el sistema

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

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

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

Recopilar datos

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

Tipo de datos a recopilar	¿Por qué recopilar estos datos?	Instrucciones
Crear una línea de tiempo de cambios recientes	Los cambios en su sistema StorageGRID , su configuración o su entorno pueden provocar un nuevo comportamiento.	• Crear una línea de tiempo de cambios recientes

Tipo de datos a recopilar	¿Por qué recopilar estos datos?	Instrucciones
Alertas de revisión	Las alertas pueden ayudarle a determinar rápidamente la causa raíz de un problema al proporcionar pistas importantes sobre los problemas subyacentes que podrían estar causándolo. Revise la lista de alertas actuales para ver si StorageGRID ha identificado la causa raíz de un problema para usted. Revise las alertas activadas en el pasado para obtener información adicional.	• "Ver alertas actuales y resueltas"
Monitorear eventos	Los eventos incluyen cualquier error del sistema o eventos de falla de un nodo, incluidos errores como errores de red. Supervise eventos para obtener más información sobre los problemas o para ayudar con la resolución de problemas.	• "Monitorear eventos"
Identificar tendencias utilizando gráficos e informes de texto	Las tendencias pueden proporcionar pistas valiosas sobre cuándo aparecieron los primeros problemas y pueden ayudarle a comprender con qué rapidez están cambiando las cosas.	• "Utilice tablas y gráficos" • "Utilice informes de texto"
Establecer líneas de base	Recopilar información sobre los niveles normales de varios valores operativos. Estos valores de referencia y las desviaciones con respecto a ellos pueden proporcionar pistas valiosas.	• Establecer líneas de base
Realizar pruebas de ingesta y recuperación	Para solucionar problemas de rendimiento con la ingesta y la recuperación, utilice una estación de trabajo para almacenar y recuperar objetos. Compare los resultados con los que se ven al utilizar la aplicación cliente.	• "Supervisar el rendimiento de PUT y GET"
Revisar los mensajes de auditoría	Revise los mensajes de auditoría para seguir las operaciones de StorageGRID en detalle. Los detalles en los mensajes de auditoría pueden ser útiles para solucionar muchos tipos de problemas, incluidos problemas de rendimiento.	• "Revisar los mensajes de auditoría"

Tipo de datos a recopilar	¿Por qué recopilar estos datos?	Instrucciones
Verificar la ubicación de los objetos y la integridad del almacenamiento	Si tiene problemas de almacenamiento, verifique que los objetos se coloquen donde espera. Verifique la integridad de los datos de los objetos en un nodo de almacenamiento.	• "Supervisar las operaciones de verificación de objetos" • "Confirmar la ubicación de los datos de los objetos" • "Verificar la integridad del objeto"
Recopilar datos para soporte técnico	Es posible que el soporte técnico le solicite que recopile datos o revise información específica para ayudar a solucionar problemas.	• "Recopilar archivos de registro y datos del sistema" • "Activar manualmente un paquete de AutoSupport" • "Revisar las métricas de soporte"

Crea una línea de tiempo de cambios recientes

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

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

Cree una tabla de cambios recientes en su sistema que incluya información sobre cuándo ocurrió cada cambio y cualquier detalle relevante sobre el cambio, como información sobre qué más estaba sucediendo mientras el cambio estaba en progreso:

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

Ejemplos de cambios recientes significativos

A continuación se presentan algunos ejemplos de cambios potencialmente significativos:

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

Establecer líneas de base

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

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

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

Analizar datos

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

El análisis depende del problema, pero en general:

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

Lista de verificación de información de escalada

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

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

	Artículo	Notas
	Información de referencia	Recopilar información de referencia sobre las operaciones de ingesta, las operaciones de recuperación y el consumo de almacenamiento. Establecer líneas de base
	Cronología de cambios recientes	Cree una línea de tiempo que resuma todos los cambios recientes en el sistema o su entorno. Crear una línea de tiempo de cambios recientes
	Historia de los esfuerzos para diagnosticar el problema	Si ha tomado medidas para diagnosticar o solucionar el problema usted mismo, asegúrese de registrar los pasos que siguió y el resultado.

Solucionar problemas de objetos y almacenamiento

Confirmar la ubicación de los datos de los objetos

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

Antes de empezar

- Debe tener un identificador de objeto, que puede ser uno de los siguientes:
 - **UUID**: Identificador único universal del objeto. Introduzca el UUID en mayúsculas.
 - **CBID**: El identificador único del objeto dentro de StorageGRID . Puede obtener el CBID de un objeto desde el registro de auditoría. Introduzca el CBD en mayúsculas.
 - **Clave de objeto y depósito S3**: cuando se ingiere un objeto a través de ["Interfaz S3"](#) La aplicación cliente utiliza una combinación de clave de objeto y depósito para almacenar e identificar el objeto.

Pasos

1. Seleccione **ILM > Búsqueda de metadatos de objetos**.
2. Escriba el identificador del objeto en el campo **Identificador**.

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

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

Object Metadata Lookup

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

Identifier

Version ID (optional)

4. Seleccione **Buscar**.

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

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

El siguiente ejemplo muestra los resultados de la búsqueda de metadatos de un objeto de prueba S3 que se almacena como dos copias replicadas.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAIIS": "2",

```

Fallos en el almacén de objetos (volumen de almacenamiento)

El almacenamiento subyacente en un nodo de almacenamiento se divide en almacenes de objetos. Los almacenes de objetos también se conocen como volúmenes de almacenamiento.

Puede ver información del almacén de objetos para cada nodo de almacenamiento. Los almacenes de objetos se muestran en la parte inferior de la página **NODES > Storage Node > Storage**.

Disk devices

Name ? ⇅	World Wide Name ? ⇅	I/O load ? ⇅	Read rate ? ⇅	Write rate ? ⇅
sdC(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

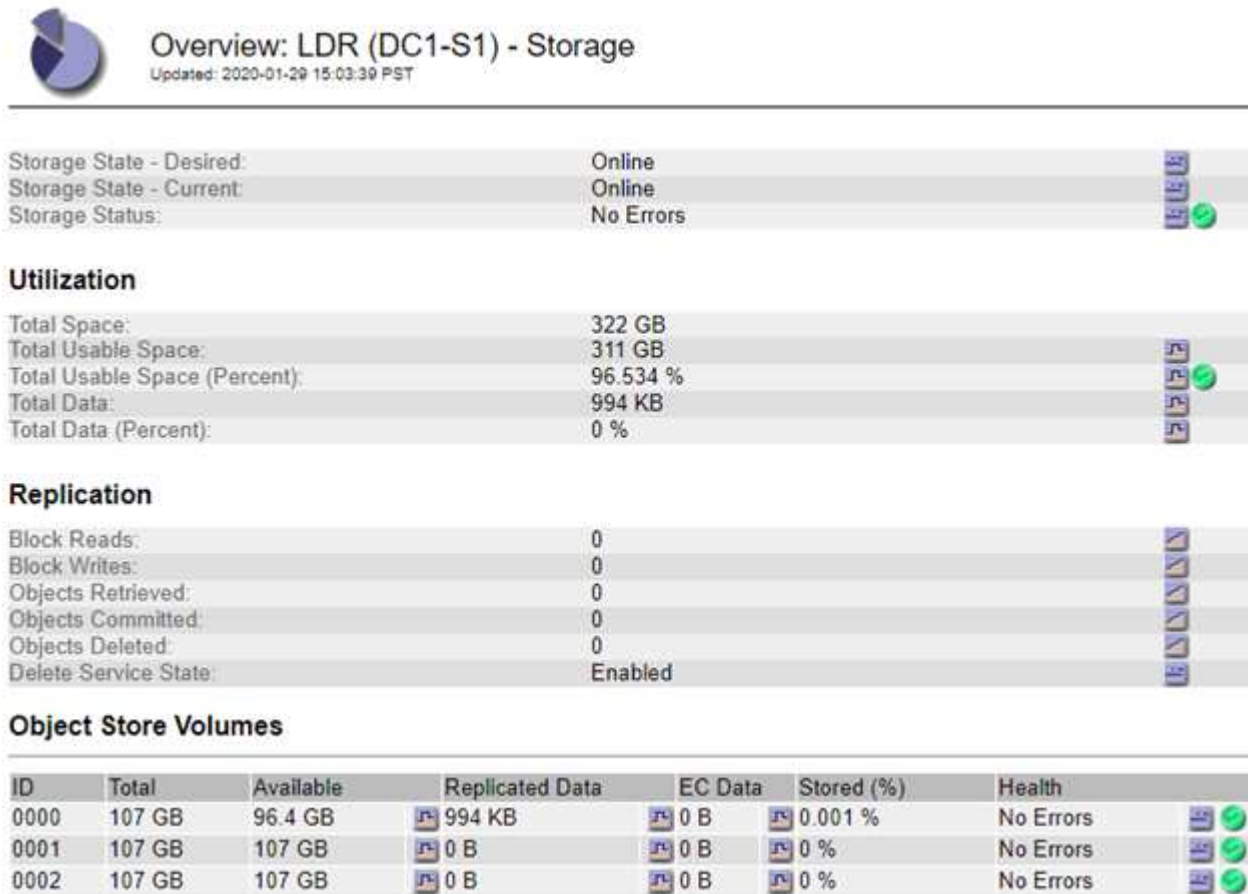
Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2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

Object stores

ID ? ⇅	Size ? ⇅	Available ? ⇅	Replicated data ? ⇅	EC data ? ⇅	Object data (%) ? ⇅	Health ? ⇅
0000	107.32 GB	96.44 GB 	1.55 MB 	0 bytes 	0.00%	No Errors
0001	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0002	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0003	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0004	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors

Para ver más ["detalles sobre cada nodo de almacenamiento"](#) , siga estos pasos:

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



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

Verificar la integridad del objeto

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

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

¿Qué es la verificación de antecedentes?

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

La verificación de antecedentes verifica la integridad de los objetos replicados y los objetos codificados por borrado, de la siguiente manera:

- **Objetos replicados:** si el proceso de verificación en segundo plano encuentra un objeto replicado que está dañado, la copia dañada se elimina de su ubicación y se pone en cuarentena en otro lugar del nodo de almacenamiento. Luego, se genera una nueva copia no dañada y se coloca para satisfacer las políticas ILM activas. Es posible que la nueva copia no se coloque en el nodo de almacenamiento que se utilizó para la copia original.



Los datos de objetos dañados se ponen en cuarentena en lugar de eliminarse del sistema, de modo que aún se pueda acceder a ellos. Para obtener más información sobre cómo acceder a los datos de objetos en cuarentena, comuníquese con el soporte técnico.

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

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

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

Alertas relacionadas con la verificación de antecedentes

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

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

Cambiar la tasa de verificación de antecedentes

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

Antes de empezar

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

Acerca de esta tarea

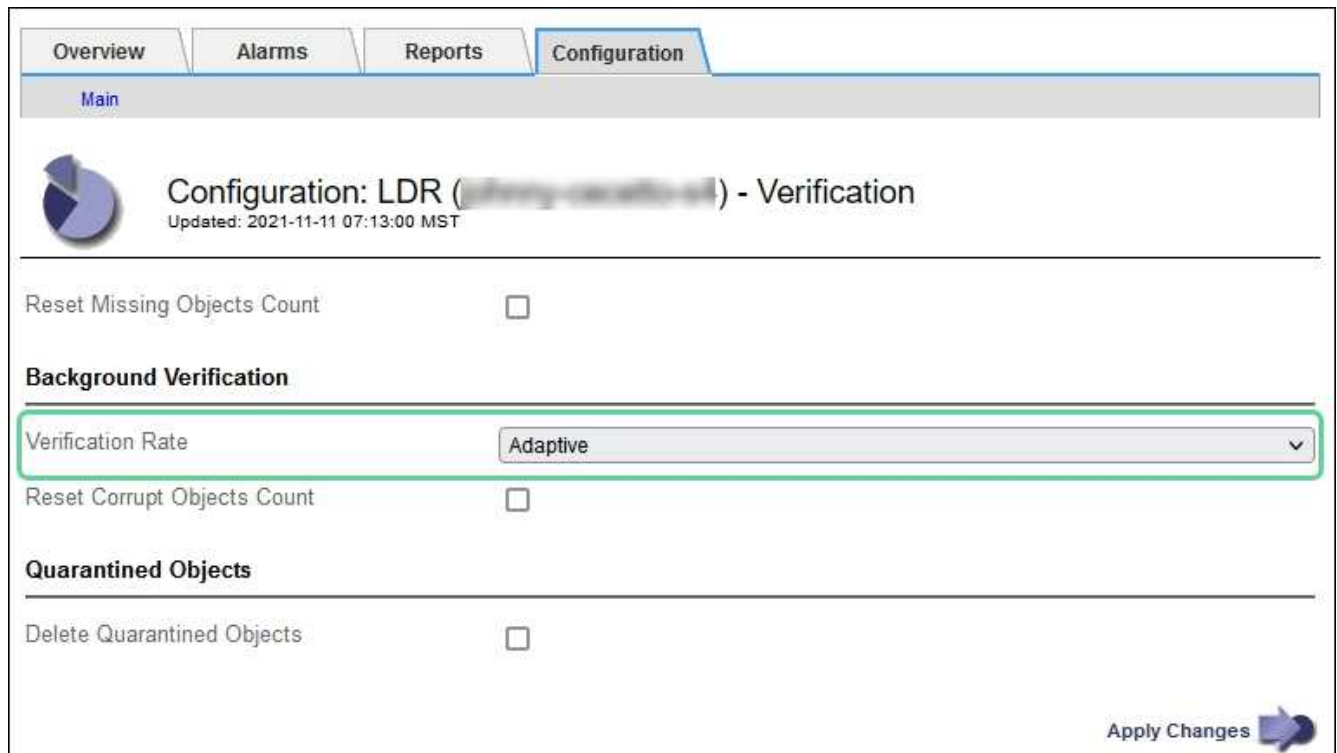
Puede cambiar la tasa de verificación para la verificación de antecedentes en un nodo de almacenamiento:

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

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

Pasos

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



Overview Alarms Reports Configuration

Main

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

Reset Missing Objects Count ☐

Background Verification

Verification Rate

Reset Corrupt Objects Count ☐

Quarantined Objects

Delete Quarantined Objects ☐

Apply Changes

6. Haga clic en **Aplicar cambios**.
7. Supervisar los resultados de la verificación en segundo plano de los objetos replicados.
 - a. Vaya a **NODOS > Nodo de almacenamiento > Objetos**.
 - b. En la sección Verificación, supervise los valores de **Objetos corruptos** y **Objetos corruptos no identificados**.

Si la verificación en segundo plano encuentra datos de objetos replicados corruptos, se incrementa la métrica **Objetos corruptos** y StorageGRID intenta extraer el identificador del objeto de los datos, de la siguiente manera:

- Si se puede extraer el identificador del objeto, StorageGRID crea automáticamente una nueva copia de los datos del objeto. La nueva copia se puede realizar en cualquier lugar del sistema StorageGRID que satisfaga las políticas ILM activas.
- Si no se puede extraer el identificador del objeto (porque está dañado), se incrementa la métrica **Objetos dañados no identificados** y se activa la alerta **Objeto dañado no identificado detectado**.

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

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

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

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

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

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

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

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

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

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

d. Haga clic en **Aplicar cambios**.

10. Si está seguro de que los objetos en cuarentena no son necesarios, puede eliminarlos.



Si se activó la alerta **Objetos perdidos**, es posible que el soporte técnico desee acceder a los objetos en cuarentena para ayudar a depurar el problema subyacente o intentar recuperar datos.

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

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

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

d. Seleccione **Aplicar cambios**.

¿Qué es la comprobación de existencia de objetos?

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

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

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

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

Ejecutar comprobación de existencia de objeto

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

Antes de empezar

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

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

Acerca de esta tarea

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

Pasos

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

Puede buscar por nombre de nodo o sitio.

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

4. Seleccione **Continuar**.

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

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

6. Seleccione **Continuar**.

7. Seleccione la consistencia para el trabajo.

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

- **Sitio fuerte:** Dos copias de metadatos en un solo sitio.
- **Fuerte-global:** Dos copias de metadatos en cada sitio.
- **Todos** (predeterminado): las tres copias de metadatos en cada sitio.

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

8. Seleccione **Continuar**.

9. Revise y verifique sus selecciones. Puede seleccionar **Anterior** para ir a un paso anterior en el asistente para actualizar sus selecciones.

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

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



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

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

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

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

Object existence check

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

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

Active job

Job history

Status: Accepted

Consistency control: All

Job ID: 2334602652907829302

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

Missing object copies detected: 0

Elapsed time: —

Progress: 0%

Estimated time to completion: —

Pause

Cancel

Volumes

Details

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

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

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

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

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

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

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

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

Object existence check

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

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

Active job | Job history

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

Displaying 4 results

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

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

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

Después de terminar

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

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

La alerta de tamaño de objeto PUT de S3 demasiado grande se activa si un inquilino

intenta una operación PutObject que no sea multiparte y que exceda el límite de tamaño de S3 de 5 GiB.

Antes de empezar

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

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

Pasos

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

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

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

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

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

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

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

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

- f. Identifique qué inquilinos utilizan objetos de más de 5 GiB.
 - i. Ingresar `zgrep SPUT * | egrep "CSIZ\ (UI64\): ([5-9] | [1-9] [0-9]+) [0-9] {9}"`
 - ii. Para cada mensaje de auditoría en los resultados, consulte `S3AI` campo para determinar el ID de la cuenta del inquilino. Utilice los demás campos del mensaje para determinar qué dirección IP utilizaron el cliente, el depósito y el objeto:

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

Ejemplo de resultados del registro de auditoría

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

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

- Vaya a **SOPORTE > Herramientas > Registros**. Recopilar registros de aplicaciones para el nodo de almacenamiento en la alerta. Especifique 15 minutos antes y después de la alerta.
- Extrae el archivo y ve a `bycast.log`:

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

- Buscar en el registro `method=PUT` e identificar al cliente en el `clientIP` campo.

Ejemplo bycast.log

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

4. Informe a los inquilinos que el tamaño máximo de `PutObject` es de 5 GiB y que deben utilizar cargas

multiparte para objetos mayores a 5 GiB.

5. Ignore la alerta durante una semana si se ha modificado la aplicación.

Solucionar problemas de datos de objetos perdidos o faltantes

Solucionar problemas de datos de objetos perdidos o faltantes

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

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

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

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

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

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

Investigar objetos perdidos

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

Antes de empezar

- Debe iniciar sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tienes "[permisos de acceso específicos](#)".
- Debes tener el `Passwords.txt` archivo.

Acerca de esta tarea

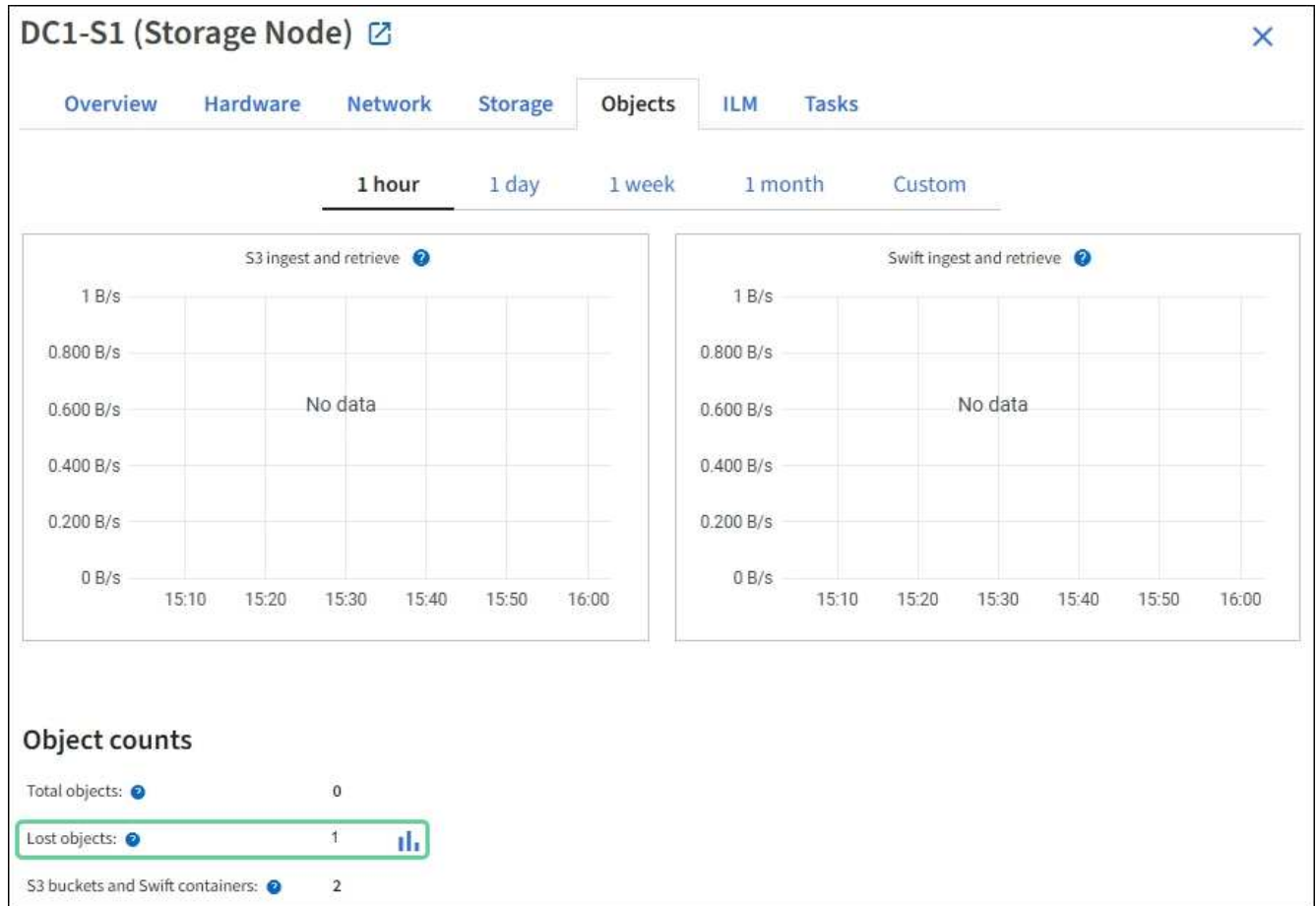
La alerta **Objetos perdidos** indica que StorageGRID cree que no hay copias de un objeto en la red. Es posible que se hayan perdido datos de forma permanente.

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

Pasos

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

Este número indica la cantidad total de objetos que este nodo de la cuadrícula detecta como faltantes en todo el sistema StorageGRID . El valor es la suma de los contadores de objetos perdidos del componente Almacén de datos dentro de los servicios LDR y DDS.



4. Desde un nodo de administración, "[acceder al registro de auditoría](#)" para determinar el identificador único (UUID) del objeto que activó la alerta **Objetos perdidos**:
 - a. Inicie sesión en el nodo de la red:
 - i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - iii. Introduzca el siguiente comando para cambiar a root: `su -`
 - iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo. Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.
 - b. Cambie al directorio donde se encuentran los registros de auditoría.

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

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

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

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

- Utilice `grep` para extraer los mensajes de auditoría de Objeto Perdido (OLST). Ingrese: `grep OLST audit_file_name`
- Tenga en cuenta el valor UUID incluido en el mensaje.

```
Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

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

Metadatos	Conclusión
Objeto <object_identifier> no encontrado	Si no se encuentra el objeto, se devuelve el mensaje "ERROR": "". Si no se encuentra el objeto, puede restablecer el recuento de Objetos perdidos para borrar la alerta. La falta de un objeto indica que el objeto fue eliminado intencionalmente.

Metadatos	Conclusión
Ubicaciones > 0	Si hay ubicaciones enumeradas en la salida, la alerta Objetos perdidos podría ser un falso positivo. Confirmar que los objetos existen. Utilice el ID de nodo y la ruta de archivo que aparecen en la salida para confirmar que el archivo de objeto se encuentra en la ubicación indicada. (El procedimiento para "buscando objetos potencialmente perdidos" (Explica cómo utilizar el ID de nodo para encontrar el nodo de almacenamiento correcto). Si los objetos existen, puede restablecer el recuento de Objetos perdidos para borrar la alerta.
Ubicaciones = 0	Si no hay ubicaciones enumeradas en la salida, es posible que el objeto no esté presente. Puedes intentarlo "buscar y restaurar el objeto" usted mismo o puede ponerse en contacto con el soporte técnico. Es posible que el soporte técnico le pida que determine si hay un procedimiento de recuperación de almacenamiento en curso. Ver la información sobre "Restaurar datos de objetos mediante Grid Manager" y "restaurar datos de objetos a un volumen de almacenamiento".

Buscar y restaurar objetos potencialmente perdidos

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

Antes de empezar

- Tienes el UUID de cualquier objeto perdido, tal como se identifica en "[Investigar objetos perdidos](#)".
- Tú tienes el `Passwords.txt` archivo.

Acerca de esta tarea

Puede seguir este procedimiento para buscar copias replicadas del objeto perdido en otra parte de la cuadrícula. En la mayoría de los casos, el objeto perdido no se encontrará. Sin embargo, en algunos casos, es posible que puedas encontrar y restaurar un objeto replicado perdido si tomas medidas rápidamente.



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

Pasos

1. Desde un nodo de administración, busque en los registros de auditoría posibles ubicaciones de objetos:
 - a. Inicie sesión en el nodo de la red:
 - i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`

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

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

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

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

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

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

Por ejemplo:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log > /var/local/tmp/messages_about_lost_object.txt
```

- d. Utilice `grep` para extraer los mensajes de auditoría de ubicación perdida (LLST) de este archivo de salida. Ingresar: `grep LLST output_file_name`

Por ejemplo:

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

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

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

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

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

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

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

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

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

a. Inicie sesión en el nodo de la red:

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

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

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

Para la ruta del archivo del objeto, utilice el valor de PCLD del mensaje de auditoría LLST.

Por ejemplo, introduzca:

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



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

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

objeto encontrado en StorageGRID.

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

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

Por ejemplo, introduzca:

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

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



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

- Si no se puede restaurar el objeto, el `Object_Found` El comando falla. Póngase en contacto con el soporte técnico.
- Si el objeto se restauró exitosamente en StorageGRID, aparecerá un mensaje de éxito. Por ejemplo:

```
ade 12448208: /proc/STOR > Object_Found
'/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

ade 12448208: /proc/STOR > Object found succeeded.
First packet of file was valid. Extracted key: 38186FE53E3C49A5
Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
'/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
```

Continúe con el siguiente paso.

4. Si el objeto se restauró exitosamente en StorageGRID, verifique que se hayan creado las nuevas ubicaciones:

- a. Sign in en Grid Manager usando un [navegador web compatible](#).
- b. Seleccione **ILM > Búsqueda de metadatos de objetos**.
- c. Ingrese el UUID y seleccione **Buscar**.
- d. Revise los metadatos y verifique las nuevas ubicaciones.

5. Desde un nodo de administración, busque en los registros de auditoría el mensaje de auditoría ORLM de este objeto para confirmar que la gestión del ciclo de vida de la información (ILM) ha colocado copias

según sea necesario.

- a. Inicie sesión en el nodo de la red:
 - i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - iii. Introduzca el siguiente comando para cambiar a root: `su -`
 - iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo. Cuando inicia sesión como root, el mensaje cambia de \$ a #.
- b. Cambie al directorio donde se encuentran los registros de auditoría. Referirse a [subpaso 1.b](#).
- c. Utilice grep para extraer los mensajes de auditoría asociados con el objeto a un archivo de salida. Ingresar: `grep uuid-value audit_file_name > output_file_name`

Por ejemplo:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_restored_object.txt
```

- d. Utilice grep para extraer los mensajes de auditoría de reglas de objeto cumplidas (ORLM) de este archivo de salida. Ingresar: `grep ORLM output_file_name`

Por ejemplo:

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

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

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

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

Si está presente, el valor de CLDI en LOCS es el ID del nodo y el ID del volumen donde se ha creado una copia del objeto. Este mensaje muestra que se ha aplicado el ILM y que se han creado dos copias de objetos en dos ubicaciones de la cuadrícula.

6. ["Restablecer los recuentos de objetos perdidos y faltantes"](#) en el Administrador de cuadrícula.

Restablecer el recuento de objetos perdidos y faltantes

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

Antes de empezar

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

Acerca de esta tarea

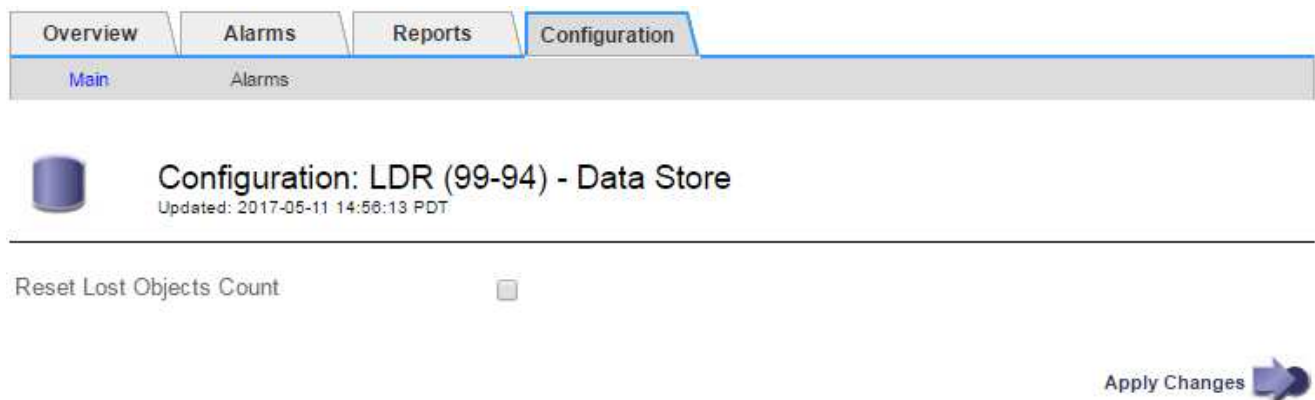
Puede restablecer el contador de objetos perdidos desde cualquiera de las siguientes páginas:

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

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

Pasos

1. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
2. Seleccione **Sitio > Nodo de almacenamiento > LDR > Almacén de datos > Configuración** para el nodo de almacenamiento que tiene la alerta **Objetos perdidos** o la alarma LOST.
3. Seleccione **Restablecer recuento de objetos perdidos**.



4. Haga clic en **Aplicar cambios**.

El atributo Objetos perdidos se restablece a 0 y la alerta **Objetos perdidos** y la alarma PERDIDO se borran, lo que puede tardar unos minutos.

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

- d. Seleccione **Sitio > Nodo de almacenamiento > LDR > Verificación > Configuración**.
- e. Seleccione **Restablecer recuento de objetos faltantes y Restablecer recuento de objetos corruptos**.
- f. Si está seguro de que los objetos en cuarentena no son necesarios, puede seleccionar **Eliminar objetos en cuarentena**.

Los objetos en cuarentena se crean cuando la verificación en segundo plano identifica una copia de objeto replicada dañada. En la mayoría de los casos, StorageGRID reemplaza automáticamente el objeto dañado y es seguro eliminar los objetos en cuarentena. Sin embargo, si se activa la alerta **Objetos perdidos** o la alarma LOST, es posible que el soporte técnico desee acceder a los objetos en cuarentena.

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

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

Solucionar la alerta de almacenamiento de datos de objetos bajos

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

Antes de empezar

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

Acerca de esta tarea

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

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

```
(storagegrid_storage_utilization_data_bytes/  
(storagegrid_storage_utilization_data_bytes +  
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

En esta condición:

- ``storagegrid_storage_utilization_data_bytes`` es una estimación del tamaño total de datos de objetos replicados y codificados por borrado para un nodo de almacenamiento.
- ``storagegrid_storage_utilization_usable_space_bytes`` es la cantidad total de espacio de almacenamiento de objetos restante para un nodo de almacenamiento.

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

Pasos

1. Seleccione **ALERTAS > Actual**.

Aparece la página de Alertas.

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

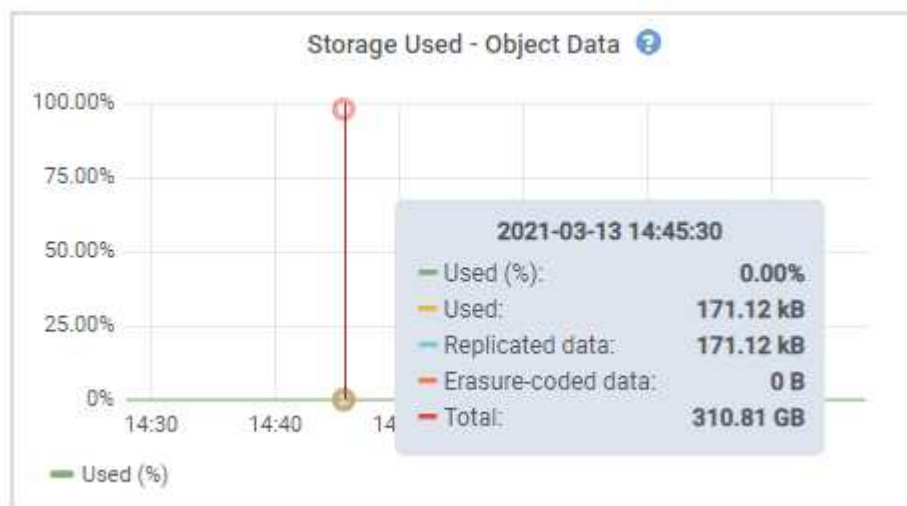


Seleccione la alerta, no el encabezado, para un grupo de alertas.

- Revise los detalles en el cuadro de diálogo y tenga en cuenta lo siguiente:
 - Tiempo activado
 - El nombre del sitio y del nodo
 - Los valores actuales de las métricas para esta alerta
- Seleccione **NODOS > Nodo de almacenamiento o Sitio > Almacenamiento**.
- Coloque el cursor sobre el gráfico Almacenamiento utilizado - Datos de objeto.

Se muestran los siguientes valores:

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



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

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

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

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



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

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

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

En versiones anteriores, los tres ["marcas de agua de volumen de almacenamiento"](#) eran configuraciones globales: los mismos valores aplicados a cada volumen de almacenamiento en cada nodo de almacenamiento. A partir de StorageGRID 11.6, el software puede optimizar estas marcas de agua para cada volumen de almacenamiento, según el tamaño del nodo de almacenamiento y la capacidad relativa del volumen.

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

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

Entender la alerta

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

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

Por ejemplo, supongamos que anteriormente configuró la marca de agua de solo lectura del volumen de almacenamiento en 5 GB. Ahora supongamos que StorageGRID ha calculado los siguientes valores optimizados para los cuatro volúmenes de almacenamiento en el Nodo de almacenamiento A:

Volumen 0	12 GB
Volumen 1	12 GB
Volumen 2	11 GB

Volumen 3	15 GB

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

Resolver la alerta

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

Antes de empezar

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

Acerca de esta tarea

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

Evaluar el uso de datos de objetos para toda la red

Pasos

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

Nodes

View the list and status of sites and grid nodes.

Search... Total node count: 13

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

4. Siga el paso apropiado:

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

Ver marcas de agua de almacenamiento optimizadas

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

Pasos

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

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

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

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

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

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

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

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

Determinar si se pueden usar marcas de agua optimizadas

Pasos

1. Seleccione **NODOS**.
2. Repita estos pasos para cada nodo de almacenamiento en línea:
 - a. Seleccione **Nodo de almacenamiento > Almacenamiento**.
 - b. Desplácese hacia abajo hasta la tabla Almacenes de objetos.
 - c. Compare el valor **Disponible** para cada almacén de objetos (volumen) con la marca de agua optimizada máxima que anotó para ese nodo de almacenamiento.
3. Si al menos un volumen en cada nodo de almacenamiento en línea tiene más espacio disponible que la marca de agua máxima optimizada para ese nodo, vaya a [Utilice marcas de agua optimizadas](#) para comenzar a utilizar las marcas de agua optimizadas.

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

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



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

Usar marcas de agua optimizadas

Pasos

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

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

volumen.

Solucionar problemas de metadatos

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

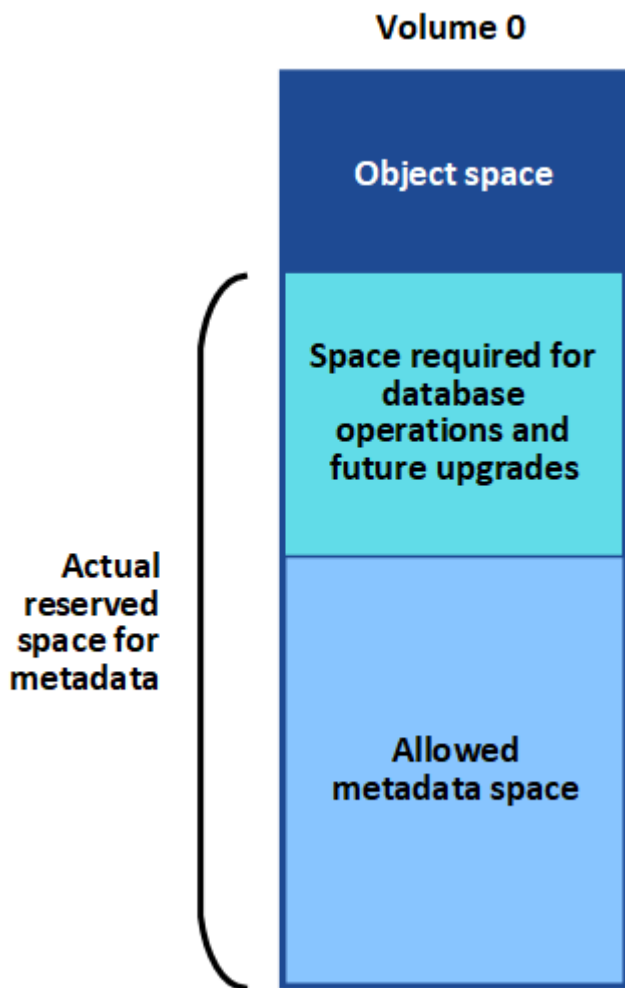
Antes de empezar

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

Acerca de esta tarea

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

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



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

Puede "[Supervisar la capacidad de metadatos de objetos para cada nodo de almacenamiento](#)" para ayudarle a anticipar errores y corregirlos antes de que ocurran.

StorageGRID utiliza la siguiente métrica de Prometheus para medir qué tan lleno está el espacio de metadatos permitido:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

Cuando esta expresión de Prometheus alcanza ciertos umbrales, se activa la alerta **Almacenamiento de metadatos bajo**.

- **Menor:** Los metadatos del objeto utilizan el 70 % o más del espacio de metadatos permitido. Debe agregar nuevos nodos de almacenamiento lo antes posible.
- **Importante:** Los metadatos del objeto están utilizando el 90 % o más del espacio de metadatos permitido. Debe agregar nuevos nodos de almacenamiento inmediatamente.



Cuando los metadatos de un objeto utilizan el 90 % o más del espacio de metadatos permitido, aparece una advertencia en el panel. Si aparece esta advertencia, debe agregar nuevos nodos de almacenamiento inmediatamente. Nunca debe permitir que los metadatos de un objeto utilicen más del 100% del espacio permitido.

- **Crítico:** Los metadatos del objeto están utilizando el 100 % o más del espacio de metadatos permitido y están comenzando a consumir el espacio necesario para las operaciones esenciales de la base de datos. Debe detener la ingesta de nuevos objetos y debe agregar nuevos nodos de almacenamiento inmediatamente.



Si el tamaño del volumen 0 es menor que la opción de almacenamiento de Espacio reservado de metadatos (por ejemplo, en un entorno que no es de producción), el cálculo para la alerta **Almacenamiento de metadatos bajo** podría ser inexacto.

Pasos

1. Seleccione **ALERTAS > Actual**.
2. Desde la tabla de alertas, expanda el grupo de alerta **Almacenamiento de metadatos bajo**, si es necesario, y seleccione la alerta específica que desea ver.
3. Revise los detalles en el cuadro de diálogo de alerta.
4. Si se ha activado una alerta importante o crítica de **Almacenamiento de metadatos bajo**, realice una expansión para agregar nodos de almacenamiento inmediatamente.



Debido a que StorageGRID mantiene copias completas de todos los metadatos de los objetos en cada sitio, la capacidad de metadatos de toda la red está limitada por la capacidad de metadatos del sitio más pequeño. Si necesita agregar capacidad de metadatos a un sitio, también debe "[ampliar cualquier otro sitio](#)" por el mismo número de nodos de almacenamiento.

Después de realizar la expansión, StorageGRID redistribuye los metadatos de los objetos existentes a los nuevos nodos, lo que aumenta la capacidad general de metadatos de la red. No se requiere ninguna acción del usuario. Se borra la alerta **Almacenamiento de metadatos bajo**.

Solucionar errores de certificado

Si observa un problema de seguridad o de certificado cuando intenta conectarse a StorageGRID mediante un navegador web, un cliente S3 o una herramienta de monitoreo externa, debe verificar el certificado.

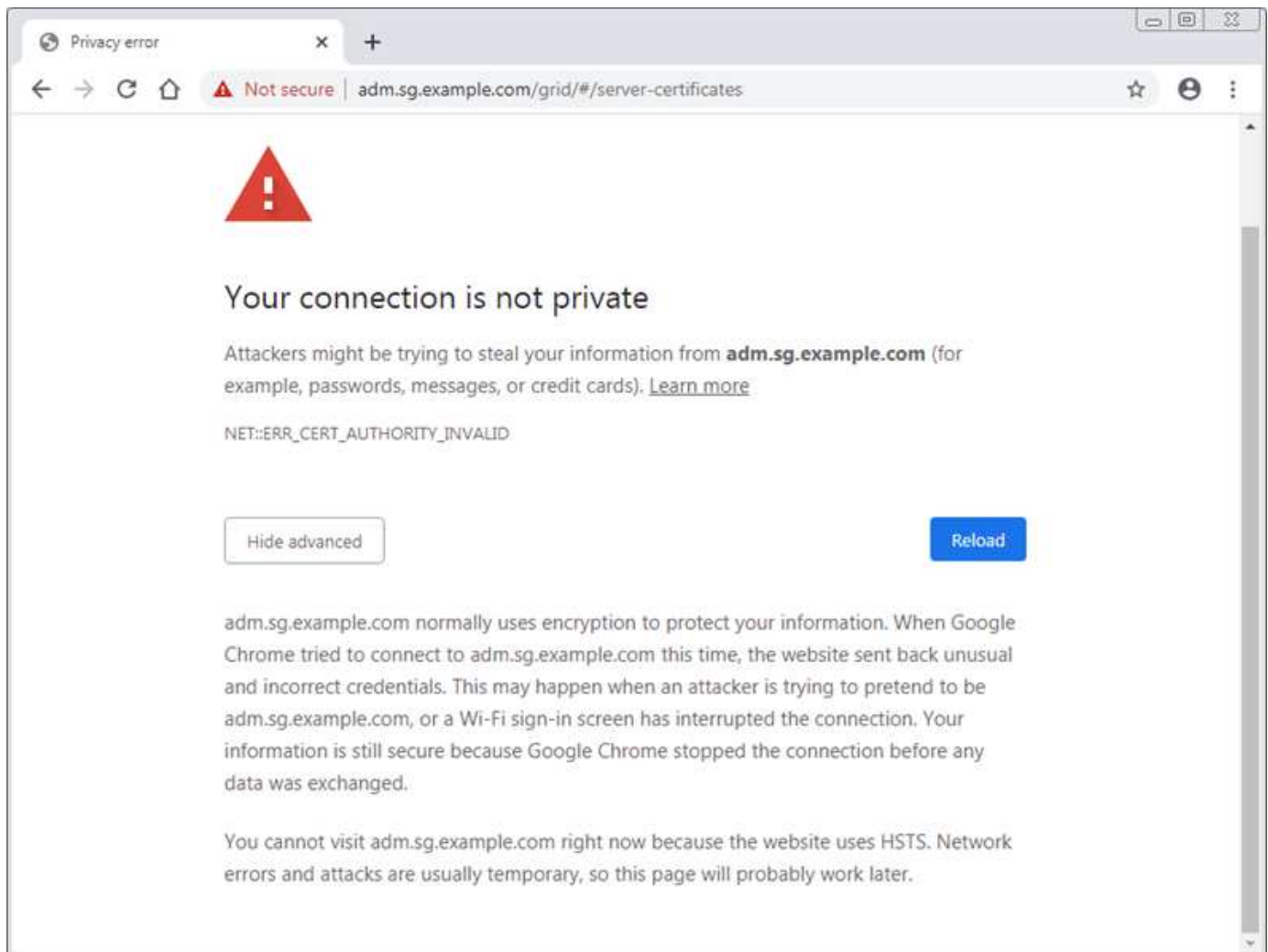
Acerca de esta tarea

Los errores de certificado pueden causar problemas cuando intenta conectarse a StorageGRID mediante Grid Manager, Grid Management API, Tenant Manager o Tenant Management API. También pueden ocurrir errores de certificado cuando intenta conectarse con un cliente S3 o una herramienta de monitoreo externa.

Si accede al Administrador de red o al Administrador de inquilinos mediante un nombre de dominio en lugar de una dirección IP, el navegador muestra un error de certificado sin una opción para omitirlo si ocurre alguna de las siguientes situaciones:

- Su certificado de interfaz de administración personalizada caduca.
- Vuelve de un certificado de interfaz de administración personalizado al certificado de servidor predeterminado.

El siguiente ejemplo muestra un error de certificado cuando el certificado de la interfaz de administración personalizada expiró:



Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor fallido, la alerta **Expiración del certificado de servidor para la interfaz de administración** se activa cuando el certificado del servidor está a punto de expirar.

Cuando utiliza certificados de cliente para la integración externa de Prometheus, los errores de certificado pueden ser causados por el certificado de la interfaz de administración de StorageGRID o por los certificados de cliente. La alerta **Expiración de certificados de cliente configurados en la página Certificados** se activa cuando un certificado de cliente está a punto de expirar.

Pasos

Si recibió una notificación de alerta sobre un certificado vencido, acceda a los detalles del certificado: . Seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego ["Seleccione la pestaña de certificado apropiada"](#) .

1. Verifique el período de validez del certificado. + Algunos navegadores web y clientes S3 no aceptan certificados con un período de validez superior a 398 días.
2. Si el certificado ha expirado o expirará pronto, cargue o genere un nuevo certificado.
 - Para obtener un certificado de servidor, consulte los pasos para ["Configuración de un certificado de servidor personalizado para Grid Manager y Tenant Manager"](#) .
 - Para obtener un certificado de cliente, consulte los pasos para ["configurar un certificado de cliente"](#) .
3. Para errores de certificado de servidor, pruebe una o ambas de las siguientes opciones:
 - Asegúrese de que el nombre alternativo del sujeto (SAN) del certificado esté completo y que el SAN coincida con la dirección IP o el nombre de host del nodo al que se está conectando.
 - Si está intentando conectarse a StorageGRID usando un nombre de dominio:
 - i. Ingrese la dirección IP del nodo de administración en lugar del nombre de dominio para evitar el error de conexión y acceder al administrador de red.
 - ii. Desde el Administrador de red, seleccione **CONFIGURACIÓN > Seguridad > Certificados** y luego ["Seleccione la pestaña de certificado apropiada"](#) para instalar un nuevo certificado personalizado o continuar con el certificado predeterminado.
 - iii. En las instrucciones para administrar StorageGRID, consulte los pasos para ["Configuración de un certificado de servidor personalizado para Grid Manager y Tenant Manager"](#) .

Solucionar problemas del nodo de administración y de la interfaz de usuario

Puede realizar varias tareas para ayudar a determinar el origen de los problemas relacionados con los nodos de administración y la interfaz de usuario de StorageGRID .

Errores de inicio de sesión en el nodo de administración

Si experimenta un error al iniciar sesión en un nodo de administración de StorageGRID , es posible que su sistema tenga un problema con un ["redes"](#) o ["hardware"](#) problema, un problema con ["Servicios del nodo de administración"](#) , o un ["Problema con la base de datos de Cassandra"](#) en nodos de almacenamiento conectados.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el `Passwords.txt` archivo.
- Tienes ["permisos de acceso específicos"](#) .

Acerca de esta tarea

Utilice estas pautas de solución de problemas si ve alguno de los siguientes mensajes de error al intentar iniciar sesión en un nodo de administración:

- Your credentials for this account were invalid. Please try again.
- Waiting for services to start...
- Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.
- Unable to communicate with server. Reloading page...

Pasos

1. Espere 10 minutos e intente iniciar sesión nuevamente.

Si el error no se resuelve automáticamente, vaya al siguiente paso.

2. Si su sistema StorageGRID tiene más de un nodo de administración, intente iniciar sesión en Grid Manager desde otro nodo de administración para verificar el estado de un nodo de administración no disponible.
 - Si puede iniciar sesión, puede utilizar las opciones **Panel de control**, **NODOS**, **Alertas** y **SOPORTE** para ayudar a determinar la causa del error.
 - Si solo tiene un nodo de administración o aún no puede iniciar sesión, vaya al siguiente paso.
3. Determinar si el hardware del nodo está fuera de línea.
4. Si el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID , consulte los pasos para ["configuración del inicio de sesión único"](#) .

Es posible que necesites deshabilitar y volver a habilitar temporalmente el SSO para un solo nodo de administración para resolver cualquier problema.



Si SSO está habilitado, no podrá iniciar sesión usando un puerto restringido. Debes utilizar el puerto 443.

5. Determinar si la cuenta que estás utilizando pertenece a un usuario federado.

Si la cuenta de usuario federada no funciona, intente iniciar sesión en Grid Manager como un usuario local, como root.

- Si el usuario local puede iniciar sesión:
 - i. Revisar alertas.
 - ii. Seleccione **CONFIGURACIÓN > Control de acceso > Federación de identidades**.
 - iii. Haga clic en **Probar conexión** para validar su configuración de conexión para el servidor LDAP.
 - iv. Si la prueba falla, resuelva cualquier error de configuración.
 - Si el usuario local no puede iniciar sesión y está seguro de que las credenciales son correctas, vaya al siguiente paso.
6. Utilice Secure Shell (ssh) para iniciar sesión en el nodo de administración:
 - a. Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`

- b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

7. Ver el estado de todos los servicios que se ejecutan en el nodo de la red: `storagegrid-status`

Asegúrese de que los servicios `nms`, `mi`, `nginx` y `mgmt api` estén todos en ejecución.

La salida se actualiza inmediatamente si cambia el estado de un servicio.

```
$ storagegrid-status
Host Name                99-211
IP Address                10.96.99.211
Operating System Kernel  4.19.0                Verified
Operating System Environment Debian 10.1            Verified
StorageGRID Webscale Release 11.4.0                Verified
Networking                Verified
Storage Subsystem        Verified
Database Engine           5.5.9999+default Running
Network Monitoring        11.4.0                Running
Time Synchronization      1:4.2.8p10+dfsg Running
ams                        11.4.0                Running
cmn                        11.4.0                Running
nms                        11.4.0                Running
ssm                        11.4.0                Running
mi                         11.4.0                Running
dynip                     11.4.0                Running
nginx                     1.10.3                Running
tomcat                    9.0.27                Running
grafana                   6.4.3                 Running
mgmt api                  11.4.0                Running
prometheus                11.4.0                Running
persistence               11.4.0                Running
ade exporter              11.4.0                Running
alertmanager              11.4.0                Running
attrDownPurge             11.4.0                Running
attrDownSamp1             11.4.0                Running
attrDownSamp2             11.4.0                Running
node exporter             0.17.0+ds             Running
sg snmp agent             11.4.0                Running
```

8. Confirme que el servicio `nginx-gw` se esté ejecutando `# service nginx-gw status`
9. Utilice `Lumberjack` para recolectar troncos: `# /usr/local/sbin/lumberjack.rb`

Si la autenticación falló en el pasado, puede usar las opciones de script `--start` y `--end` de Lumberjack para especificar el rango de tiempo apropiado. Utilice `lumberjack -h` para obtener detalles sobre estas opciones.

La salida a la terminal indica dónde se ha copiado el archivo de registro.

10. Revise los siguientes registros:

- `/var/local/log/bycast.log`
- `/var/local/log/bycast-err.log`
- `/var/local/log/nms.log`
- `**/*commands.txt`

11. Si no pudo identificar ningún problema con el nodo de administración, emita cualquiera de los siguientes comandos para determinar las direcciones IP de los tres nodos de almacenamiento que ejecutan el servicio ADC en su sitio. Normalmente, estos son los primeros tres nodos de almacenamiento que se instalan en el sitio.

```
# cat /etc/hosts
```

```
# gpt-list-services adc
```

Los nodos de administración utilizan el servicio ADC durante el proceso de autenticación.

12. Desde el nodo de administración, use `ssh` para iniciar sesión en cada uno de los nodos de almacenamiento de ADC, utilizando las direcciones IP que identificó.
13. Ver el estado de todos los servicios que se ejecutan en el nodo de la red: `storagegrid-status`

Asegúrese de que los servicios `idnt`, `acct`, `nginx` y `cassandra` estén todos en ejecución.

14. Repetir los pasos [Utilice a Lumberjack para recolectar troncos](#) y [Revisar registros](#) para revisar los registros en los nodos de almacenamiento.
15. Si no puede resolver el problema, comuníquese con el soporte técnico.

Proporcione los registros que recopiló al soporte técnico. Consulte también ["Referencia de archivos de registro"](#).

Problemas de interfaz de usuario

Es posible que la interfaz de usuario del Administrador de red o del Administrador de inquilinos no responda como se espera después de actualizar el software StorageGRID.

Pasos

1. Asegúrate de que estás usando un ["navegador web compatible"](#).
2. Limpia el caché de tu navegador web.

Al borrar la memoria caché se eliminan los recursos obsoletos utilizados por la versión anterior del software StorageGRID y se permite que la interfaz de usuario vuelva a funcionar correctamente. Para obtener instrucciones, consulte la documentación de su navegador web.

Solucionar problemas de red, hardware y plataforma

Hay varias tareas que puede realizar para ayudar a determinar el origen de los problemas relacionados con la red, el hardware y la plataforma de StorageGRID .

Errores "422: Entidad no procesable"

El error 422: Entidad no procesable puede ocurrir por diferentes motivos. Verifique el mensaje de error para determinar qué causó el problema.

Si ve uno de los mensajes de error enumerados, realice la acción recomendada.

Mensaje de error	Causa raíz y acción correctiva
<pre>422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839</pre>	Este mensaje puede aparecer si selecciona la opción No usar TLS para Seguridad de la capa de transporte (TLS) al configurar la federación de identidad mediante Windows Active Directory (AD). El uso de la opción No usar TLS no es compatible con servidores AD que implementan la firma LDAP. Debe seleccionar la opción Usar STARTTLS o la opción Usar LDAPS para TLS.

Mensaje de error	Causa raíz y acción correctiva
<pre>422: Unprocessable Entity Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)</pre>	Este mensaje aparece si intenta utilizar un cifrado no compatible para realizar una conexión de seguridad de la capa de transporte (TLS) desde StorageGRID a un sistema externo utilizado para identificar federaciones o grupos de almacenamiento en la nube. Verifique los cifrados que ofrece el sistema externo. El sistema debe utilizar uno de los "cifrados compatibles con StorageGRID" para conexiones TLS salientes, como se muestra en las instrucciones para administrar StorageGRID.

Alerta de discrepancia de MTU de la red Grid

La alerta **Desajuste de MTU de red de cuadrícula** se activa cuando la configuración de la unidad de transmisión máxima (MTU) para la interfaz de red de cuadrícula (eth0) difiere significativamente entre los nodos de la cuadrícula.

Acerca de esta tarea

Las diferencias en la configuración de MTU podrían indicar que algunas redes eth0, pero no todas, están configuradas para tramas gigantes. Una discrepancia en el tamaño de MTU de más de 1000 podría provocar problemas de rendimiento de la red.

Pasos

1. Enumere las configuraciones de MTU para eth0 en todos los nodos.
 - Utilice la consulta proporcionada en el Administrador de cuadrícula.
 - Navegar a *primary Admin Node IP address/metrics/graph* e ingrese la siguiente consulta: `node_network_mtu_bytes{device="eth0"}`
2. ["Modificar la configuración de MTU"](#) según sea necesario para garantizar que sean los mismos para la interfaz de red Grid (eth0) en todos los nodos.
 - Para los nodos basados en Linux y VMware, utilice el siguiente comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

Ejemplo: `change-ip.py -n node 1500 grid admin`

Nota: En los nodos basados en Linux, si el valor de MTU deseado para la red en el contenedor excede el valor ya configurado en la interfaz del host, primero debe configurar la interfaz del host para que tenga el valor de MTU deseado y luego usar el `change-ip.py` script para cambiar el valor de MTU de la red en el contenedor.

Utilice los siguientes argumentos para modificar la MTU en nodos basados en Linux o VMware.

Argumentos posicionales	Descripción
<code>mtu</code>	La MTU a configurar. Debe estar en el rango de 1280 a 9216.
<code>network</code>	Las redes a las que se aplicará la MTU. Incluya uno o más de los siguientes tipos de red: • red • administración • cliente

+

Argumentos opcionales	Descripción
<code>-h, - help</code>	Mostrar el mensaje de ayuda y salir.
<code>-n node, --node node</code>	El nodo. El valor predeterminado es el nodo local.

Alerta de error en la recepción de trama de la red del nodo

Las alertas de **Error de trama de recepción de red de nodo** pueden deberse a problemas de conectividad entre StorageGRID y el hardware de su red. Esta alerta desaparece por sí sola una vez que se soluciona el problema subyacente.

Acerca de esta tarea

Las alertas de **Error de trama de recepción de red de nodo** pueden deberse a los siguientes problemas con el hardware de red que se conecta a StorageGRID:

- La corrección de errores hacia adelante (FEC) es necesaria y no se utiliza
- Desajuste entre el puerto del conmutador y la MTU de la NIC
- Altas tasas de error de enlace
- Desbordamiento del búfer de anillo de la NIC

Pasos

1. Siga los pasos de solución de problemas para todas las posibles causas de esta alerta dada su configuración de red.
2. Realice los siguientes pasos según la causa del error:

Desajuste de FEC



Estos pasos se aplican únicamente a las alertas de **Error de trama de recepción de red de nodo** provocadas por una falta de coincidencia de FEC en los dispositivos StorageGRID .

- a. Verifique el estado FEC del puerto en el conmutador conectado a su dispositivo StorageGRID .
- b. Verifique la integridad física de los cables del aparato al interruptor.
- c. Si desea cambiar la configuración de FEC para intentar resolver la alerta, primero asegúrese de que el dispositivo esté configurado para el modo **Automático** en la página Configuración de enlace del Instalador del dispositivo StorageGRID (consulte las instrucciones para su dispositivo):
 - "SG6160"
 - "SGF6112"
 - "SG6000"
 - "SG5800"
 - "SG5700"
 - "SG110 y SG1100"
 - "SG100 y SG1000"
- d. Cambie la configuración de FEC en los puertos del conmutador. Los puertos del dispositivo StorageGRID ajustarán su configuración FEC para que coincida, si es posible.

No se pueden configurar los ajustes de FEC en los dispositivos StorageGRID . En lugar de ello, los dispositivos intentan descubrir y reflejar la configuración de FEC en los puertos del conmutador a los que están conectados. Si los enlaces se fuerzan a velocidades de red de 25 GbE o 100 GbE, es posible que el conmutador y la NIC no puedan negociar una configuración FEC común. Sin una configuración FEC común, la red volverá al modo "sin FEC". Cuando FEC no está habilitado, las conexiones son más susceptibles a errores causados por ruido eléctrico.



Los dispositivos StorageGRID admiten FEC Firecode (FC) y Reed Solomon (RS), así como también no admiten FEC.

Desajuste entre el puerto del conmutador y la MTU de la NIC

Si la alerta es causada por una falta de coincidencia entre el puerto del conmutador y la MTU de la NIC, verifique que el tamaño de MTU configurado en el nodo sea el mismo que la configuración de MTU para el puerto del conmutador.

El tamaño de MTU configurado en el nodo puede ser menor que la configuración en el puerto del conmutador al que está conectado el nodo. Si un nodo StorageGRID recibe una trama Ethernet más grande que su MTU, lo cual es posible con esta configuración, es posible que se informe la alerta **Error de trama de recepción de red de nodo**. Si cree que esto es lo que está sucediendo, cambie la MTU del puerto del conmutador para que coincida con la MTU de la interfaz de red StorageGRID , o cambie la MTU de la interfaz de red StorageGRID para que coincida con el puerto del conmutador, según sus objetivos o requisitos de MTU de extremo a extremo.



Para obtener el mejor rendimiento de la red, todos los nodos deben configurarse con valores de MTU similares en sus interfaces de red Grid. La alerta **No coincide la MTU de la red de cuadrícula** se activa si hay una diferencia significativa en las configuraciones de MTU para la red de cuadrícula en nodos individuales. Los valores de MTU no tienen que ser los mismos para todos los tipos de red. Ver [Solucionar la alerta de desajuste de MTU de la red Grid](#) Para más información.



Ver también "[Cambiar la configuración de MTU](#)".

Altas tasas de error de enlace

- Habilitar FEC, si aún no está habilitado.
- Verifique que su cableado de red sea de buena calidad y no esté dañado o mal conectado.
- Si los cables no parecen ser el problema, comuníquese con el soporte técnico.



Es posible que notes altos índices de error en un entorno con alto ruido eléctrico.

Desbordamiento del búfer de anillo de la NIC

Si el error es un desbordamiento del búfer del anillo de NIC, comuníquese con el soporte técnico.

El búfer de anillo puede saturarse cuando el sistema StorageGRID está sobrecargado y no puede procesar eventos de red de manera oportuna.

3. Monitoree el problema y comuníquese con el soporte técnico si la alerta no se resuelve.

Errores de sincronización horaria

Es posible que experimente problemas con la sincronización horaria en su red.

Si encuentra problemas de sincronización horaria, verifique que haya especificado al menos cuatro fuentes NTP externas, cada una de las cuales proporcione una referencia Stratum 3 o superior, y que todas las fuentes NTP externas estén funcionando normalmente y sean accesibles para los nodos StorageGRID.



Cuando "[especificando la fuente NTP externa](#)" Para una instalación de StorageGRID a nivel de producción, no utilice el servicio de hora de Windows (W32Time) en una versión de Windows anterior a Windows Server 2016. El servicio de hora en versiones anteriores de Windows no es lo suficientemente preciso y Microsoft no lo admite para su uso en entornos de alta precisión, como StorageGRID.

Linux: Problemas de conectividad de red

Es posible que experimente problemas con la conectividad de red para los nodos StorageGRID alojados en hosts Linux.

Clonación de direcciones MAC

En algunos casos, los problemas de red se pueden resolver mediante la clonación de direcciones MAC. Si está utilizando hosts virtuales, configure el valor de la clave de clonación de dirección MAC para cada una de sus redes en "verdadero" en su archivo de configuración de nodo. Esta configuración hace que la dirección MAC del contenedor StorageGRID utilice la dirección MAC del host. Para crear archivos de configuración de nodo, consulte las instrucciones para "[Red Hat Enterprise Linux](#)" o "[Ubuntu o Debian](#)".



Cree interfaces de red virtuales independientes para que las utilice el sistema operativo host Linux. El uso de las mismas interfaces de red para el sistema operativo host Linux y el contenedor StorageGRID puede provocar que el sistema operativo host se vuelva inaccesible si no se ha habilitado el modo promiscuo en el hipervisor.

Para obtener más información sobre cómo habilitar la clonación de MAC, consulte las instrucciones para ["Red Hat Enterprise Linux"](#) o ["Ubuntu o Debian"](#).

Modo promiscuo

Si no desea utilizar la clonación de direcciones MAC y prefiere permitir que todas las interfaces reciban y transmitan datos para direcciones MAC distintas de las asignadas por el hipervisor, asegúrese de que las propiedades de seguridad en los niveles de conmutador virtual y grupo de puertos estén configuradas en **Aceptar** para Modo promiscuo, Cambios de dirección MAC y Transmisiones falsificadas. Los valores establecidos en el conmutador virtual pueden ser anulados por los valores a nivel del grupo de puertos, así que asegúrese de que las configuraciones sean las mismas en ambos lugares.

Para obtener más información sobre el uso del modo promiscuo, consulte las instrucciones para ["Red Hat Enterprise Linux"](#) o ["Ubuntu o Debian"](#).

Linux: El estado del nodo es "huérfano"

Un nodo Linux en estado huérfano generalmente indica que el servicio StorageGrid o el demonio del nodo StorageGRID que controla el contenedor del nodo murió inesperadamente.

Acerca de esta tarea

Si un nodo Linux informa que está en estado huérfano, debe:

- Verifique los registros para detectar errores y mensajes.
- Intente iniciar el nodo nuevamente.
- Si es necesario, utilice los comandos del motor de contenedor para detener el contenedor de nodo existente.
- Reinicie el nodo.

Pasos

1. Verifique los registros tanto del demonio de servicio como del nodo huérfano para detectar errores obvios o mensajes sobre salidas inesperadas.
2. Inicie sesión en el host como root o usando una cuenta con permiso sudo.
3. Intente iniciar el nodo nuevamente ejecutando el siguiente comando: `$ sudo storagegrid node start node-name`

```
$ sudo storagegrid node start DC1-S1-172-16-1-172
```

Si el nodo está huérfano, la respuesta es

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. Desde Linux, detenga el motor del contenedor y cualquier proceso de control del nodo de almacenamiento en red. Por ejemplo: `sudo docker stop --time secondscontainer-name`

Para `seconds` , ingrese la cantidad de segundos que desea esperar hasta que el contenedor se detenga (normalmente 15 minutos o menos). Por ejemplo:

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. Reiniciar el nodo: `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

Linux: Solución de problemas de compatibilidad con IPv6

Es posible que necesite habilitar la compatibilidad con IPv6 en el kernel si ha instalado nodos StorageGRID en hosts Linux y observa que las direcciones IPv6 no se han asignado a los contenedores de nodos como se esperaba.

Acerca de esta tarea

Para ver la dirección IPv6 que se ha asignado a un nodo de la red:

1. Seleccione **NODOS** y seleccione el nodo.
2. Seleccione **Mostrar direcciones IP adicionales** junto a **Direcciones IP** en la pestaña Descripción general.

Si no se muestra la dirección IPv6 y el nodo está instalado en un host Linux, siga estos pasos para habilitar la compatibilidad con IPv6 en el kernel.

Pasos

1. Inicie sesión en el host como root o usando una cuenta con permiso sudo.
2. Ejecute el siguiente comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

El resultado debe ser 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```



Si el resultado no es 0, consulte la documentación de su sistema operativo para cambiarlo. `sysctl` ajustes. Luego, cambie el valor a 0 antes de continuar.

3. Ingrese al contenedor del nodo StorageGRID : `storagegrid node enter node-name`
4. Ejecute el siguiente comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

El resultado debería ser 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```



Si el resultado no es 1, este procedimiento no se aplica. Póngase en contacto con el soporte técnico.

5. Salir del contenedor: `exit`

```
root@DC1-S1:~ # exit
```

6. Como root, edite el siguiente archivo: `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Localice las siguientes dos líneas y elimine las etiquetas de comentarios. Luego, guarde y cierre el archivo.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Ejecute estos comandos para reiniciar el contenedor StorageGRID :

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

Solucionar problemas de un servidor syslog externo

La siguiente tabla describe los mensajes de error que pueden estar relacionados con el uso de un servidor syslog externo y enumera las acciones correctivas.

El asistente para configurar el servidor syslog externo muestra estos errores si tiene problemas al enviar mensajes de prueba para validar que el servidor syslog externo esté configurado correctamente.

Los problemas en tiempo de ejecución podrían ser reportados por el ["Error de reenvío del servidor syslog externo"](#) alerta. Si recibe esta alerta, siga las instrucciones de la alerta para reenviar los mensajes de prueba para poder obtener mensajes de error detallados.

Para obtener más información sobre cómo enviar información de auditoría a un servidor syslog externo, consulte:

- ["Consideraciones para el uso de un servidor syslog externo"](#)
- ["Configurar mensajes de auditoría y servidor syslog externo"](#)

Mensaje de error	Descripción y acciones recomendadas
No se puede resolver el nombre de host	El FQDN que ingresó para el servidor syslog no se pudo resolver a una dirección IP. 1. Verifique el nombre de host ingresado. Si ingresó una dirección IP, asegúrese de que sea una dirección IP válida en notación WXYZ ("decimal punteado"). 2. Verifique que los servidores DNS estén configurados correctamente. 3. Confirme que cada nodo pueda acceder a las direcciones IP del servidor DNS.
Conexión rechazada	Se rechazó una conexión TCP o TLS al servidor syslog. Es posible que no haya ningún servicio escuchando en el puerto TCP o TLS del host, o que un firewall esté bloqueando el acceso. 1. Verifique que haya ingresado el FQDN o la dirección IP, el puerto y el protocolo correctos para el servidor syslog. 2. Confirme que el host del servicio syslog esté ejecutando un demonio syslog que esté escuchando en el puerto especificado. 3. Confirme que un firewall no esté bloqueando el acceso a las conexiones TCP/TLS desde los nodos a la IP y al puerto del servidor syslog.
Red inalcanzable	El servidor syslog no está en una subred conectada directamente. Un enrutador devolvió un mensaje de error ICMP para indicar que no pudo reenviar los mensajes de prueba desde los nodos enumerados al servidor syslog. 1. Verifique que haya ingresado el FQDN o la dirección IP correctos para el servidor syslog. 2. Para cada nodo enumerado, verifique la Lista de subredes de red de cuadrícula, las Listas de subredes de redes de administración y las puertas de enlace de red de cliente. Confirme que estén configurados para enrutar el tráfico al servidor syslog a través de la interfaz de red y la puerta de enlace esperadas (Grid, Admin o Client).

Mensaje de error	Descripción y acciones recomendadas
Host inalcanzable	El servidor syslog está en una subred conectada directamente (subred utilizada por los nodos enumerados para sus direcciones IP de red, administrador o cliente). Los nodos intentaron enviar mensajes de prueba, pero no recibieron respuestas a las solicitudes ARP para la dirección MAC del servidor syslog. 1. Verifique que haya ingresado el FQDN o la dirección IP correctos para el servidor syslog. 2. Compruebe que el host que ejecuta el servicio syslog esté activo.
Se agotó el tiempo de conexión	Se intentó una conexión TCP/TLS, pero no se recibió respuesta del servidor syslog durante mucho tiempo. Es posible que haya una configuración incorrecta de enrutamiento o que un firewall esté descartando tráfico sin enviar ninguna respuesta (una configuración común). 1. Verifique que haya ingresado el FQDN o la dirección IP correctos para el servidor syslog. 2. Para cada nodo enumerado, verifique la Lista de subredes de red de cuadrícula, las Listas de subredes de redes de administración y las puertas de enlace de red de cliente. Confirme que estén configurados para enrutar el tráfico al servidor syslog utilizando la interfaz de red y la puerta de enlace (Grid, Admin o Cliente) a través de las cuales espera que se llegue al servidor syslog. 3. Confirme que un firewall no esté bloqueando el acceso a las conexiones TCP/TLS desde los nodos enumerados a la IP y al puerto del servidor syslog.
Conexión cerrada por el socio	Se estableció exitosamente una conexión TCP con el servidor syslog pero luego se cerró. Las razones para esto podrían incluir: • Es posible que se haya reiniciado o reiniciado el servidor syslog. • El nodo y el servidor syslog pueden tener diferentes configuraciones TCP/TLS. • Es posible que un firewall intermedio esté cerrando conexiones TCP inactivas. • Es posible que un servidor que no sea syslog y que esté escuchando en el puerto del servidor syslog haya cerrado la conexión. Para resolver este problema: 1. Verifique que haya ingresado el FQDN o la dirección IP, el puerto y el protocolo correctos para el servidor syslog. 2. Si está utilizando TLS, confirme que el servidor syslog también esté utilizando TLS. Si está utilizando TCP, confirme que el servidor syslog también esté utilizando TCP. 3. Compruebe que no haya un firewall intermedio configurado para cerrar conexiones TCP inactivas.

Mensaje de error	Descripción y acciones recomendadas
Error de certificado TLS	El certificado de servidor recibido del servidor syslog no era compatible con el paquete de certificados CA y el certificado de cliente que proporcionó. 1. Confirme que el paquete de certificados de CA y el certificado de cliente (si hay alguno) sean compatibles con el certificado del servidor en el servidor syslog. 2. Confirme que las identidades en el certificado del servidor del servidor syslog incluyan los valores de IP o FQDN esperados.
Reenvío suspendido	Los registros de syslog ya no se reenvían al servidor de syslog y StorageGRID no puede detectar el motivo. Revise los registros de depuración proporcionados con este error para intentar determinar la causa raíz.
Sesión TLS finalizada	El servidor syslog finalizó la sesión TLS y StorageGRID no puede detectar el motivo. 1. Revise los registros de depuración proporcionados con este error para intentar determinar la causa raíz. 2. Verifique que haya ingresado el FQDN o la dirección IP, el puerto y el protocolo correctos para el servidor syslog. 3. Si está utilizando TLS, confirme que el servidor syslog también esté utilizando TLS. Si está utilizando TCP, confirme que el servidor syslog también esté utilizando TCP. 4. Confirme que el paquete de certificados de CA y el certificado de cliente (si hay alguno) sean compatibles con el certificado del servidor del servidor syslog. 5. Confirme que las identidades en el certificado del servidor del servidor syslog incluyan los valores de IP o FQDN esperados.
Consulta de resultados fallida	El nodo de administración utilizado para la configuración y prueba del servidor syslog no puede solicitar resultados de pruebas de los nodos enumerados. Es posible que uno o más nodos estén inactivos. 1. Siga los pasos estándar de solución de problemas para asegurarse de que los nodos estén en línea y que todos los servicios esperados estén funcionando. 2. Reinicie el servicio miscd en los nodos enumerados.

Revisar los registros de auditoría

Mensajes y registros de auditoría

Estas instrucciones contienen información sobre la estructura y el contenido de los mensajes de auditoría y los registros de auditoría de StorageGRID . Puede utilizar esta

información para leer y analizar el registro de auditoría de la actividad del sistema.

Estas instrucciones están dirigidas a los administradores responsables de producir informes de actividad y uso del sistema que requieren el análisis de los mensajes de auditoría del sistema StorageGRID .

Para utilizar el archivo de registro de texto, debe tener acceso al recurso compartido de auditoría configurado en el nodo de administración.

Para obtener información sobre cómo configurar los niveles de mensajes de auditoría y utilizar un servidor syslog externo, consulte "[Configurar mensajes de auditoría y destinos de registro](#)".

Auditoría del flujo y retención de mensajes

Todos los servicios de StorageGRID generan mensajes de auditoría durante el funcionamiento normal del sistema. Debe comprender cómo estos mensajes de auditoría se mueven a través del sistema StorageGRID hasta el `audit.log` archivo.

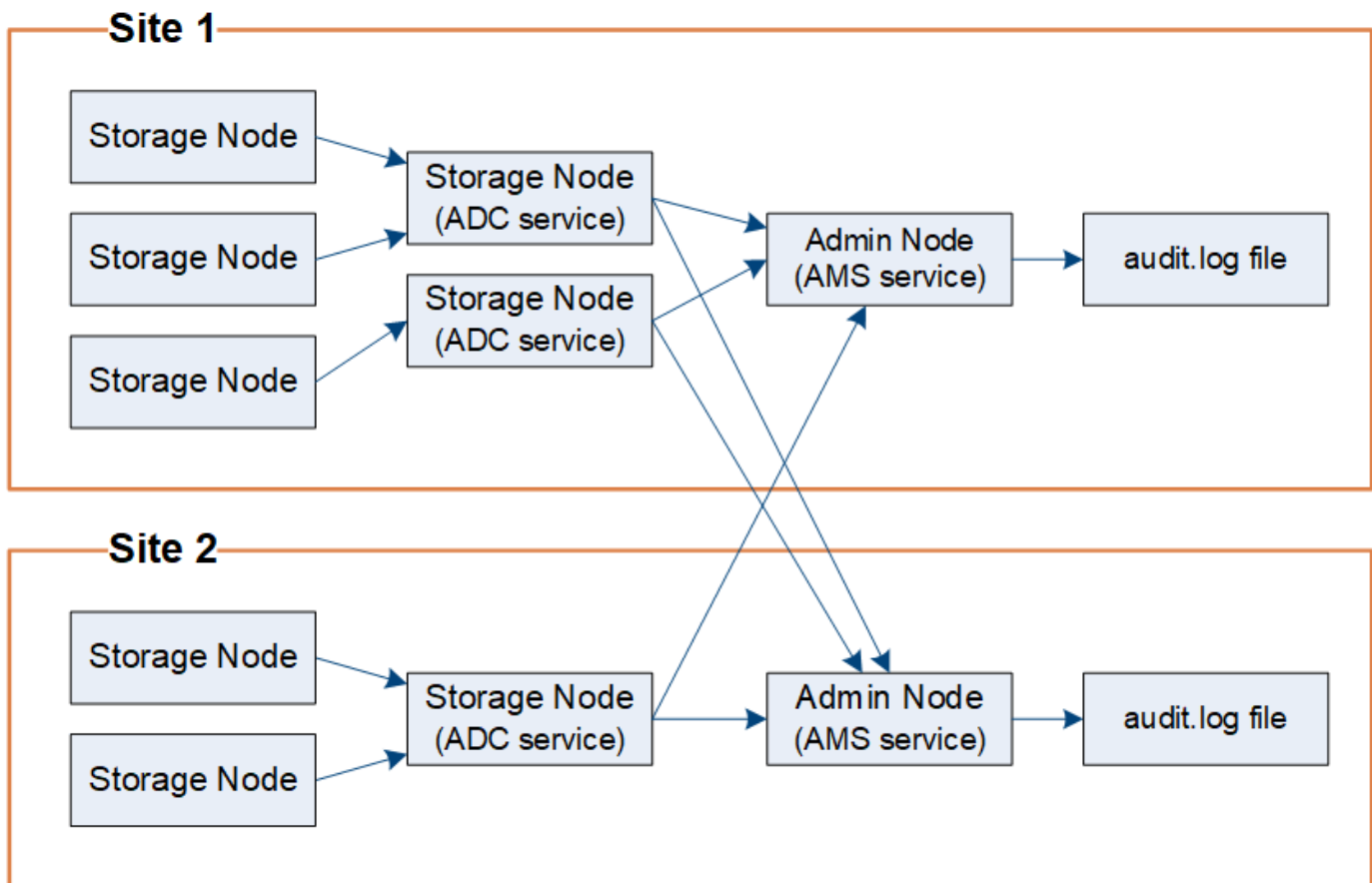
Flujo de mensajes de auditoría

Los mensajes de auditoría son procesados por los nodos de administración y por aquellos nodos de almacenamiento que tienen un servicio de controlador de dominio administrativo (ADC).

Como se muestra en el diagrama de flujo de mensajes de auditoría, cada nodo StorageGRID envía sus mensajes de auditoría a uno de los servicios ADC en el 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 un relé y envía su colección de mensajes de auditoría a cada nodo de administración en el sistema StorageGRID , lo que proporciona a cada nodo de administración un registro completo de la actividad del sistema.

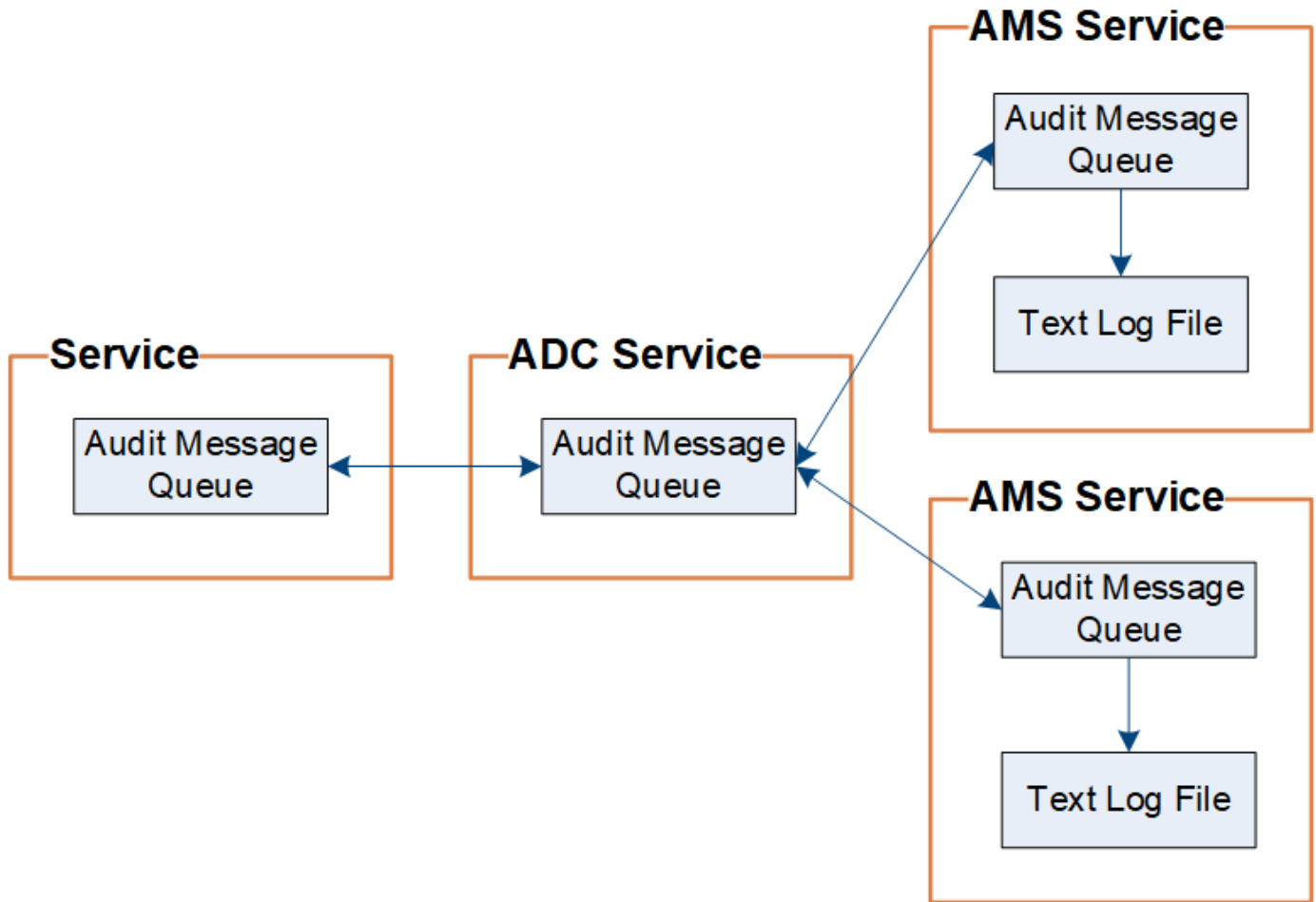
Cada nodo de administración almacena mensajes de auditoría en archivos de registro de texto; el archivo de registro activo se denomina `audit.log` .



Retención de mensajes de auditoría

StorageGRID utiliza un proceso de copia y eliminación para garantizar que no se pierdan mensajes de auditoría antes de que puedan escribirse en el registro de auditoría.

Cuando un nodo genera o retransmite un mensaje de auditoría, el mensaje se almacena en una cola de mensajes de auditoría en el disco del sistema del nodo de la red. Siempre se guarda una copia del mensaje en una cola de mensajes de auditoría hasta que el mensaje se escribe en el archivo de registro de auditoría en el nodo de administración. `/var/local/log` directorio. Esto ayuda a evitar la pérdida de un mensaje de auditoría durante el transporte.



La cola de mensajes de auditoría puede aumentar temporalmente debido a problemas de conectividad de red o capacidad de auditoría insuficiente. A medida que aumentan las colas, consumen más espacio disponible en cada nodo. `/var/local/` directorio. Si el problema persiste y el directorio de mensajes de auditoría de un nodo se llena demasiado, los nodos individuales priorizarán el procesamiento de su trabajo atrasado y quedarán temporalmente no disponibles para nuevos mensajes.

En concreto, es posible que veas los siguientes comportamientos:

- Si el `/var/local/log` Si el directorio utilizado por un nodo de administración se llena, dicho nodo se marcará como no disponible para nuevos mensajes de auditoría hasta que el directorio ya no esté lleno. Las solicitudes de cliente S3 no se ven afectadas. La alarma XAMS (Repositorios de auditoría inaccesibles) se activa cuando un repositorio de auditoría no está disponible.
- Si el `/var/local/` Si el directorio utilizado por un nodo de almacenamiento con el servicio ADC se llena en un 92 %, el nodo se marcará como no disponible para auditar mensajes hasta que el directorio esté lleno solo en un 87 %. Las solicitudes del cliente S3 a otros nodos no se ven afectadas. La alarma NRLY (Relés de auditoría disponibles) se activa cuando los relés de auditoría no están disponibles.



Si no hay nodos de almacenamiento disponibles con el servicio ADC, los nodos de almacenamiento almacenan los mensajes de auditoría localmente en el `/var/local/log/localaudit.log` archivo.

- Si el `/var/local/` Cuando el directorio utilizado por un nodo de almacenamiento se llena al 85 %, el nodo comenzará a rechazar solicitudes de clientes S3 con `503 Service Unavailable`.

Los siguientes tipos de problemas pueden provocar que las colas de mensajes de auditoría crezcan mucho:

- La interrupción de un nodo de administración o de un nodo de almacenamiento con el servicio ADC. Si uno de los nodos del sistema está inactivo, los nodos restantes pueden quedar atrasados.
- Una tasa de actividad sostenida que excede la capacidad de auditoría del sistema.
- El `/var/local/` El espacio en un nodo de almacenamiento ADC se llena por razones no relacionadas con los mensajes de auditoría. Cuando esto sucede, el nodo deja de aceptar nuevos mensajes de auditoría y prioriza su trabajo pendiente actual, lo que puede provocar retrasos en otros nodos.

Alerta de cola de auditoría grande y alarma de mensajes de auditoría en cola (AMQS)

Para ayudarlo a monitorear 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 la cantidad de mensajes en una cola de nodo de almacenamiento o en una cola de nodo de administración alcanza ciertos umbrales.

Si se activa la alerta **Cola de auditoría grande** o la alarma AMQS heredada, comience por verificar la carga en el sistema: si hubo una cantidad significativa de transacciones recientes, la alerta y la alarma deberían resolverse con el tiempo y pueden ignorarse.

Si la alerta o alarma persiste y aumenta en gravedad, vea un gráfico del tamaño de la cola. Si el número aumenta de manera constante a lo largo de horas o días, es probable que la carga de auditoría haya excedido la capacidad de auditoría del sistema. Reduzca la tasa de operación del cliente o disminuya la cantidad de mensajes de auditoría registrados cambiando el nivel de auditoría de Escrituras de cliente y Lecturas de cliente a Error o Desactivado. Ver ["Configurar mensajes de auditoría y destinos de registro"](#) .

Mensajes duplicados

El sistema StorageGRID adopta un enfoque conservador si ocurre una falla en la red o en un nodo. Por este motivo, podrían existir mensajes duplicados en el registro de auditoría.

Archivo de registro de auditoría de acceso

La parte de auditoría contiene los activos `audit.log` archivo y cualquier archivo de registro de auditoría comprimido. Puede acceder a los archivos de registro de auditoría directamente desde la línea de comando del nodo de administración.

Antes de empezar

- Tienes ["permisos de acceso específicos"](#) .
- Debes tener el `Passwords.txt` archivo.
- Debes conocer la dirección IP de un nodo de administración.

Pasos

1. Inicie sesión en un nodo de administración:

- a. Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
- b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#` .

2. Vaya al directorio que contiene los archivos de registro de auditoría:

```
cd /var/local/log
```

3. Ver el archivo de registro de auditoría actual o guardado, según sea necesario.

Rotación de archivos de registro de auditoría

Los archivos de registros de auditoría se guardan en un nodo de administración.

`/var/local/log` directorio. Los archivos de registro de auditoría activos se denominan `audit.log`.



Opcionalmente, puede cambiar el destino de los registros de auditoría y enviar información de auditoría a un servidor syslog externo. Los registros locales de registros de auditoría continúan generándose y almacenándose cuando se configura un servidor syslog externo. Ver ["Configurar mensajes de auditoría y destinos de registro"](#).

Una vez al día, el activo `audit.log` El archivo se guarda y se crea uno nuevo. `audit.log` El archivo se inicia. 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 archivo utilizan la fecha en que se guardó el archivo, más un número, en el formato `yyyy-mm-dd.txt.n`. Por ejemplo, `2018-04-15.txt` y `2018-04-15.txt.1` son el primer y segundo archivo de registro creados y guardados el 15 de abril de 2018.

Después de un día, el archivo guardado se comprime y se renombra, en el formato `yyyy-mm-dd.txt.gz`, que conserva la fecha original. Con el tiempo, esto genera el consumo del almacenamiento asignado para los registros de auditoría en el nodo de administración. Un script monitorea el consumo de espacio del registro de auditoría y elimina archivos de registro según sea necesario para liberar espacio en el `/var/local/log` directorio. Los registros de auditoría se eliminan según la fecha en que se crearon, siendo los más antiguos los que se eliminan primero. Puedes monitorizar las acciones del script en el siguiente archivo: `/var/local/log/manage-audit.log`.

Este ejemplo muestra el activo `audit.log` archivo, archivo del día anterior(`2018-04-15.txt`), y el archivo comprimido del día anterior(`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Formato de archivo de registro de auditoría

Formato de archivo de registro de auditoría

Los archivos de registro de auditoría se encuentran en cada nodo de administración y contienen una colección de mensajes de auditoría individuales.

Cada mensaje de auditoría contiene lo siguiente:

- El Tiempo Universal Coordinado (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 en sí, encerrado entre corchetes y comenzando con AUDT .

El siguiente ejemplo muestra tres mensajes de auditoría en un archivo de registro de auditoría (se agregan saltos de línea para facilitar la lectura). Estos mensajes se generaron cuando un inquilino creó un depósito S3 y agregó dos objetos a ese depósito.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][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(FC32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][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(FC32):S3RQ][ATID(UI64):13489590586043706682]]
```

En su formato predeterminado, los mensajes de auditoría en los archivos de registro de auditoría no son

fáciles de leer ni interpretar. Puedes utilizar el "[herramienta de auditoría y explicación](#)" para obtener resúmenes simplificados de los mensajes de auditoría en el registro de auditoría. Puedes utilizar el "[herramienta de suma de auditoría](#)" para resumir cuántas operaciones de escritura, lectura y eliminación se registraron y cuánto tiempo tomaron estas operaciones.

Utilice la herramienta de auditoría y explicación

Puedes utilizar el `audit-explain` herramienta para traducir los mensajes de auditoría en el registro de auditoría a un formato fácil de leer.

Antes de empezar

- Tienes "[permisos de acceso específicos](#)".
- Debes tener el `Passwords.txt` archivo.
- Debe conocer la dirección IP del nodo de administración principal.

Acerca de esta tarea

El `audit-explain` La herramienta, disponible en el nodo de administración principal, proporciona resúmenes simplificados de los mensajes de auditoría en un registro de auditoría.



El `audit-explain` La herramienta está destinada principalmente a ser utilizada por el soporte técnico durante operaciones de resolución de problemas. Tratamiento `audit-explain` Las consultas pueden consumir una gran cantidad de energía de la CPU, lo que podría afectar las operaciones de StorageGRID .

Este ejemplo muestra una salida típica del `audit-explain` herramienta. Estos cuatro "[ESPOLVO](#)" Se generaron mensajes de auditoría cuando el inquilino S3 con ID de cuenta 92484777680322627870 utilizó solicitudes S3 PUT para crear un depósito llamado "bucket1" y agregar tres objetos a ese depósito.

```
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
```

El `audit-explain` La herramienta puede hacer lo siguiente:

- Procesar registros de auditoría simples o comprimidos. Por ejemplo:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

- Procesar múltiples archivos simultáneamente. Por ejemplo:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/log/*
```


- Acepte la entrada de una tubería, lo que le permite filtrar y preprocesar la entrada utilizando el `grep` comando u otros medios. Por ejemplo:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Debido a que los registros de auditoría pueden ser muy grandes y lentos de analizar, puede ahorrar tiempo filtrando las partes que desea ver y ejecutando `audit-explain` en las partes, en lugar de en todo el archivo.



El `audit-explain` La herramienta no acepta archivos comprimidos como entrada canalizada. Para procesar archivos comprimidos, proporcione sus nombres de archivo como argumentos de línea de comando o utilice el `zcat` herramienta para descomprimir los archivos primero. Por ejemplo:

```
zcat audit.log.gz | audit-explain
```

Utilice el `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 el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Introduzca el siguiente comando, donde `/var/local/log/audit.log` representa el nombre y la ubicación del archivo o archivos que desea analizar:

```
$ audit-explain /var/local/log/audit.log
```

El `audit-explain` La herramienta imprime interpretaciones legibles por humanos de todos los mensajes en el archivo o archivos especificados.



Para reducir la longitud de las líneas y facilitar la legibilidad, las marcas de tiempo no se muestran de forma predeterminada. Si desea ver las marcas de tiempo, utilice la marca de tiempo (`-t`) opción.

Utilice la herramienta de suma de auditoría

Puedes utilizar el `audit-sum` herramienta para contar los mensajes de auditoría de escritura, lectura, encabezado y eliminación y para ver el tiempo mínimo, máximo y promedio (o tamaño) para cada tipo de operación.

Antes de empezar

- Tienes ["permisos de acceso específicos"](#) .
- Debes tener el Passwords.txt archivo.
- Debe conocer la dirección IP del nodo de administración principal.

Acerca de esta tarea

El `audit-sum` La herramienta, disponible en el nodo de administración principal, resume cuántas operaciones de escritura, lectura y eliminación se registraron y cuánto tiempo tomaron estas operaciones.



El `audit-sum` La herramienta está destinada principalmente a ser utilizada por el soporte técnico durante operaciones de resolución de problemas. Tratamiento `audit-sum` Las consultas pueden consumir una gran cantidad de energía de la CPU, lo que podría afectar las operaciones de StorageGRID .

Este ejemplo muestra una salida típica del `audit-sum` herramienta. Este ejemplo muestra cuánto tiempo tomaron las operaciones del 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			

El `audit-sum` La herramienta proporciona recuentos y tiempos para los siguientes mensajes de auditoría de S3, Swift e ILM en un registro de auditoría.



Los códigos de auditoría se eliminan del producto y de la documentación a medida que las funciones quedan obsoletas. Si encuentra un código de auditoría que no aparece aquí, consulte las versiones anteriores de este tema para ver versiones anteriores de SG. Por ejemplo, ["Documentación sobre el uso de la herramienta de suma de auditoría de StorageGRID 11.8"](#) .

Código	Descripción	Referirse a
IDEL	Eliminación iniciada por ILM: registra cuándo ILM inicia el proceso de eliminación de un objeto.	"IDEL: Eliminación iniciada por ILM"
SDEL	S3 ELIMINAR: registra una transacción exitosa para eliminar un objeto o depósito.	"SDEL: S3 ELIMINAR"

Código	Descripción	Referirse a
SGET	S3 GET: registra una transacción exitosa para recuperar un objeto o enumerar los objetos en un depósito.	"SGET: S3 OBTENER"
KARITÉ	S3 HEAD: Registra una transacción exitosa para verificar la existencia de un objeto o depósito.	"SHEA: CABEZA T3"
ESPOLVO	S3 PUT: Registra una transacción exitosa para crear un nuevo objeto o depósito.	"SPUT: S3 PONER"
WDEL	Swift DELETE: registra una transacción exitosa para eliminar un objeto o contenedor.	"WDEL: Eliminación rápida"
WGET	Swift GET: registra una transacción exitosa para recuperar un objeto o enumerar los objetos en un contenedor.	"WGET: Obtención rápida"
TRIGO	Swift HEAD: registra una transacción exitosa para verificar la existencia de un objeto o contenedor.	"WHEA: CABEZA Veloz"
WPUT	Swift PUT: registra una transacción exitosa para crear un nuevo objeto o contenedor.	"WPUT: PUT rápido"

El `audit-sum` La herramienta puede hacer lo siguiente:

- Procesar registros de auditoría simples o comprimidos. Por ejemplo:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

- Procesar múltiples archivos simultáneamente. Por ejemplo:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/log/*
```

- Acepte la entrada de una tubería, lo que le permite filtrar y preprocesar la entrada utilizando el `grep` comando u otros medios. Por ejemplo:

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```



Esta herramienta no acepta archivos comprimidos como entrada canalizada. Para procesar archivos comprimidos, proporcione sus nombres de archivo como argumentos de línea de comando o utilice el `zcat` herramienta para descomprimir los archivos primero. Por ejemplo:

```
audit-sum audit.log.gz

zcat audit.log.gz | audit-sum
```

Puede utilizar las opciones de la línea de comandos para resumir las operaciones en los depósitos por separado de las operaciones en los objetos o para agrupar resúmenes de mensajes por nombre de depósito, por período de tiempo o por tipo de destino. De forma predeterminada, los resúmenes muestran el tiempo de operación mínimo, máximo y promedio, pero puede utilizar el `size (-s)` Opción para mirar el tamaño del objeto en su lugar.

Utilice el `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 el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Si desea analizar todos los mensajes relacionados con las operaciones de escritura, lectura, encabezado y eliminación, siga estos pasos:

- a. Introduzca el siguiente comando, donde `/var/local/log/audit.log` representa el nombre y la ubicación del archivo o archivos que desea analizar:

```
$ audit-sum /var/local/log/audit.log
```

Este ejemplo muestra una salida típica del `audit-sum` herramienta. Este ejemplo muestra cuánto tiempo tomaron las operaciones del protocolo.

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
=====			
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

En este ejemplo, las operaciones SGET (S3 GET) son las más lentas en promedio, con 1,13 segundos, pero las operaciones SGET y SPUT (S3 PUT) muestran tiempos de peor caso prolongados de aproximadamente 1770 segundos.

- b. Para mostrar las 10 operaciones de recuperación más lentas, utilice el comando `grep` para seleccionar solo mensajes SGET y agregar la opción de salida larga (`-l`) para incluir rutas de objetos:

```
grep SGET audit.log | audit-sum -l
```

Los resultados incluyen el tipo (objeto o depósito) y la ruta, lo que le permite buscar en el registro de auditoría otros mensajes relacionados con estos objetos particulares.

```

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/r90l0aQ8JB-1566861764-4519.iso
      1624414429      10.96.101.125      object      5375001556
      backup/r90l0aQ8JB-1566861764-6618.iso
      1533143793      10.96.101.125      object      5183661466
      backup/r90l0aQ8JB-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

```

+

En este ejemplo de salida, puede ver que las tres solicitudes GET de S3 más lentas fueron para objetos de aproximadamente 5 GB de tamaño, lo cual es mucho más grande que los otros objetos. El gran tamaño explica los tiempos de recuperación lentos en el peor de los casos.

3. Si desea determinar qué tamaños de objetos se están ingiriendo y recuperando de su cuadrícula, utilice la opción de tamaño(-s):

```
audit-sum -s audit.log
```

message group average (MB)	count	min (MB)	max (MB)
=====	=====	=====	=====
IDEL 1654.502	274	0.004	5000.000
SDEL 1.695	213371	0.000	10.504
SGET 14.920	201906	0.000	5000.000
SHEA 2.967	22716	0.001	10.504
SPUT 2.495	1771398	0.000	5000.000

En este ejemplo, el tamaño de objeto promedio para SPUT es inferior a 2,5 MB, pero el tamaño promedio para SGET es mucho mayor. La cantidad de mensajes SPUT es mucho mayor que la cantidad de mensajes SGET, lo que indica que la mayoría de los objetos nunca se recuperan.

4. Si desea determinar si las recuperaciones fueron lentas ayer:

- a. Emita el comando en el registro de auditoría apropiado y utilice la opción agrupar por tiempo(-gt), seguido del período de tiempo (por ejemplo, 15M, 1H, 10S):

```
grep SGET audit.log | audit-sum -gt 1H
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
2019-09-05T00 1.254	7591	0.010	1481.867
2019-09-05T01 1.115	4173	0.011	1740.290
2019-09-05T02 1.562	20142	0.011	1274.961
2019-09-05T03 1.254	57591	0.010	1383.867
2019-09-05T04 1.405	124171	0.013	1740.290
2019-09-05T05 1.562	420182	0.021	1274.511
2019-09-05T06 5.562	1220371	0.015	6274.961
2019-09-05T07 2.002	527142	0.011	1974.228
2019-09-05T08 1.105	384173	0.012	1740.290
2019-09-05T09 1.354	27591	0.010	1481.867

Estos resultados muestran que el tráfico GET de S3 aumentó entre las 06:00 y las 07:00. Los tiempos máximos y promedio también son considerablemente más altos en estos momentos y no aumentan gradualmente a medida que aumenta el recuento. Esto sugiere que se excedió la capacidad en algún lugar, quizás en la red o en la capacidad de la red para procesar solicitudes.

- b. Para determinar qué tamaño de objetos se recuperaron cada hora ayer, agregue la opción de tamaño(-s) al comando:

```
grep SGET audit.log | audit-sum -gt 1H -s
```


message group average(B)	count	min(B)	max(B)
=====	=====	=====	=====
2019-09-05T00 1.976	7591	0.040	1481.867
2019-09-05T01 2.062	4173	0.043	1740.290
2019-09-05T02 2.303	20142	0.083	1274.961
2019-09-05T03 1.182	57591	0.912	1383.867
2019-09-05T04 1.528	124171	0.730	1740.290
2019-09-05T05 2.398	420182	0.875	4274.511
2019-09-05T06 51.328	1220371	0.691	5663711385.961
2019-09-05T07 2.147	527142	0.130	1974.228
2019-09-05T08 1.878	384173	0.625	1740.290
2019-09-05T09 1.354	27591	0.689	1481.867

Estos resultados indican que algunas recuperaciones muy grandes ocurrieron cuando el tráfico de recuperación general estaba en su máximo.

- c. Para ver más detalles, utilice el ["herramienta de auditoría y explicación"](#) 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` tenga muchas líneas, agregue el `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 depósitos son más lentas que las operaciones SPUT en objetos:

- a. Comience usando el `-go` opción, que agrupa los mensajes para operaciones de objetos y depósitos por separado:

```
grep SPUT sample.log | audit-sum -go
```

message group average(sec)	count	min(sec)	max(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 contenedores tienen características de rendimiento diferentes a las de las operaciones SPUT para objetos.

- b. Para determinar qué buckets tienen las operaciones SPUT más lentas, utilice el `-gb` opción, que agrupa los mensajes por contenedor:

```
grep SPUT audit.log | audit-sum -gb
```

message group average(sec)	count	min(sec)	max(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.ltd002	1564563	0.011	51.569
0.361			

- c. Para determinar qué depósitos tienen el tamaño de objeto SPUT más grande, utilice ambos `-gb` y el `-s` opciones:

```
grep SPUT audit.log | audit-sum -gb -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
=====			
SPUT.cho-non-versioning 21.672	71943	2.097	5000.000
SPUT.cho-versioning 21.120	54277	2.097	5000.000
SPUT.cho-west-region 14.433	80615	2.097	800.000
SPUT.ltd002 0.352	1564563	0.000	999.972

Formato del mensaje de auditoría

Formato del 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 informa.

Si la información resumida proporcionada por el ["auditoría-explicación"](#) y ["suma de auditoría"](#) Si las herramientas son insuficientes, consulte esta sección para comprender el formato general de todos los mensajes de auditoría.

El siguiente es un ejemplo de mensaje de auditoría tal como podría 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(FC32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):9445736326500603516]]
```

Cada mensaje de auditoría contiene una cadena de elementos de atributos. La cadena completa está entre corchetes.([]), y cada elemento de atributo en la cadena tiene las siguientes características:

- Entre paréntesis []
- Introducido por la cadena AUDT , lo que indica un mensaje de auditoría
- Sin delimitadores (sin comas ni espacios) antes ni después
- Terminado por un carácter de avance de línea \n

Cada elemento incluye un código de atributo, un tipo de dato y un valor que se informan en este formato:

```
[ATTR(type):value] [ATTR(type):value] ...  
[ATTR(type):value]\n
```

La cantidad de elementos de atributo en el mensaje depende del tipo de evento del mensaje. Los elementos de atributo no se enumeran en ningún orden particular.

La siguiente lista describe los elementos de 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 otros que son específicos del evento.
- `type` es un identificador de cuatro caracteres del tipo de datos de programación del valor, como `UI64`, `FC32`, etc. El tipo está entre paréntesis. `( )`.
- `value` es el contenido del atributo, normalmente un valor numérico o de texto. Los valores siempre siguen a dos puntos (`:`). Los valores del tipo de datos `CSTR` están rodeados por comillas dobles `" "`.

Tipos de datos

Se utilizan diferentes tipos de datos para almacenar información en los mensajes de auditoría.

Tipo	Descripción
UI32	Entero largo sin signo (32 bits); puede almacenar los números del 0 al 4.294.967.295.
UI64	Entero doble largo sin signo (64 bits); puede almacenar los números del 0 al 18.446.744.073.709.551.615.
FC32	Constante de cuatro caracteres; un valor entero sin signo de 32 bits representado como cuatro caracteres ASCII como "ABCD".
iPad	Se utiliza para direcciones IP.
CSTR	Una matriz de longitud variable de caracteres UTF-8. Los caracteres se pueden escapar con las siguientes convenciones: • La barra invertida es <code>\\</code>. • El retorno de carro es <code>\r</code>. • Las comillas dobles son <code>\"</code>. • El salto de línea (nueva línea) es <code>\n</code>. • Los caracteres se pueden reemplazar por sus equivalentes hexadecimales (en el formato <code>\xHH</code>, donde <code>HH</code> es el valor hexadecimal que representa el carácter).

Datos específicos del evento

Cada mensaje de auditoría en el registro de auditoría registra datos específicos de un evento del sistema.

Tras la inauguración [AUDT: contenedor que identifica el mensaje en sí, el siguiente conjunto de atributos proporciona información sobre el evento o la acción descrita por el mensaje de auditoría. Estos atributos se resaltan en el siguiente ejemplo:

```
2018-12-05T08:24:45.921845 [AUDT:*[RSLT\FC32\):SUCS\]*
\[TIEMPO\UI64\):11454\]\[SAIP\IPAD\):"10.224.0.100"\]\[S3AI\CSTR\):"60025621595611246499"\]
\[SACC\CSTR\):"cuenta"\]\[S3AK\CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsK
JA=="\]\[SUSR\CSTR\):"urn:sgws:identity::60025621595611246499:root"\]
\[SBAI\CSTR\):"60025621595611246499"\]\[SBAC\CSTR\):"cuenta"\]\[S3BK\CSTR\):"depósito"\]
\[S3KY\CSTR\):"objeto"\]\[CBID\UI64\):0xCC128B9B9E428347\]\[UUID\CSTR\):"B975D2CE-E4DA-
4D14-8A23-1CB4B83F2CD8"\]\[CSIZ\UI64\):30720\]\[AVER\UI32\):10]
\[ATIM\UI64\):1543998285921845\]\[ATYP\FC32\):SHEA\]\[ANID\UI32\):12281045\]\[AMID\FC32\):S3RQ]
\[ATID\UI64\):15552417629170647261]]
```

El ATYP El elemento (subrayado en el ejemplo) identifica qué evento generó el mensaje. Este mensaje de ejemplo incluye el "KARITÉ" código de mensaje ([ATYP(FC32):SHEA]), que indica que fue generado por una solicitud S3 HEAD exitosa.

Elementos comunes en los mensajes de auditoría

Todos los mensajes de auditoría contienen los elementos comunes.

Código	Tipo	Descripción
EN MEDIO DE	FC32	ID del módulo: un identificador de cuatro caracteres del ID del módulo que generó el mensaje. Esto indica el segmento de código dentro del cual se generó el mensaje de auditoría.
ANID	UI32	ID de nodo: el ID del nodo de la red 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 . Esta identificación no se puede cambiar.
ASES	UI64	Identificador de sesión de auditoría: en versiones anteriores, este elemento indicaba el momento en el que se inicializaba el sistema de auditoría después de iniciarse el servicio. Este valor de tiempo se midió en microsegundos desde la época del sistema operativo (00:00:00 UTC del 1 de enero de 1970). Nota: Este elemento está obsoleto y ya no aparece en los mensajes de auditoría.

Código	Tipo	Descripción
ASQN	UI64	Recuento de secuencia: en versiones anteriores, este contador se incrementaba para cada mensaje de auditoría generado en el nodo de la red (ANID) y se restablecía a cero al reiniciar el servicio. Nota: Este elemento está obsoleto y ya no aparece en los mensajes de auditoría.
ATID	UI64	ID de seguimiento: un identificador que comparte el conjunto de mensajes que se activaron mediante un solo evento.
ATIM	UI64	Marca de tiempo: la hora en que se generó el evento que activó el mensaje de auditoría, medido en microsegundos desde la época del sistema operativo (00:00:00 UTC del 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 locales se basan en milisegundos. Podría ser necesario redondear o truncar la marca de tiempo registrada. La hora legible por humanos que aparece al comienzo del mensaje de auditoría en el <code>audit.log</code> El archivo es el atributo ATIM en formato ISO 8601. La fecha y la hora se representan como <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code>, donde el T es un carácter de cadena literal que indica el comienzo del segmento de tiempo de la fecha. <code>UUUUUU</code> son microsegundos.
ATYP	FC32	Tipo de evento: un identificador de cuatro caracteres del evento que se está registrando. Esto regula el contenido de "carga útil" del mensaje: los atributos que se incluyen.
AFIRMAR	UI32	Versión: La 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 auditoría. Este campo permite la compatibilidad con versiones anteriores del servicio AMS para procesar mensajes de versiones anteriores de los servicios.
RSLT	FC32	Resultado: El resultado de un evento, proceso o transacción. Si no es relevante para un mensaje, se utiliza NONE 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 utilizan el mismo formato.

El siguiente es un ejemplo de mensaje de auditoría tal como podría aparecer en el `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):"s3small11"] [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 registrando, así como información sobre el mensaje de auditoría en sí.

Para identificar qué evento registra el mensaje de auditoría, busque el atributo ATYP (resaltado a continuación):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK(CSTR):"s3small11"] [S3K
Y(CSTR):"hello1"] [CBID(UI64):0x50C4F7AC2BC8EDF7] [CSIZ(UI64):0
] [AVER(UI32):10] [ATIM(UI64):1405631878959669] [ATYP(FC32):SP
UT] [ANID(UI32):12872812] [AMID(FC32):S3RQ] [ATID(UI64):1579224
144102530435]]
```

El valor del atributo ATYP es SPUT. "ESPOLVO" representa una transacción S3 PUT, que registra la ingesta de un objeto en un depósito.

El siguiente mensaje de auditoría también muestra el depósito al que está asociado el objeto:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK\ (CSTR\):"s3small11"] [S3
KY(CSTR):"hello1"] [CBID(UI64):0x50C4F7AC2BC8EDF7] [CSIZ(UI64):
0] [AVER(UI32):10] [ATIM(UI64):1405631878959669] [ATYP(FC32):SPU
T] [ANID(UI32):12872812] [AMID(FC32):S3RQ] [ATID(UI64):157922414
4102530435]]
```

Para descubrir cuándo ocurrió el evento PUT, observe la marca de tiempo del Tiempo Universal Coordinado (UTC) al comienzo del mensaje de auditoría. Este valor es una versión legible para humanos del atributo ATIM del mensaje de auditoría en sí:

2014-07-17T21:17:58.959669

```
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK(CSTR):"s3small11"] [S3KY(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):1579224144102530435]]
```

ATIM registra el tiempo, en microsegundos, desde el comienzo de la época UNIX. En el ejemplo, el valor 1405631878959669 se traduce al jueves, 17 de julio de 2014 21:17:59 UTC.

Mensajes de auditoría y el ciclo de vida de los objetos

¿Cuándo se generan los mensajes de auditoría?

Los mensajes de auditoría se generan cada vez que se ingiere, recupera o elimina un objeto. Puede identificar estas transacciones en el registro de auditoría ubicando los mensajes de auditoría específicos de la API de S3.

Los mensajes de auditoría están vinculados a través de identificadores específicos de cada protocolo.

Protocolo	Código
Vinculación de operaciones S3	S3BK (cubo), S3KY (llave) o ambos
Vinculación de operaciones Swift	WCON (contenedor), WOBJ (objeto) o ambos
Vinculación de operaciones internas	CBID (identificador interno del objeto)

Momento de los mensajes de auditoría

Debido a factores como las diferencias de tiempo entre los nodos de la red, el tamaño de los objetos y los retrasos de la red, el orden de los mensajes de auditoría generados por los diferentes servicios puede variar del que se muestra en los ejemplos de esta sección.

Transacciones de ingesta de objetos

Puede identificar las transacciones de ingesta del cliente en el registro de auditoría ubicando los mensajes de auditoría específicos de la API de S3.

No todos los mensajes de auditoría generados durante una transacción de ingesta se enumeran en las siguientes tablas. Solo se incluyen los mensajes necesarios para rastrear la transacción de ingesta.

Mensajes de auditoría de ingesta de S3

Código	Nombre	Descripción	Rastro	Ver
ESPOLVO	Transacción PUT S3	Se ha completado exitosamente una transacción de ingesta S3 PUT.	CBID, S3BK, S3KY	"SPUT: S3 PONER"
ORLM	Reglas de objeto cumplidas	La política de ILM se ha cumplido para este objeto.	CBD	"ORLM: Se cumplen las reglas de objeto"

Mensajes de auditoría de ingesta de Swift

Código	Nombre	Descripción	Rastro	Ver
WPUT	Transacción PUT rápida	Se ha completado exitosamente una transacción de ingesta Swift PUT.	CBID, WCON, WOBJ	"WPUT: PUT rápido"
ORLM	Reglas de objeto cumplidas	La política de ILM se ha cumplido para este objeto.	CBD	"ORLM: Se cumplen las reglas de objeto"

Ejemplo: ingesta de objetos S3

La serie de mensajes de auditoría a continuación es un ejemplo de los mensajes de auditoría generados y guardados en el registro de auditoría cuando un cliente S3 ingiere un objeto en un nodo de almacenamiento (servicio LDR).

En este ejemplo, la política ILM activa incluye la regla ILM Hacer 2 copias.



No todos los mensajes de auditoría generados durante una transacción se enumeran en el siguiente ejemplo. Solo se enumeran aquellos relacionados con la transacción de ingesta S3 (SPUT).

Este ejemplo supone que previamente se ha creado un bucket S3.

SPUT: S3 PONER

El mensaje SPUT se genera para indicar que se ha emitido una transacción S3 PUT para crear un objeto en un depósito 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 se ha cumplido la política ILM para 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 del nodo LDR y el ID del volumen de las ubicaciones de los 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 con codificación de borrado, el campo LOCS incluye el ID del perfil de codificación de borrado y el ID del grupo de codificación 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 de clave y depósito S3 o información de objeto y contenedor Swift, según qué API se utilizó.

```
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]]
```

Transacciones de eliminación de objetos

Puede identificar transacciones de eliminación de objetos en el registro de auditoría ubicando los mensajes de auditoría específicos de la API de S3.

No todos los mensajes de auditoría generados durante una transacción de eliminación aparecen en las siguientes tablas. Sólo se incluyen los mensajes necesarios para rastrear la transacción de eliminación.

Mensajes de auditoría de eliminación de S3

Código	Nombre	Descripción	Rastro	Ver
SDEL	S3 Eliminar	Solicitud realizada para eliminar el objeto de un depósito.	CBD, S3KY	"SDEL: S3 ELIMINAR"

Eliminar mensajes de auditoría de Swift

Código	Nombre	Descripción	Rastro	Ver
WDEL	Eliminación rápida	Solicitud realizada para eliminar el objeto de un contenedor, o el contenedor.	CBDI, WOBJ	"WDEL: Eliminación rápida"

Ejemplo: eliminación de objetos 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.



No todos los mensajes de auditoría generados durante una transacción de eliminación se enumeran en el siguiente ejemplo. Solo se enumeran aquellos relacionados con la transacción de eliminación S3 (SDEL).

SDEL: S3 Eliminar

La eliminación de objetos comienza cuando el cliente envía una solicitud DeleteObject a un servicio LDR. El mensaje contiene el depósito desde el cual eliminar el objeto y la clave S3 del objeto, que se utiliza para identificarlo.

```
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):"SGKHya1RU_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]]
```

Transacciones de recuperación de objetos

Puede identificar transacciones de recuperación de objetos en el registro de auditoría ubicando mensajes de auditoría específicos de la API de S3.

No todos los mensajes de auditoría generados durante una transacción de recuperación se enumeran en las siguientes tablas. Sólo se incluyen los mensajes necesarios para rastrear la transacción recuperada.

Mensajes de auditoría de recuperación de S3

Código	Nombre	Descripción	Rastro	Ver
SGET	S3 GET	Solicitud realizada para recuperar un objeto de un depósito.	CBID, S3BK, S3KY	"SGET: S3 OBTENER"

Mensajes de auditoría de recuperación rápida

Código	Nombre	Descripción	Rastro	Ver
WGET	Obtener rápidamente	Solicitud realizada para recuperar un objeto de un contenedor.	CBID, WCON, WOBJ	"WGET: Obtención rápida"

Ejemplo: recuperación de objetos 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 aparecen en el siguiente ejemplo. Sólo se enumeran aquellos relacionados con la transacción de recuperación S3 (SGET).

SGET: S3 OBTENER

La recuperación de objetos comienza cuando el cliente envía una solicitud `GetObject` a un servicio LDR. El mensaje contiene el depósito desde el cual recuperar el objeto y la clave S3 del objeto, que se utiliza para identificarlo.

```

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 política del depósito lo permite, un cliente puede recuperar objetos de forma anónima o puede recuperar objetos de un depósito que sea propiedad de una cuenta de inquilino diferente. El mensaje de auditoría contiene información sobre la cuenta de inquilino del propietario del depósito para que pueda realizar un seguimiento de estas solicitudes anónimas y entre cuentas.

En el siguiente mensaje de ejemplo, el cliente envía una solicitud GetObject para un objeto almacenado en un depósito que no es de su propiedad. Los valores para SBAI y SBAC registran el ID y el nombre de la cuenta de inquilino del propietario del depósito, que difieren del ID y el nombre de la cuenta de inquilino del cliente registrados 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):SGE
T][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]

```

Ejemplo: S3 Seleccionar un objeto

Cuando un cliente S3 emite una consulta S3 Select sobre 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 aparecen en el siguiente ejemplo. Solo se enumeran aquellos relacionados con la transacción S3 Select (SelectObjectContent).

Cada consulta genera dos mensajes de auditoría: uno que realiza la autorización de la solicitud S3 Select (el campo S3SR está configurado como "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][SAIP(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(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][SAIP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-for\":\"unix:\"}"]][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(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):10185581][MTME(UI64):1636380348695262][AVER(UI32):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][AMID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Mensajes de actualización de metadatos

Los mensajes de auditoría se generan cuando un cliente S3 actualiza los metadatos de un objeto.

Mensajes de auditoría de actualización de metadatos de S3

Código	Nombre	Descripción	Rastro	Ver
SUPD	Metadatos S3 actualizados	Se genera cuando un cliente S3 actualiza los metadatos de un objeto ingerido.	CBID, S3KY, HTRH	"SUPD: Metadatos S3 actualizados"

Ejemplo: actualización de metadatos de S3

El ejemplo muestra una transacción exitosa para actualizar los metadatos de un objeto S3 existente.

SUPD: Actualización de metadatos S3

El cliente S3 realiza una solicitud (SUPD) para actualizar los metadatos especificados (`x-amz-meta-\*`) para el objeto S3 (S3KY). En este ejemplo, los encabezados de solicitud se incluyen en el campo HTRH porque se ha configurado como un encabezado de protocolo de auditoría (**CONFIGURACIÓN > Monitoreo > Servidor de auditoría y syslog**). Ver ["Configurar mensajes de auditoría y destinos de registro"](#).

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\": \"identity\", \"authorization\": \"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\": \"0\", \"date\": \"Tue, 11 Jul 2017 21:54:03
GMT\", \"host\": \"10.96.99.163:18082\",
\"user-agent\": \"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\": \"/testbkt1/testobj1\", \"x-amz-metadata-
directive\": \"REPLACE\", \"x-amz-meta-city\": \"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Mensajes de auditoría

Descripciones de los mensajes de auditoría

En las siguientes secciones 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 según la clase de actividad que representa el mensaje. Estas agrupaciones son útiles tanto para comprender los tipos de actividades que se auditan como para seleccionar el tipo de filtrado de mensajes de auditoría deseado.

Los mensajes de auditoría también se enumeran en orden alfabético por sus códigos de cuatro caracteres. Esta lista alfabética le permite encontrar información sobre mensajes específicos.

Los códigos de cuatro caracteres utilizados en este capítulo son los valores ATYP que se encuentran en los mensajes de auditoría, como se muestra en el siguiente mensaje de ejemplo:

```
2014-07-17T03:50:47.484627
```

```
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

Para obtener información sobre cómo configurar los niveles de mensajes de auditoría, cambiar los destinos de los registros y usar un servidor syslog externo para su información de auditoría, consulte ["Configurar mensajes de auditoría y destinos de registro"](#)

Categorías de mensajes de auditoría

Mensajes de auditoría del sistema

Los mensajes de auditoría que pertenecen a la categoría de auditoría del sistema se utilizan para eventos relacionados con el sistema de auditoría en sí, estados de los nodos de la red, actividad de tareas de todo el sistema (tareas de la red) y operaciones de respaldo de servicio.

Código	Título y descripción del mensaje	Ver
ECMC	Fragmento de datos codificado por borrado faltante: indica que se ha detectado un fragmento de datos codificado por borrado faltante.	"ECMC: Fragmento de datos con código de borrado faltante"
ECOC	Fragmento de datos codificado por borrado corrupto: indica que se ha detectado un fragmento de datos codificado por borrado corrupto.	"ECOC: Fragmento de datos corruptos codificados por borrado"
ETAF	Error de autenticación de seguridad: falló un intento de conexión mediante Seguridad de la capa de transporte (TLS).	"ETAF: Falló la autenticación de seguridad"
GNRG	Registro GNDS: Un servicio actualiza o registra información sobre sí mismo en el sistema StorageGRID .	"GNRG: Registro GNDS"
GNUR	Anulación del registro de GNDS: un servicio se ha anulado su registro en el sistema StorageGRID .	"GNUR: Anulación del registro de GNDS"
GTED	Tarea de cuadrícula finalizada: el servicio CMN terminó de procesar la tarea de cuadrícula.	"GTED: Tarea de cuadrícula finalizada"
GTST	Tarea de cuadrícula iniciada: el servicio CMN comenzó a procesar la tarea de cuadrícula.	"GTST: Tarea de cuadrícula iniciada"
GTSU	Tarea de cuadrícula enviada: se envió una tarea de cuadrícula al servicio CMN.	"GTSU: Tarea de cuadrícula enviada"

Código	Título y descripción del mensaje	Ver
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"
Tristeza	Deshabilitar auditoría de seguridad: se desactivó el registro de mensajes de auditoría.	"SADD: Desactivación de auditoría de seguridad"
SADE	Habilitar auditoría de seguridad: se ha restaurado el registro de mensajes de auditoría.	"SADE: Habilitación de auditoría de seguridad"
SVRF	Error de verificación del almacén de objetos: un bloque de contenido no pasó las verificaciones de verificación.	"SVRF: Error en la verificación del almacén de objetos"
Unidad de Registro de Víctimas de Violencia Doméstica	Verificación de almacén de objetos desconocido: se detectaron datos de objetos inesperados en el almacén de objetos.	"SVRU: Verificación de almacén de objetos desconocida"
Distrito Escolar Unificado de Syracuse	Parada de nodo: se solicitó un apagado.	"SYSD: Parada de nodo"
SISTEMA	Detención de nodo: un servicio inició una detención elegante.	"SYST: Nodo deteniéndose"
SYSU	Inicio de nodo: se inició un servicio; la naturaleza del apagado anterior se indica en el mensaje.	"SYSU: Inicio del nodo"

Mensajes de auditoría de almacenamiento de objetos

Los mensajes de auditoría que pertenecen a la categoría de auditoría de almacenamiento de objetos se utilizan para eventos relacionados con el almacenamiento y la administración de objetos dentro del sistema StorageGRID . Estos incluyen almacenamiento y recuperación de objetos, transferencias de nodo de red a nodo de red y verificaciones.



Los códigos de auditoría se eliminan del producto y de la documentación a medida que las funciones quedan obsoletas. Si encuentra un código de auditoría que no aparece aquí, consulte las versiones anteriores de este tema para ver versiones anteriores de SG. Por ejemplo, ["Mensajes de auditoría de almacenamiento de objetos de StorageGRID 11.8"](#) .

Código	Descripción	Ver
HERMANO	Solicitud de solo lectura de depósito: un depósito ingresó o salió del modo de solo lectura.	"BROR: Solicitud de solo lectura de depósito"

Código	Descripción	Ver
CBSE	Fin de envío de objeto: la entidad de origen completó una operación de transferencia de datos de un nodo de la red a otro nodo de la red.	"CBSE: Fin de envío de objetos"
CBRE	Fin de recepción del objeto: la entidad de destino completó una operación de transferencia de datos de un nodo de la red a otro nodo de la red.	"CBRE: Extremo de recepción de objetos"
CGRR	Solicitud de replicación entre redes: StorageGRID intentó una operación de replicación entre redes para replicar objetos entre depósitos en una conexión de federación de redes.	"CGRR: Solicitud de replicación entre redes"
EBDL	Eliminar depósito vacío: el escáner ILM eliminó un objeto en un depósito que está eliminando todos los objetos (realizando una operación de depósito vacío).	"EBDL: Eliminar depósito vacío"
EBKR	Solicitud de depósito vacío: un usuario envió una solicitud para activar o desactivar el depósito vacío (es decir, para eliminar objetos del depósito o para dejar de eliminar objetos).	"EBKR: Solicitud de cubo vacío"
SCMT	Confirmación de almacén de objetos: se almacenó y verificó completamente un bloque de contenido y ahora se puede solicitar.	"SCMT: Solicitud de confirmación del almacén de objetos"
SREM	Eliminar almacén de objetos: se eliminó un bloque de contenido de un nodo de la cuadrícula y ya no se puede solicitar directamente.	"SREM: Eliminar almacén de objetos"

El cliente lee mensajes de auditoría

Los mensajes de auditoría de lectura del cliente se registran cuando una aplicación cliente S3 realiza una solicitud para recuperar un objeto.

Código	Descripción	Utilizado por	Ver
S3SL	Solicitud de selección S3: registra una finalización después de que se haya devuelto una solicitud de selección S3 al cliente. El mensaje S3SL puede incluir detalles del mensaje de error y del código de error. Es posible que la solicitud no haya tenido éxito.	Cliente S3	"S3SL: Solicitud de selección de S3"

Código	Descripción	Utilizado por	Ver
SGET	S3 GET: registra una transacción exitosa para recuperar un objeto o enumerar los objetos en un depósito. Nota: Si la transacción opera en un subrecurso, el mensaje de auditoría incluirá el campo S3SR.	Cliente S3	"SGET: S3 OBTENER"
KARITÉ	S3 HEAD: Registra una transacción exitosa para verificar la existencia de un objeto o depósito.	Cliente S3	"SHEA: CABEZA T3"
WGET	Swift GET: registra una transacción exitosa para recuperar un objeto o enumerar los objetos en un contenedor.	Cliente Swift	"WGET: Obtención rápida"
TRIGO	Swift HEAD: registra una transacción exitosa para verificar la existencia de un objeto o contenedor.	Cliente Swift	"WHEA: CABEZA Veloz"

El cliente escribe mensajes de auditoría

Los mensajes de auditoría de escritura del cliente se registran cuando una aplicación cliente S3 realiza una solicitud para crear o modificar un objeto.

Código	Descripción	Utilizado por	Ver
OVWR	Sobrescritura de objeto: registra una transacción para sobrescribir un objeto con otro objeto.	Cientes S3 y Swift	"OVWR: Sobrescritura de objetos"
SDEL	S3 ELIMINAR: registra una transacción exitosa para eliminar un objeto o depósito. Nota: Si la transacción opera en un subrecurso, el mensaje de auditoría incluirá el campo S3SR.	Cliente S3	"SDEL: S3 ELIMINAR"
SPOS	S3 POST: registra una transacción exitosa para restaurar un objeto del almacenamiento de AWS Glacier a un grupo de almacenamiento en la nube.	Cliente S3	"SPOS: PUBLICACIÓN S3"
ESPOLVO	S3 PUT: Registra una transacción exitosa para crear un nuevo objeto o depósito. Nota: Si la transacción opera en un subrecurso, el mensaje de auditoría incluirá el campo S3SR.	Cliente S3	"SPUT: S3 PONER"
SUPD	Metadatos S3 actualizados: registra una transacción exitosa para actualizar los metadatos de un objeto o depósito existente.	Cliente S3	"SUPD: Metadatos S3 actualizados"

Código	Descripción	Utilizado por	Ver
WDEL	Swift DELETE: registra una transacción exitosa para eliminar un objeto o contenedor.	Cliente Swift	"WDEL: Eliminación rápida"
WPUT	Swift PUT: registra una transacción exitosa para crear un nuevo objeto o contenedor.	Cliente Swift	"WPUT: PUT rápido"

Mensaje de auditoría de gestión

La categoría Administración registra las solicitudes de los usuarios a la API de Administración.

Código	Título y descripción del mensaje	Ver
Universidad Estatal de Michigan	Mensaje de auditoría de la API de administración: un registro de solicitudes de usuario.	"MGAU: Mensaje de auditoría de gestión"

Mensajes de auditoría de ILM

Los mensajes de auditoría que pertenecen a la categoría de auditoría ILM se utilizan para eventos relacionados con las operaciones de gestión del ciclo de vida de la información (ILM).

Código	Título y descripción del mensaje	Ver
IDEL	Eliminación iniciada por ILM: este mensaje de auditoría se genera cuando ILM inicia el proceso de eliminación de un objeto.	"IDEL: Eliminación iniciada por ILM"
LKCU	Limpieza de objetos sobrescritos. Este mensaje de auditoría se genera cuando un objeto sobrescrito se elimina automáticamente para liberar espacio de almacenamiento.	"LKCU: Limpieza de objetos sobrescritos"
ORLM	Reglas de objeto cumplidas: este mensaje de auditoría se genera cuando los datos del objeto se almacenan según lo especificado por las reglas de ILM.	"ORLM: Se cumplen las reglas de objeto"

Referencia del mensaje de auditoría

BROR: Solicitud de solo lectura de depósito

El servicio LDR genera este mensaje de auditoría cuando un depósito entra o sale del modo de solo lectura. Por ejemplo, un depósito entra en modo de solo lectura mientras se eliminan todos los objetos.

Código	Campo	Descripción
BKHD	UUID del depósito	El identificador del depósito.
Brov	Valor de solicitud de solo lectura del depósito	Si el depósito se está convirtiendo en de solo lectura o está abandonando el estado de solo lectura (1 = solo lectura, 0 = no de solo lectura).
Hermanos	Razón de solo lectura del bucket	El motivo por el cual el depósito se convierte en de solo lectura o abandona ese estado. Por ejemplo, emptyBucket.
S3AI	ID de cuenta de inquilino de S3	El ID de la cuenta del inquilino que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.

CBRB: Inicio de recepción de objetos

Durante las operaciones normales del sistema, los bloques de contenido se transfieren continuamente 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.

Código	Campo	Descripción
CNID	Identificador de conexión	El identificador único de la sesión/conexión de nodo a nodo.
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido que se está transfiriendo.
CTDR	Dirección de transferencia	Indica si la transferencia de CBID se inició mediante inserción o extracción: PUSH: La operación de transferencia fue solicitada por la entidad remitente. PULL: La operación de transferencia fue solicitada por la entidad receptora.
CTSR	Entidad de origen	El ID del nodo de la fuente (remitente) de la transferencia CBID.
CTDS	Entidad de destino	El ID del nodo del destino (receptor) de la transferencia CBID.

Código	Campo	Descripción
CTSS	Iniciar recuento de secuencias	Indica el primer recuento de secuencia solicitado. Si tiene éxito, la transferencia comienza a partir de este recuento de secuencia.
CTES	Recuento esperado de secuencia final	Indica el último recuento de secuencia solicitado. Si es exitosa, la transferencia se considera completa cuando se haya recibido este recuento de secuencia.
RSLT	Estado de inicio de la transferencia	Estado en el momento en que se inició la transferencia: SUCS: Transferencia iniciada exitosamente.

Este mensaje de auditoría significa que se inició una operación de transferencia de datos de nodo a nodo en una sola pieza de contenido, según lo identificado por su Identificador de bloque de contenido. La operación solicita datos desde "Recuento de secuencia inicial" hasta "Recuento de secuencia final esperado". Los nodos de envío y recepción se identifican mediante sus ID de nodo. Esta información se puede utilizar para rastrear el flujo de datos del sistema y, cuando se combina con mensajes de auditoría de almacenamiento, para verificar los recuentos de réplicas.

CBRE: Extremo de recepción de objetos

Cuando se completa la transferencia de un bloque de contenido de un nodo a otro, la entidad de destino emite este mensaje.

Código	Campo	Descripción
CNID	Identificador de conexión	El identificador único de la sesión/conexión de nodo a nodo.
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido que se está transfiriendo.
CTDR	Dirección de transferencia	Indica si la transferencia de CBID se inició mediante inserción o extracción: PUSH: La operación de transferencia fue solicitada por la entidad remitente. PULL: La operación de transferencia fue solicitada por la entidad receptora.
CTSR	Entidad de origen	El ID del nodo de la fuente (remitente) de la transferencia CBID.
CTDS	Entidad de destino	El ID del nodo del destino (receptor) de la transferencia CBID.

Código	Campo	Descripción
CTSS	Iniciar recuento de secuencias	Indica el recuento de secuencia en el que se inició la transferencia.
CTAS	Recuento de secuencia final real	Indica el último recuento de secuencia transferido exitosamente. Si el recuento de secuencia final real es el mismo que el recuento de secuencia inicial y el resultado de la transferencia no fue exitoso, no se intercambiaron datos.
RSLT	Resultado de la transferencia	El resultado de la operación de transferencia (desde la perspectiva de la entidad remitente): SUCS: transferencia completada exitosamente; se enviaron todos los recuentos de secuencia solicitados. CONL: conexión perdida durante la transferencia CTMO: tiempo de conexión agotado durante el establecimiento o la transferencia UNRE: ID de nodo de destino inalcanzable CRPT: transferencia finalizada debido a la recepción de datos corruptos o inválidos

Este mensaje de auditoría significa que se completó una operación de transferencia de datos de nodo a nodo. Si el resultado de la transferencia fue exitoso, la operación transfirió datos de "Recuento de secuencia inicial" a "Recuento de secuencia final real". Los nodos de envío y recepción se identifican mediante sus ID de nodo. Esta información se puede utilizar para rastrear el flujo de datos del sistema y para localizar, tabular y analizar errores. Cuando se combina con mensajes de auditoría de almacenamiento, también se puede utilizar para verificar los recuentos de réplicas.

CBSB: Inicio de envío de objetos

Durante las operaciones normales del sistema, los bloques de contenido se transfieren continuamente 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.

Código	Campo	Descripción
CNID	Identificador de conexión	El identificador único de la sesión/conexión de nodo a nodo.
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido que se está transfiriendo.

Código	Campo	Descripción
CTDR	Dirección de transferencia	Indica si la transferencia de CBID se inició mediante inserción o extracción: PUSH: La operación de transferencia fue solicitada por la entidad remitente. PULL: La operación de transferencia fue solicitada por la entidad receptora.
CTSR	Entidad de origen	El ID del nodo de la fuente (remitente) de la transferencia CBID.
CTDS	Entidad de destino	El ID del nodo del destino (receptor) de la transferencia CBID.
CTSS	Iniciar recuento de secuencias	Indica el primer recuento de secuencia solicitado. Si tiene éxito, la transferencia comienza a partir de este recuento de secuencia.
CTES	Recuento esperado de secuencia final	Indica el último recuento de secuencia solicitado. Si es exitosa, la transferencia se considera completa cuando se haya recibido este recuento de secuencia.
RSLT	Estado de inicio de la transferencia	Estado en el momento en que se inició la transferencia: SUCS: transferencia iniciada exitosamente.

Este mensaje de auditoría significa que se inició una operación de transferencia de datos de nodo a nodo en una sola pieza de contenido, según lo identificado por su Identificador de bloque de contenido. La operación solicita datos desde "Recuento de secuencia inicial" hasta "Recuento de secuencia final esperado". Los nodos de envío y recepción se identifican mediante sus ID de nodo. Esta información se puede utilizar para rastrear el flujo de datos del sistema y, cuando se combina con mensajes de auditoría de almacenamiento, para verificar los recuentos de réplicas.

CBSE: Fin de envío de objetos

Cuando se completa la transferencia de un bloque de contenido de un nodo a otro, la entidad de origen emite este mensaje.

Código	Campo	Descripción
CNID	Identificador de conexión	El identificador único de la sesión/conexión de nodo a nodo.
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido que se está transfiriendo.

Código	Campo	Descripción
CTDR	Dirección de transferencia	Indica si la transferencia de CBID se inició mediante inserción o extracción: PUSH: La operación de transferencia fue solicitada por la entidad remitente. PULL: La operación de transferencia fue solicitada por la entidad receptora.
CTSR	Entidad de origen	El ID del nodo de la fuente (remitente) de la transferencia CBID.
CTDS	Entidad de destino	El ID del nodo del destino (receptor) de la transferencia CBID.
CTSS	Iniciar recuento de secuencias	Indica el recuento de secuencia en el que se inició la transferencia.
CTAS	Recuento de secuencia final real	Indica el último recuento de secuencia transferido exitosamente. Si el recuento de secuencia final real es el mismo que el recuento de secuencia inicial y el resultado de la transferencia no fue exitoso, no se intercambiaron datos.
RSLT	Resultado de la transferencia	El resultado de la operación de transferencia (desde la perspectiva de la entidad remitente): SUCS: Transferencia completada exitosamente; se enviaron todos los recuentos de secuencia solicitados. CONL: conexión perdida durante la transferencia CTMO: tiempo de conexión agotado durante el establecimiento o la transferencia UNRE: ID de nodo de destino inalcanzable CRPT: transferencia finalizada debido a la recepción de datos corruptos o inválidos

Este mensaje de auditoría significa que se completó una operación de transferencia de datos de nodo a nodo. Si el resultado de la transferencia fue exitoso, la operación transfirió datos de "Recuento de secuencia inicial" a "Recuento de secuencia final real". Los nodos de envío y recepción se identifican mediante sus ID de nodo. Esta información se puede utilizar para rastrear el flujo de datos del sistema y para localizar, tabular y analizar errores. Cuando se combina con mensajes de auditoría de almacenamiento, también se puede utilizar para verificar los recuentos de réplicas.

CGRR: Solicitud de replicación entre redes

Este mensaje se genera cuando StorageGRID intenta una operación de replicación entre redes para replicar objetos entre depósitos en una conexión de federación de redes.

Código	Campo	Descripción
CSIZ	Tamaño del objeto	El tamaño del objeto en bytes. El atributo CSIZ se introdujo en StorageGRID 11.8. Como resultado, las solicitudes de replicación entre redes que abarcan una actualización de StorageGRID 11.7 a 11.8 podrían tener un tamaño de objeto total inexacto.
S3AI	ID de cuenta de inquilino de S3	El ID de la cuenta de inquilino que posee el depósito desde el que se está replicando el objeto.
GFID	ID de conexión de la federación de red	El ID de la conexión de federación de red que se utiliza para la replicación entre redes.
ÓPERA	Operación de la CGR	El tipo de operación de replicación entre redes que se intentó: • 0 = Replicar objeto • 1 = Replicar objeto multiparte • 2 = Replicar marcador de eliminación
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito.
VSID	ID de versión	El ID de la versión de la versión específica de un objeto que se estaba replicando.
RSLT	Código de resultado	Devuelve un resultado exitoso (SUCS) o un error general (GERR).

EBDL: Eliminar depósito vacío

El escáner ILM eliminó un objeto en un depósito que está eliminando todos los objetos (realizando una operación de depósito vacío).

Código	Campo	Descripción
CSIZ	Tamaño del objeto	El tamaño del objeto en bytes.
CAMINO	Cubo/clave S3	El nombre del depósito S3 y el nombre de la clave S3.
SEGC	UUID del contenedor	UUID del contenedor del objeto segmentado. Este valor solo está disponible si el objeto está segmentado.

Código	Campo	Descripción
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
RSLT	Resultado de la operación de eliminación	El resultado de un evento, proceso o transacción. Si no es relevante para un mensaje, se utiliza NONE en lugar de SUCS para que el mensaje no se filtre accidentalmente.

EBKR: Solicitud de cubo vacío

Este mensaje indica que un usuario envió una solicitud para activar o desactivar el depósito vacío (es decir, para eliminar objetos del depósito o para dejar de eliminar objetos).

Código	Campo	Descripción
CONSTRUIR	UUID del depósito	El identificador del depósito.
EBJS	Configuración JSON de depósito vacío	Contiene el JSON que representa la configuración actual del depósito vacío.
S3AI	ID de cuenta de inquilino de S3	El ID de la cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.

ECMC: Fragmento de datos con código de borrado faltante

Este mensaje de auditoría indica que el sistema ha detectado un fragmento de datos con código de borrado faltante.

Código	Campo	Descripción
VCMC	Identificación de VCS	El nombre del VCS que contiene el fragmento faltante.
MCID	Identificación del fragmento	El identificador del fragmento codificado por borrado que falta.
RSLT	Resultado	Este campo tiene el valor 'NINGUNO'. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje en particular. Se utiliza 'NONE' en lugar de 'SUCS' para que este mensaje no se filtre.

ECOC: Fragmento de datos corruptos codificados por borrado

Este mensaje de auditoría indica que el sistema ha detectado un fragmento de datos codificado por borrado corrupto.

Código	Campo	Descripción
VCCO	Identificación de VCS	El nombre del VCS que contiene el fragmento dañado.
VLID	ID de volumen	El volumen RangeDB que contiene el fragmento codificado de borrado dañado.
CCID	Identificación del fragmento	El identificador del fragmento codificado de borrado corrupto.
RSLT	Resultado	Este campo tiene el valor 'NINGUNO'. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje en particular. Se utiliza 'NONE' en lugar de 'SUCS' para que este mensaje no se filtre.

ETAF: Falló la autenticación de seguridad

Este mensaje se genera cuando falla un intento de conexión mediante Seguridad de la capa de transporte (TLS).

Código	Campo	Descripción
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP en la que falló la autenticación.
RUIDO	Identidad del usuario	Un identificador dependiente del servicio que representa la identidad del usuario remoto.

Código	Campo	Descripción
RSLT	Código de motivo	La razón del fallo: SCNI: Error en el establecimiento de conexión segura. CERM: Falta el certificado. CERT: El certificado no era válido. CERE: El certificado ha expirado. CERR: El certificado fue revocado. CSGN: La firma del certificado no era válida. CSGU: Se desconoce el firmante del certificado. UCRM: Faltaban credenciales de usuario. UCRI: Las credenciales de usuario no eran válidas. UCRU: No se permitieron las credenciales de usuario. TOUT: Se agotó el tiempo de autenticación.

Cuando se establece una conexión a un servicio seguro que utiliza TLS, las credenciales de la entidad remota se verifican utilizando el perfil TLS y la lógica adicional incorporada al servicio. Si esta autenticación falla debido a certificados o credenciales no válidos, inesperados o no permitidos, se registra un mensaje de auditoría. Esto permite realizar consultas sobre intentos de acceso no autorizado y otros problemas de conexión relacionados con la seguridad.

El mensaje podría ser el resultado de una entidad remota que tiene una configuración incorrecta o de intentos de presentar credenciales no válidas o no permitidas al sistema. Este mensaje de auditoría debe ser monitoreado para detectar intentos de obtener 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 .

Código	Campo	Descripción
RSLT	Resultado	El resultado de la solicitud de actualización: • SUCS: Exitoso • SUNV: Servicio no disponible • GERR: Otro fracaso
GNID	Nodo ID	El ID del nodo del servicio que inició la solicitud de actualización.

Código	Campo	Descripción
GNTTP	Tipo de dispositivo	El tipo de dispositivo del nodo de la red (por ejemplo, BLDR para un servicio LDR).
GNDV	Versión del modelo del dispositivo	La cadena que identifica la versión del modelo del dispositivo del nodo de la red en el paquete DMDL.
GNGP	Grupo	El grupo al que pertenece el nodo de la red (en el contexto de los costos de enlace y la clasificación de consultas de servicio).
GNIA	Dirección IP	La dirección IP del nodo de la red.

Este mensaje se genera cada vez que un nodo de la cuadrícula actualiza su entrada en el paquete de nodos de la cuadrícula.

GNUR: Anulación del registro de GNDS

El servicio CMN genera este mensaje de auditoría cuando un servicio no ha registrado información sobre sí mismo en el sistema StorageGRID .

Código	Campo	Descripción
RSLT	Resultado	El resultado de la solicitud de actualización: • SUCS: Exitoso • SUNV: Servicio no disponible • GERR: Otro fracaso
GNID	Nodo ID	El ID del nodo del servicio que inició la solicitud de actualización.

GTED: Tarea de cuadrícula finalizada

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 de tarea de cuadrícula iniciada correspondiente. Los demás resultados indican que el procesamiento de esta tarea de cuadrícula nunca comenzó.

Código	Campo	Descripción
TSID	ID de tarea	Este campo identifica de forma única una tarea de cuadrícula generada y permite administrarla durante 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 Enviado, Iniciado y Finalizado.
RSLT	Resultado	El resultado del estado final de la tarea de cuadrícula: • SUCS: La tarea de cuadrícula se completó exitosamente. • ABRT: La tarea de cuadrícula se finalizó sin un error de reversión. • ROLF: La tarea de la red se finalizó y no se pudo completar el proceso de reversión. • CANC: La tarea de cuadrícula fue cancelada por el usuario antes de iniciarse. • EXPR: La tarea de la cuadrícula expiró antes de iniciarse. • IVLD: La tarea de cuadrícula no era válida. • AUTORIZACIÓN: La tarea de cuadrícula no fue autorizada. • DUPL: La tarea de cuadrícula fue rechazada por ser duplicada.

GTST: Tarea de cuadrícula iniciada

Este mensaje de auditoría indica que el servicio CMN ha comenzado a procesar la tarea de cuadrícula especificada. El mensaje de auditoría sigue inmediatamente al mensaje de Tarea de cuadrícula enviada para las tareas de cuadrícula iniciadas por el servicio interno de Envío de tareas de cuadrícula y seleccionadas para activación automática. Para las tareas de cuadrícula enviadas a la tabla Pendientes, este mensaje se genera cuando el usuario inicia la tarea de cuadrícula.

Código	Campo	Descripción
TSID	ID de tarea	Este campo identifica de forma única una tarea de cuadrícula generada y permite administrar la tarea durante 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 Enviado, Iniciado y Finalizado.
RSLT	Resultado	El resultado. Este campo solo tiene un valor: • SUCS: La tarea de cuadrícula se inició exitosamente.

Este mensaje de auditoría indica que se ha enviado una tarea de red al servicio CMN.

Código	Campo	Descripción
TSID	ID de tarea	Identifica de forma única una tarea de cuadrícula generada y permite gestionarla 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 Enviado, Iniciado y Finalizado.
TTYP	Tipo de tarea	El tipo de tarea de cuadrícula.
TVER	Versión de la tarea	Un número que indica la versión de la tarea de cuadrícula.
TDSC	Descripción de la tarea	Una descripción legible por humanos de la tarea de la cuadrícula.
VATS	Válido después de la marca de tiempo	El momento más temprano (microsegundos UINT64 a partir del 1 de enero de 1970 - hora UNIX) en el que la tarea de cuadrícula es válida.
VBTS	Válido antes de la marca de tiempo	El último momento (microsegundos UINT64 a partir del 1 de enero de 1970 - hora UNIX) en el que la tarea de cuadrícula es válida.
TSRC	Fuente	La fuente de la tarea: • TXTB: La tarea de cuadrícula se envió a través del sistema StorageGRID como un bloque de texto firmado. • GRID: La tarea de cuadrícula se envió a través del Servicio de envío de tareas de cuadrícula interno.
ACTV	Tipo de activación	El tipo de activación: • AUTO: La tarea de cuadrícula fue enviada para activación automática. • PEND: La tarea de la cuadrícula se envió a la tabla pendiente. Esta es la única posibilidad para la fuente TXTB.
RSLT	Resultado	El resultado de la presentación: • SUCS: La tarea de cuadrícula se envió correctamente. • ERROR: La tarea se ha movido directamente a la tabla histórica.

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 en depósitos S3 compatibles:** este mensaje se genera cuando ILM inicia el proceso de eliminación automática de un objeto porque su período de retención ha expirado (suponiendo que la configuración de eliminación automática está habilitada y la retención legal está desactivada).
- **Para objetos en depósitos S3 no compatibles.** Este mensaje se genera cuando ILM inicia el proceso de eliminación de un objeto porque no hay instrucciones de ubicación en las políticas ILM activas que se apliquen actualmente al objeto.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El CBID del objeto.
CMPA	Cumplimiento: Eliminación automática	Solo para objetos en depósitos S3 compatibles. 0 (falso) o 1 (verdadero), indica si un objeto compatible debe eliminarse automáticamente cuando finaliza su período de retención, a menos que el depósito esté bajo una retención legal.
CMPL	Cumplimiento: Retención legal	Solo para objetos en depósitos S3 compatibles. 0 (falso) o 1 (verdadero), indica si el depósito se encuentra actualmente bajo retención legal.
CMPR	Cumplimiento: Periodo de conservación	Solo para objetos en depósitos S3 compatibles. La duración del período de retención del objeto en minutos.
CTME	Cumplimiento: Tiempo de ingesta	Solo para objetos en depósitos S3 compatibles. El tiempo de ingesta del objeto. Puede agregar el período de retención en minutos a este valor para determinar cuándo se puede eliminar el objeto del depósito.
DMRK	Eliminar ID de versión del marcador	El ID de la versión del marcador de eliminación creado al eliminar un objeto de un depósito versionado. Las operaciones en depósitos no incluyen este campo.
CSIZ	Tamaño del contenido	El tamaño del objeto en bytes.

Código	Campo	Descripción
LOCS	Ubicaciones	La ubicación de almacenamiento de los datos de objetos dentro del sistema StorageGRID . El valor de LOCS es "" si el objeto no tiene ubicaciones (por ejemplo, ha sido eliminado). CLEC: para objetos con código de borrado, el ID del perfil de codificación de borrado y el ID del grupo de codificación de borrado que se aplica a los datos del objeto. CLDI: para objetos replicados, el ID del nodo LDR y el ID del volumen de la ubicación del objeto. CLNL: ID del nodo ARC de la ubicación del objeto si los datos del objeto están archivados.
CAMINO	Cubo/clave S3	El nombre del depósito S3 y el nombre de la clave S3.
RSLT	Resultado	El resultado de la operación ILM. SUCS: La operación ILM fue exitosa.
REGLA	Etiqueta de reglas	• Si un objeto en un bucket S3 compatible se elimina automáticamente porque su período de retención ha expirado, este campo estará en blanco. • Si se elimina el objeto porque no hay más instrucciones de ubicación que se apliquen actualmente al objeto, este campo muestra la etiqueta legible por humanos de la última regla ILM que se aplicó al objeto.
SGRP	Sitio (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 ID de la versión de la versión específica de un objeto que se eliminó. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.

LKCU: Limpieza de objetos sobrescritos

Este mensaje se genera cuando StorageGRID elimina un objeto sobrescrito que anteriormente requería limpieza para liberar espacio de almacenamiento. Un objeto se sobrescribe cuando un cliente S3 escribe un objeto en una ruta que ya contiene un objeto. El proceso de eliminación se produce de forma automática y en segundo plano.

Código	Campo	Descripción
CSIZ	Tamaño del contenido	El tamaño del objeto en bytes.
LTYP	Tipo de limpieza	<i>Sólo para uso interno.</i>
LUID	UUID del objeto eliminado	El identificador del objeto que fue eliminado.
CAMINO	Cubo/clave S3	El nombre del depósito S3 y el nombre de la clave S3.
SEGC	UUID del contenedor	UUID del contenedor del objeto segmentado. Este valor solo está disponible si el objeto está segmentado.
UUID	Identificador único universal	El identificador del objeto que todavía existe. Este valor solo está disponible si el objeto no ha sido eliminado.

LKDM: Limpieza de objetos filtrados

Este mensaje se genera cuando se ha limpiado o eliminado un fragmento filtrado. Un fragmento puede ser parte de un objeto replicado o de un objeto codificado para borrado.

Código	Campo	Descripción
CLOC	Ubicación del fragmento	La ruta del archivo del fragmento filtrado que se eliminó.
CTYP	Tipo de trozo	Tipo de fragmento: ec: Erasure-coded object chunk repl: Replicated object chunk

Código	Campo	Descripción
LTyp	Tipo de fuga	Los cinco tipos de fugas que se pueden detectar: <code>object_leaked</code>: Object doesn't exist in the grid <code>location_leaked</code>: Object exists in the grid, but found location doesn't belong to object <code>mup_seg_leaked</code>: Multipart upload was stopped or not completed, and the segment/part was left out <code>segment_leaked</code>: Parent UUID/CBID (associated container object) is valid but doesn't contain this segment <code>no_parent</code>: Container object is deleted, but object segment was left out and not deleted
CTIM	Tiempo de creación de fragmentos	Hora en que se creó el fragmento filtrado.
UUID	Identificador único universal	El identificador del objeto al que pertenece el fragmento.
CBD	Identificador de bloque de contenido	CBID del objeto al que pertenece el fragmento filtrado.
CSIZ	Tamaño del contenido	El tamaño del fragmento en bytes.

LLST: Ubicación perdida

Este mensaje se genera siempre que no se puede encontrar una ubicación para una copia de un objeto (replicada o codificada por borrado).

Código	Campo	Descripción
CBIL	CBD	El CBD afectado.
ECPR	Perfil de codificación de borrado	Para datos de objetos codificados por borrado. El ID del perfil de codificación de borrado utilizado.

Código	Campo	Descripción
LTyp	Tipo de ubicación	CLDI (en línea): para datos de objetos replicados CLEC (en línea): para datos de objetos codificados por borrado CLNL (Nearline): para datos de objetos replicados archivados
NOID	ID del nodo de origen	El ID del nodo en el que se perdieron las ubicaciones.
PCLD	Ruta al objeto replicado	La ruta completa a la ubicación del disco de los datos del objeto perdido. Sólo se devuelve cuando LTyp tiene un valor de CLDI (es decir, para objetos replicados). Toma la forma <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@</code>
RSLT	Resultado	Siempre NINGUNO. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. Se utiliza NONE en lugar de SUCS para que este mensaje no se filtre.
TSRC	Fuente de activación	USUARIO: Usuario activado SYST: Sistema activado
UUID	Identificación universalmente única	El identificador del objeto afectado en el sistema StorageGRID .

MGAU: Mensaje de auditoría de gestión

La categoría Administración registra las solicitudes de los usuarios a la API de Administración. Cada solicitud HTTP que no sea una solicitud GET o HEAD a una URI de API válida registra una respuesta que contiene el nombre de usuario, la IP y el tipo de solicitud a la API. Las URI de API no válidas (como /api/v3-authorize) y las solicitudes no válidas a URI de API válidas no se registran.

Código	Campo	Descripción
MDIP	Dirección IP de destino	La dirección IP del servidor (destino).
ADNmd	Nombre de dominio	El nombre de dominio del host.
MPAT	Solicitar PATH	La ruta de la solicitud.

Código	Campo	Descripción
MPQP	Parámetros de consulta de solicitud	Los parámetros de consulta para la solicitud.
MRBD	Cuerpo de la solicitud	El contenido del cuerpo de la solicitud. Si bien el cuerpo de la respuesta se registra de forma predeterminada, el cuerpo de la solicitud se registra en ciertos casos cuando el cuerpo de la respuesta está vacío. Como la siguiente información no está disponible en el cuerpo de la respuesta, se toma del cuerpo de la solicitud para los siguientes métodos POST: • Nombre de usuario e ID de cuenta en POST autorizar • Nueva configuración de subredes en POST /grid/grid-networks/update • Nuevos servidores NTP en POST /grid/ntp-servers/update • ID de servidores dados de baja en POST /grid/servers/decommission 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: • CORREO • PONER • BORRAR • PARCHE
MRSC	Código de respuesta	El código de respuesta.
Precio de venta sugerido al público	Cuerpo de la 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 (fuente).
MUUN	URN de usuario	El URN (nombre uniforme del recurso) del usuario que envió la solicitud.
RSLT	Resultado	Devuelve el éxito (SUCS) o el error informado 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 .

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El CBID del objeto perdido.
NOID	Nodo ID	Si está disponible, la última ubicación conocida, directa o cercana, del objeto perdido. Es posible tener solo el ID de nodo sin un ID de volumen si la información del volumen no está disponible.
CAMINO	Cubo/clave S3	Si está disponible, el nombre del depósito S3 y el nombre de la clave S3.
RSLT	Resultado	Este campo tiene el valor NINGUNO. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. Se utiliza NONE en lugar de SUCS para que este mensaje no se filtre.
UUID	Identificación universalmente única	El identificador del objeto perdido dentro del sistema StorageGRID .
VOLI	ID de volumen	Si está disponible, el ID de volumen del nodo de almacenamiento de la última ubicación conocida del objeto perdido.

ORLM: Se cumplen las reglas de objeto

Este mensaje se genera cuando el objeto se almacena y copia correctamente según lo especificado por las reglas de ILM.



El mensaje ORLM no se genera cuando un objeto se almacena correctamente mediante la regla predeterminada Hacer 2 copias si otra regla en la política utiliza el filtro avanzado Tamaño del objeto.

Código	Campo	Descripción
CONSTRUIR	Encabezado del cubo	Campo de identificación del depósito. Se utiliza para operaciones internas. Sólo aparece si STAT es PRGD.
CBD	Identificador de bloque de contenido	El CBID del objeto.
CSIZ	Tamaño del contenido	El tamaño del objeto en bytes.

Código	Campo	Descripción
LOCS	Ubicaciones	La ubicación de almacenamiento de los datos de objetos dentro del sistema StorageGRID . El valor de LOCS es "" si el objeto no tiene ubicaciones (por ejemplo, ha sido eliminado). CLEC: para objetos con código de borrado, el ID del perfil de codificación de borrado y el ID del grupo de codificación de borrado que se aplica a los datos del objeto. CLDI: para objetos replicados, el ID del nodo LDR y el ID del volumen de la ubicación del objeto. CLNL: ID del nodo ARC de la ubicación del objeto si los datos del objeto están archivados.
CAMINO	Cubo/clave S3	El nombre del depósito S3 y el nombre de la clave S3.
RSLT	Resultado	El resultado de la operación ILM. SUCS: La operación ILM fue exitosa.
REGLA	Etiqueta de reglas	La etiqueta legible por humanos dada a la regla ILM aplicada a este objeto.
SEGC	UUID del contenedor	UUID del contenedor del objeto segmentado. Este valor solo está disponible si el objeto está segmentado.
SGCB	Contenedor CBDI	CBID del contenedor del objeto segmentado. Este valor solo está disponible para objetos segmentados y multiparte.
ESTADÍSTICA	Estado	El estado de la operación de ILM. HECHO: Se han completado las operaciones ILM contra el objeto. DFER: El objeto ha sido marcado para una futura reevaluación ILM. PRGD: El objeto ha sido eliminado del sistema StorageGRID . NLOC: Los datos del objeto ya no se pueden encontrar en el sistema StorageGRID . Este estado podría indicar que todas las copias de los datos del objeto faltan o están dañadas.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de un nuevo objeto creado en un depósito versionado. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.

El mensaje de auditoría ORLM se puede emitir más de una vez para un solo objeto. Por ejemplo, se emite

siempre que ocurre uno de los siguientes eventos:

- Las reglas ILM para el objeto se satisfacen para siempre.
- Las reglas ILM para el objeto se cumplen para esta época.
- Las reglas de ILM han eliminado el objeto.
- El proceso de verificación de fondo detecta que una copia de los datos del objeto replicado está dañada. El sistema StorageGRID realiza una evaluación ILM para reemplazar el objeto dañado.

Información relacionada

- ["Transacciones de ingesta de objetos"](#)
- ["Transacciones de eliminación de objetos"](#)

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.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido (nuevo)	El CBID del nuevo objeto.
CSIZ	Tamaño del objeto anterior	El tamaño, en bytes, del objeto que se está sobrescribiendo.
Trastorno obsesivo-compulsivo (OCBD)	Identificador de bloque de contenido (anterior)	El CBID del objeto anterior.
UUID	Identificación única universal (nueva)	El identificador del nuevo objeto dentro del sistema StorageGRID .
OUID	Identificación única universal (anterior)	El identificador del objeto anterior dentro del sistema StorageGRID .
CAMINO	Ruta del objeto S3	La ruta del objeto S3 utilizada tanto para el objeto anterior como para el nuevo
RSLT	Código de resultado	Resultado de la transacción de sobrescritura de objeto. El resultado siempre es: SUCS: Exitoso

Código	Campo	Descripción
SGRP	Sitio (Grupo)	Si está presente, el objeto sobrescrito se eliminó en el sitio especificado, que no es el sitio donde se ingirió el objeto sobrescrito.

S3SL: Solicitud de selección de S3

Este mensaje registra una finalización después de que se haya devuelto una solicitud S3 Select al cliente. El mensaje S3SL puede incluir detalles del mensaje de error y del código de error. Es posible que la solicitud no haya tenido éxito.

Código	Campo	Descripción
BYSC	Bytes escaneados	Número de bytes escaneados (recibidos) desde los nodos de almacenamiento. Es probable que BYSC y BYPR sean diferentes si el objeto está comprimido. Si el objeto está comprimido, BYSC tendrá el recuento de bytes comprimidos y BYPR serán los bytes después de la descompresión.
BYPR	Bytes procesados	Número de bytes procesados. Indica cuántos bytes de "Bytes escaneados" fueron realmente procesados o procesados por un trabajo S3 Select.
BYRT	Bytes devueltos	Número de bytes que un trabajo S3 Select devolvió al cliente.
REPR	Registros procesados	Número de registros o filas que un trabajo S3 Select recibió de los nodos de almacenamiento.
RERT	Registros devueltos	Número de registros o filas que un trabajo S3 Select devolvió al cliente.
JOFI	Trabajo terminado	Indica si el trabajo S3 Select finalizó el procesamiento o no. Si esto es falso, entonces el trabajo no pudo finalizar y los campos de error probablemente contendrán datos. Es posible que el cliente haya recibido resultados parciales o ningún resultado.
REID	ID de solicitud	Identificador de la solicitud S3 Select.
EXTRA	Tiempo de ejecución	El tiempo, en segundos, que tardó el trabajo de selección S3 en completarse.
ERMG	Mensaje de error	Mensaje de error que generó el trabajo S3 Select.
TERRENO	Tipo de error	Tipo de error que generó el trabajo S3 Select.

Código	Campo	Descripción
ANTE TODO	Seguimiento de errores	Seguimiento de pila de errores que generó el trabajo S3 Select.
S3BK	Cubo S3	El nombre del depósito S3.
S3AK	ID de clave de acceso S3 (remitente de la solicitud)	El ID de la clave de acceso S3 del usuario que envió la solicitud.
S3AI	ID de cuenta de inquilino de S3 (remitente de la solicitud)	El ID de la cuenta de inquilino del usuario que envió la solicitud.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito.

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 envían.

Código	Campo	Descripción
AETM	Habilitar método	El método utilizado para deshabilitar la auditoría.
AEUN	Nombre de usuario	El nombre de usuario que ejecutó el comando para deshabilitar el registro de auditoría.
RSLT	Resultado	Este campo tiene el valor NINGUNO. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. Se utiliza NONE en lugar de SUCS para que este mensaje no se filtre.

El mensaje implica que el registro estaba habilitado anteriormente, pero ahora se ha deshabilitado. Normalmente esto se usa solo durante la ingesta masiva para mejorar el rendimiento del sistema. Luego de la actividad masiva, se restablece la auditoría (SADE) y la capacidad de deshabilitarla se bloquea de forma permanente.

SADE: Habilitación 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 están recopilando y entregando nuevamente.

Código	Campo	Descripción
AETM	Habilitar método	El método utilizado para permitir la auditoría.
AEUN	Nombre de usuario	El nombre de usuario que ejecutó el comando para habilitar el registro de auditoría.
RSLT	Resultado	Este campo tiene el valor NINGUNO. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. Se utiliza NONE en lugar de SUCS para que este mensaje no se filtre.

El mensaje implica que el registro estaba previamente deshabilitado (SADD), pero ahora ha sido restaurado. Normalmente esto solo se utiliza durante la ingesta masiva para mejorar el rendimiento del sistema. Luego de la actividad masiva, se restablece la auditoría y la capacidad de deshabilitarla se bloquea de forma permanente.

SCMT: Confirmación del almacén de objetos

El contenido de la red no se pone a disposición ni se reconoce como almacenado hasta que se haya confirmado (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 emite cuando un bloque de contenido se envía al almacenamiento.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido destinado al almacenamiento permanente.
RSLT	Código de resultado	Estado en el momento en que el objeto se almacenó en el disco: SUCS: Objeto almacenado exitosamente.

Este mensaje significa que un bloque de contenido determinado se ha almacenado y verificado por completo y ahora se puede solicitar. Se puede utilizar para rastrear el flujo de datos dentro del sistema.

SDEL: S3 ELIMINAR

Cuando un cliente S3 emite una transacción DELETE, se realiza una solicitud para eliminar el objeto o depósito especificado, o para eliminar un subrecurso de depósito/objeto. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones en depósitos no incluyen este campo.

Código	Campo	Descripción
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP Consistency-Control, si está presente en la solicitud.
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño del contenido	El tamaño del objeto eliminado en bytes. Las operaciones en depósitos no incluyen este campo.
DMRK	Eliminar ID de versión del marcador	El ID de la versión del marcador de eliminación creado al eliminar un objeto de un depósito versionado. Las operaciones en depósitos no incluyen este campo.
GFID	ID de conexión de la federación de red	El ID de conexión de la conexión de federación de red asociada con una solicitud de eliminación de replicación entre redes. Sólo se incluye en los registros de auditoría de la red de destino.
GFSA	ID de cuenta de origen de Grid Federation	El ID de cuenta del inquilino en la red de origen para una solicitud de eliminación de replicación entre redes. Sólo se incluye en los registros de auditoría de la red de destino.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP). `x-amz-bypass-governance-retention` Se incluye automáticamente si está presente en la solicitud.
MTME	Hora de última modificación	La marca de tiempo de Unix, en microsegundos, que indica cuándo se modificó el objeto por última vez.
RSLT	Código de resultado	Resultado de la transacción DELETE. El resultado siempre es: SUCS: Exitoso
S3AI	ID de cuenta de inquilino de S3 (remitente de la solicitud)	El ID de la cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.

Código	Campo	Descripción
S3AK	ID de clave de acceso S3 (remitente de la solicitud)	El ID de clave de acceso S3 en formato hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito. Las operaciones en depósitos no incluyen este campo.
S3SR	Subrecurso S3	El subrecurso del objeto o depósito en el que se opera, si corresponde.
SACC	Nombre de la cuenta del inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de inquilino del usuario que envió la solicitud. Vacío para solicitudes anónimas.
SAIP	Dirección IP (remitente de la solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de la cuenta del inquilino de S3 (propietario del depósito)	El nombre de la cuenta del inquilino del propietario del depósito. Se utiliza para identificar acceso entre cuentas o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del depósito)	El ID de la cuenta de inquilino del propietario del depósito de destino. Se utiliza para identificar acceso entre cuentas o anónimo.
SGRP	Sitio (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 S3 (remitente de la solicitud)	El ID de la cuenta del inquilino 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 total de procesamiento de la solicitud en microsegundos.

Código	Campo	Descripción
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUDM	Identificador único universal para un marcador de eliminación	El identificador de un marcador de eliminación. Los mensajes del registro de auditoría especifican UUDM o UUID, donde UUDM indica un marcador de eliminación creado como resultado de una solicitud de eliminación de objeto y UUID indica un objeto.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de la versión específica de un objeto que se eliminó. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.

SGET: S3 OBTENER

Cuando un cliente S3 emite una transacción GET, se realiza una solicitud para recuperar un objeto o enumerar los objetos en un depósito, o para eliminar un subrecurso de depósito/objeto. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones en depósitos no incluyen este campo.
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP Consistency-Control, si está presente en la solicitud.
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño del contenido	El tamaño del objeto recuperado en bytes. Las operaciones en depósitos no incluyen este campo.

Código	Campo	Descripción
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
LIDAD	ListObjectsV2	Se solicitó una respuesta en formato v2. Para más detalles, consulte "AWS ListObjectsV2" . Solo para operaciones de depósito GET.
NCHD	Número de niños	Incluye claves y prefijos comunes. Solo para operaciones de depósito GET.
RANG	Rango de lectura	Solo para operaciones de lectura de rango. Indica el rango de bytes que se leyeron en esta solicitud. El valor después de la barra (/) muestra el tamaño del objeto completo.
RSLT	Código de resultado	Resultado de la transacción GET. El resultado siempre es: SUCS: Exitoso
S3AI	ID de cuenta de inquilino de S3 (remitente de la solicitud)	El ID de la cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de la solicitud)	El ID de clave de acceso S3 en formato hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito. Las operaciones en depósitos no incluyen este campo.
S3SR	Subrecurso S3	El subrecurso del objeto o depósito en el que se opera, si corresponde.
SACC	Nombre de la cuenta del inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de inquilino del usuario que envió la solicitud. Vacío para solicitudes anónimas.

Código	Campo	Descripción
SAIP	Dirección IP (remitente de la solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de la cuenta del inquilino de S3 (propietario del depósito)	El nombre de la cuenta del inquilino del propietario del depósito. Se utiliza para identificar acceso entre cuentas o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del depósito)	El ID de la cuenta de inquilino del propietario del depósito de destino. Se utiliza para identificar acceso entre cuentas o anónimo.
SUSR	URN de usuario S3 (remitente de la solicitud)	El ID de la cuenta del inquilino y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vacío para solicitudes anónimas.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
República Turca del Norte de Tennessee	Truncado o no truncado	Establezca como falso si se devolvieron todos los resultados. Establezca como verdadero si hay más resultados disponibles para devolver. Solo para operaciones de depósito GET.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de la versión específica de un objeto que se solicitó. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.

SHEA: CABEZA T3

Cuando un cliente S3 emite una transacción HEAD, se realiza una solicitud para verificar la existencia de un objeto o depósito y recuperar los metadatos sobre un objeto. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones en depósitos no incluyen este campo.
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño del contenido	El tamaño del objeto comprobado en bytes. Las operaciones en depósitos no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
RSLT	Código de resultado	Resultado de la transacción GET. El resultado siempre es: SUCS: Exitoso
S3AI	ID de cuenta de inquilino de S3 (remitente de la solicitud)	El ID de la cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de la solicitud)	El ID de clave de acceso S3 en formato hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito. Las operaciones en depósitos no incluyen este campo.
SACC	Nombre de la cuenta del inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de inquilino del usuario que envió la solicitud. Vacío para solicitudes anónimas.

Código	Campo	Descripción
SAIP	Dirección IP (remitente de la solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de la cuenta del inquilino de S3 (propietario del depósito)	El nombre de la cuenta del inquilino del propietario del depósito. Se utiliza para identificar acceso entre cuentas o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del depósito)	El ID de la cuenta de inquilino del propietario del depósito de destino. Se utiliza para identificar acceso entre cuentas o anónimo.
SUSR	URN de usuario S3 (remitente de la solicitud)	El ID de la cuenta del inquilino y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vacío para solicitudes anónimas.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de la versión específica de un objeto que se solicitó. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.

SPOS: PUBLICACIÓN S3

Cuando un cliente S3 emite una solicitud de objeto POST, el servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0.

Código	Campo	Descripción
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP Consistency-Control, si está presente en la solicitud.
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño del contenido	El tamaño del objeto recuperado en bytes.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP). (No esperado para SPOS).
RSLT	Código de resultado	Resultado de la solicitud RestoreObject. El resultado siempre es: SUCS: Exitoso
S3AI	ID de cuenta de inquilino de S3 (remitente de la solicitud)	El ID de la cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de la solicitud)	El ID de clave de acceso S3 en formato hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito. Las operaciones en depósitos no incluyen este campo.
S3SR	Subrecurso S3	El subrecurso del objeto o depósito en el que se opera, si corresponde. Establezca en "seleccionar" para una operación de selección S3.

Código	Campo	Descripción
SACC	Nombre de la cuenta del inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de inquilino del usuario que envió la solicitud. Vacío para solicitudes anónimas.
SAIP	Dirección IP (remitente de la solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de la cuenta del inquilino de S3 (propietario del depósito)	El nombre de la cuenta del inquilino del propietario del depósito. Se utiliza para identificar acceso entre cuentas o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del depósito)	El ID de la cuenta de inquilino del propietario del depósito de destino. Se utiliza para identificar acceso entre cuentas o anónimo.
SRCF	Configuración de subrecursos	Restaurar información.
SUSR	URN de usuario S3 (remitente de la solicitud)	El ID de la cuenta del inquilino y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vacío para solicitudes anónimas.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de la versión específica de un objeto que se solicitó. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.

SPUT: S3 PONER

Cuando un cliente S3 emite una transacción PUT, se realiza una solicitud para crear un

nuevo objeto o depósito, o para eliminar un subrecurso de depósito/objeto. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones en depósitos no incluyen este campo.
CMPS	Configuración de cumplimiento	La configuración de cumplimiento utilizada al crear el depósito, si está presente en la solicitud (truncada a los primeros 1024 caracteres).
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP Consistency-Control, si está presente en la solicitud.
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño del contenido	El tamaño del objeto recuperado en bytes. Las operaciones en depósitos no incluyen este campo.
GFID	ID de conexión de la federación de red	El ID de conexión de la conexión de federación de red asociada con una solicitud PUT de replicación entre redes. Sólo se incluye en los registros de auditoría de la red de destino.
GFSA	ID de cuenta de origen de Grid Federation	El ID de cuenta del inquilino en la red de origen para una solicitud PUT de replicación entre redes. Sólo se incluye en los registros de auditoría de la red de destino.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. <code>`X-Forwarded-For`</code> se incluye automáticamente si está presente en la solicitud y si el <code>`X-Forwarded-For`</code> El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP). <code>`x-amz-bypass-governance-retention`</code> Se incluye automáticamente si está presente en la solicitud.
LKEN	Bloqueo de objetos habilitado	Valor del encabezado de la solicitud <code>x-amz-bucket-object-lock-enabled</code> , si está presente en la solicitud.

Código	Campo	Descripción
LKLH	Bloqueo de objeto con retención legal	Valor del encabezado de la solicitud <code>x-amz-object-lock-legal-hold</code> , si está presente en la solicitud PutObject.
LKMD	Modo de retención de bloqueo de objetos	Valor del encabezado de la solicitud <code>x-amz-object-lock-mode</code> , si está presente en la solicitud PutObject.
LKRU	Bloqueo de objeto Retener hasta fecha	Valor del encabezado de la solicitud <code>x-amz-object-lock-retain-until-date</code> , si está presente en la solicitud PutObject. Los valores están limitados a los 100 años a partir de la fecha en que se ingirió el objeto.
MTME	Hora de última modificación	La marca de tiempo de Unix, en microsegundos, que indica cuándo se modificó el objeto por última vez.
RSLT	Código de resultado	Resultado de la transacción PUT. El resultado siempre es: SUCS: Exitoso
S3AI	ID de cuenta de inquilino de S3 (remitente de la solicitud)	El ID de la cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de la solicitud)	El ID de clave de acceso S3 en formato hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito. Las operaciones en depósitos no incluyen este campo.
S3SR	Subrecurso S3	El subrecurso del objeto o depósito en el que se opera, si corresponde.
SACC	Nombre de la cuenta del inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de inquilino del usuario que envió la solicitud. Vacío para solicitudes anónimas.
SAIP	Dirección IP (remitente de la solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.

Código	Campo	Descripción
SBAC	Nombre de la cuenta del inquilino de S3 (propietario del depósito)	El nombre de la cuenta del inquilino del propietario del depósito. Se utiliza para identificar acceso entre cuentas o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del depósito)	El ID de la cuenta de inquilino del propietario del depósito de destino. Se utiliza para identificar acceso entre cuentas o anónimo.
SRCF	Configuración de subrecursos	La nueva configuración del subrecurso (truncada a los primeros 1024 caracteres).
SUSR	URN de usuario S3 (remitente de la solicitud)	El ID de la cuenta del inquilino y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vacío para solicitudes anónimas.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
ULID	Subir ID	Incluido solo en mensajes SPUT para operaciones CompleteMultipartUpload. Indica que todas las piezas se han cargado y ensamblado.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de un nuevo objeto creado en un depósito versionado. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.
VSST	Estado de versiones	El nuevo estado de versión de un bucket. Se utilizan dos estados: "habilitado" o "suspendido". Las operaciones sobre objetos no incluyen este campo.

SREM: Eliminar almacén de objetos

Este mensaje se emite cuando se elimina contenido del almacenamiento persistente y ya no es accesible a través de las API normales.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido eliminado del almacenamiento permanente.
RSLT	Código de resultado	Indica el resultado de las operaciones de eliminación de contenido. El único valor definido es: SUCS: Contenido eliminado del almacenamiento persistente

Este mensaje de auditoría significa que un bloque de contenido determinado se ha eliminado de un nodo y ya no se puede solicitar directamente. El mensaje se puede utilizar para rastrear el flujo de contenido eliminado dentro del sistema.

SUPD: Metadatos S3 actualizados

La API S3 genera este mensaje cuando un cliente S3 actualiza los metadatos de un objeto ingerido. El servidor emite el mensaje si la actualización de metadatos es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones en depósitos no incluyen este campo.
CNCH	Encabezado de control de consistencia	El valor del encabezado de solicitud HTTP Consistency-Control, si está presente en la solicitud, al actualizar la configuración de cumplimiento de un depósito.
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP.
CSIZ	Tamaño del contenido	El tamaño del objeto recuperado en bytes. Las operaciones en depósitos no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).

Código	Campo	Descripción
RSLT	Código de resultado	Resultado de la transacción GET. El resultado siempre es: SUCS: exitoso
S3AI	ID de cuenta de inquilino de S3 (remitente de la solicitud)	El ID de la cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de clave de acceso S3 (remitente de la solicitud)	El ID de clave de acceso S3 en formato hash para el usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Cubo S3	El nombre del depósito S3.
S3KY	Clave S3	El nombre de la clave S3, sin incluir el nombre del depósito. Las operaciones en depósitos no incluyen este campo.
SACC	Nombre de la cuenta del inquilino de S3 (remitente de la solicitud)	El nombre de la cuenta de inquilino del usuario que envió la solicitud. Vacío para solicitudes anónimas.
SAIP	Dirección IP (remitente de la solicitud)	La dirección IP de la aplicación cliente que realizó la solicitud.
SBAC	Nombre de la cuenta del inquilino de S3 (propietario del depósito)	El nombre de la cuenta del inquilino del propietario del depósito. Se utiliza para identificar acceso entre cuentas o anónimo.
SBAI	ID de cuenta de inquilino de S3 (propietario del depósito)	El ID de la cuenta de inquilino del propietario del depósito de destino. Se utiliza para identificar acceso entre cuentas o anónimo.
SUSR	URN de usuario S3 (remitente de la solicitud)	El ID de la cuenta del inquilino y el nombre de usuario del usuario que realiza la solicitud. El usuario puede ser un usuario local o un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Vacío para solicitudes anónimas.

Código	Campo	Descripción
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
VSID	ID de versión	El ID de la versión de la versión específica de un objeto cuyos metadatos se actualizaron. Las operaciones en depósitos y objetos en depósitos no versionados no incluyen este campo.

SVRF: Error en la verificación del almacén de objetos

Este mensaje se emite siempre que un bloque de contenido no pasa el proceso de verificación. Cada vez que se leen o escriben datos de un objeto replicado en un disco, se realizan varias verificaciones e integridad para garantizar que los datos enviados al usuario solicitante sean idénticos a los datos ingresados originalmente en el sistema. Si alguna de estas comprobaciones falla, el sistema pone automáticamente en cuarentena los datos del objeto replicado dañado para evitar que se recuperen nuevamente.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido que no pasó la verificación.
RSLT	Código de resultado	Tipo de error de verificación: CRCF: Error en la verificación de redundancia cíclica (CRC). HMAC: Error en la verificación del código de autenticación de mensajes basado en hash (HMAC). EHS: Hash de contenido cifrado inesperado. PHS: Hash de contenido original inesperado. SEQC: Secuencia de datos incorrecta en el disco. PERR: Estructura no válida del archivo de disco. DERR: Error de disco. FNAM: Nombre de archivo incorrecto.



Este mensaje debe ser monitoreado de cerca. Las fallas de verificación de contenido pueden indicar fallas de hardware inminentes.

Para determinar qué operación activó el mensaje, consulte el valor del campo AMID (ID del módulo). Por ejemplo, un valor SVFY indica que el mensaje fue generado por el módulo Storage Verifier, es decir, verificación en segundo plano, y STOR indica que el mensaje fue activado por la recuperación de contenido.

SVRU: Verificación de almacén de objetos desconocida

El componente de almacenamiento del servicio LDR escanea continuamente todas las copias de datos de objetos replicados en el almacén de objetos. Este mensaje se emite cuando se detecta una copia desconocida o inesperada de datos de objetos replicados en el almacén de objetos y se mueve al directorio de cuarentena.

Código	Campo	Descripción
FPTH	Ruta del archivo	La ruta del archivo de la copia del objeto inesperado.
RSLT	Resultado	Este campo tiene el valor 'NINGUNO'. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. Se utiliza 'NONE' en lugar de 'SUCS' para que este mensaje no se filtre.



El mensaje de auditoría SVRU: Object Store Verify Unknown debe monitorearse de cerca. Significa que se detectaron copias inesperadas de datos de objetos en el almacén de objetos. Esta situación debe investigarse inmediatamente para determinar cómo se crearon estas copias, ya que puede indicar fallas inminentes de hardware.

SYSD: Parada de nodo

Cuando un servicio se detiene correctamente, se genera este mensaje para indicar que se solicitó el apagado. Normalmente, este mensaje se envía solo después de un reinicio posterior, porque la cola de mensajes de auditoría no se borra antes del apagado. Busque el mensaje SYST, enviado al comienzo de la secuencia de apagado, si el servicio no se ha reiniciado.

Código	Campo	Descripción
RSLT	Apagado limpio	La naturaleza del cierre: SUCS: El sistema se apagó limpiamente.

El mensaje no indica si se está deteniendo el servidor host, solo el servicio de informes. El RSLT de un SYSD no puede indicar un apagado "sucio", porque el mensaje se genera únicamente mediante apagados "limpios".

SYST: Nodo deteniéndose

Cuando un servicio se detiene correctamente, se genera este mensaje para indicar que se solicitó el apagado 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 reiniciar el servicio).

Código	Campo	Descripción
RSLT	Apagado limpio	La naturaleza del cierre: SUCS: El sistema se apagó limpiamente.

El mensaje no indica si se está deteniendo el servidor host, solo el servicio de informes. El código RSLT de un mensaje SYST no puede indicar un apagado "sucio", porque el mensaje se genera únicamente mediante apagados "limpios".

SYSU: Inicio del nodo

Cuando se reinicia un servicio, se genera este mensaje para indicar si el apagado anterior fue limpio (ordenado) o desordenado (inesperado).

Código	Campo	Descripción
RSLT	Apagado limpio	La naturaleza del cierre: SUCS: El sistema se apagó limpiamente. DSDN: El sistema no se apagó limpiamente. VRGN: El sistema se inició por primera vez después de la instalación (o reinstalación) del servidor.

El mensaje no indica si se inició el servidor host, solo el servicio de informes. Este mensaje se puede utilizar para:

- Detectar discontinuidad en el registro de auditoría.
- Determinar si un servicio está fallando durante la operación (ya que la naturaleza distribuida del sistema StorageGRID puede enmascarar estas fallas). El Administrador de servidor reinicia automáticamente un servicio fallido.

WDEL: Eliminación rápida

Cuando un cliente Swift emite una transacción DELETE, se realiza una solicitud para eliminar el objeto o contenedor especificado. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones sobre contenedores no incluyen este campo.
CSIZ	Tamaño del contenido	El tamaño del objeto eliminado en bytes. Las operaciones sobre contenedores no incluyen este campo.

Código	Campo	Descripción
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
MTME	Hora de última modificación	La marca de tiempo de Unix, en microsegundos, que indica cuándo se modificó el objeto por última vez.
RSLT	Código de resultado	Resultado de la transacción DELETE. El resultado siempre es: SUCS: Exitoso
SAIP	Dirección IP del cliente solicitante	La dirección IP de la aplicación cliente que realizó la solicitud.
SGRP	Sitio (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 total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
WACC	ID de cuenta Swift	El ID de cuenta único según lo especificado por el sistema StorageGRID .
WCON	Contenedor Swift	El nombre del contenedor Swift.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones sobre contenedores no incluyen este campo.
WUSR	Usuario de cuenta Swift	El nombre de usuario de la cuenta Swift que identifica de forma única al cliente que realiza la transacción.

WGET: Obtención rápida

Cuando un cliente Swift emite una transacción GET, se realiza una solicitud para recuperar un objeto, enumerar los objetos en un contenedor o enumerar los contenedores en una cuenta. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones sobre cuentas y contenedores no incluyen este campo.
CSIZ	Tamaño del contenido	El tamaño del objeto recuperado en bytes. Las operaciones sobre cuentas y contenedores no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. <code>`X-Forwarded-For`</code> se incluye automáticamente si está presente en la solicitud y si el <code>`X-Forwarded-For`</code> El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
RSLT	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 total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
WACC	ID de cuenta Swift	El ID de cuenta único según lo especificado por el sistema StorageGRID .
WCON	Contenedor Swift	El nombre del contenedor Swift. Las operaciones sobre cuentas no incluyen este campo.

Código	Campo	Descripción
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones sobre cuentas y contenedores no incluyen este campo.
WUSR	Usuario de cuenta Swift	El nombre de usuario de la cuenta Swift que identifica de forma única al cliente que realiza la transacción.

WHEA: CABEZA Veloz

Cuando un cliente Swift emite una transacción HEAD, se realiza una solicitud para verificar la existencia de una cuenta, un contenedor o un objeto y recuperar cualquier metadato relevante. El servidor emite este mensaje si la transacción es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones sobre cuentas y contenedores no incluyen este campo.
CSIZ	Tamaño del contenido	El tamaño del objeto recuperado en bytes. Las operaciones sobre cuentas y contenedores no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si el `X-Forwarded-For` El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
RSLT	Código de resultado	Resultado de la transacción HEAD. El resultado siempre es: SUCS: exitoso
SAIP	Dirección IP del cliente solicitante	La dirección IP de la aplicación cliente que realizó la solicitud.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.

Código	Campo	Descripción
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
WACC	ID de cuenta Swift	El ID de cuenta único según lo especificado por el sistema StorageGRID .
WCON	Contenedor Swift	El nombre del contenedor Swift. Las operaciones sobre cuentas no incluyen este campo.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones sobre cuentas y contenedores no incluyen este campo.
WUSR	Usuario de cuenta Swift	El nombre de usuario de la cuenta Swift que identifica de forma única al cliente que realiza la transacción.

WPUT: PUT rápido

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 es exitosa.

Código	Campo	Descripción
CBD	Identificador de bloque de contenido	El identificador único del bloque de contenido solicitado. Si se desconoce el CBID, este campo se establece en 0. Las operaciones sobre contenedores no incluyen este campo.
CSIZ	Tamaño del contenido	El tamaño del objeto recuperado en bytes. Las operaciones sobre contenedores no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de nombres y valores de encabezado de solicitud HTTP registrados según se seleccionaron durante la configuración. <code>`X-Forwarded-For`</code> se incluye automáticamente si está presente en la solicitud y si el <code>`X-Forwarded-For`</code> El valor es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
MTME	Hora de última modificación	La marca de tiempo de Unix, en microsegundos, que indica cuándo se modificó el objeto por última vez.
RSLT	Código de resultado	Resultado de la transacción PUT. El resultado siempre es: SUCS: exitoso

Código	Campo	Descripción
SAIP	Dirección IP del cliente solicitante	La dirección IP de la aplicación cliente que realizó la solicitud.
TIEMPO	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP del balanceador de carga confiable	Si la solicitud fue enrutada por un balanceador de carga de capa 7 confiable, la dirección IP del balanceador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID .
WACC	ID de cuenta Swift	El ID de cuenta único según lo especificado por el sistema StorageGRID .
WCON	Contenedor Swift	El nombre del contenedor Swift.
WOBJ	Objeto Swift	El identificador del objeto Swift. Las operaciones sobre contenedores no incluyen este campo.
WUSR	Usuario de cuenta Swift	El nombre de usuario de la cuenta Swift que identifica de forma única al cliente que realiza la transacción.

Expandir una cuadrícula

Tipos de expansión

Puede ampliar la capacidad o las capacidades de su sistema StorageGRID sin interrumpir las operaciones del sistema.

Una expansión de StorageGRID le permite agregar:

- Volúmenes de almacenamiento a nodos de almacenamiento
- Nuevos nodos de red en un sitio existente
- Un sitio completamente nuevo

El motivo por el que realiza la expansión determina cuántos nodos nuevos de cada tipo debe agregar y la ubicación de esos nuevos nodos. Por ejemplo, existen diferentes requisitos de nodo si está realizando una expansión para aumentar la capacidad de almacenamiento, agregar capacidad de metadatos o agregar redundancia o nuevas capacidades.

Siga los pasos según el tipo de expansión que esté realizando:

Agregar volúmenes de almacenamiento

Siga los pasos para ["Agregar volúmenes de almacenamiento a los nodos de almacenamiento"](#) .

Agregar nodos de cuadrícula

1. Siga los pasos para ["Agregar nodos de cuadrícula a un sitio existente"](#) .
2. ["Actualizar las subredes"](#) .
3. Implementar nodos de cuadrícula:
 - ["Accesorios"](#)
 - ["VMware"](#)
 - ["Linux"](#)



"Linux" se refiere a una implementación de Red Hat Enterprise Linux, Ubuntu o Debian. Para obtener una lista de las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp \(IMT\)"](#) .

4. ["Realizar la expansión"](#) .
5. ["Configurar el sistema expandido"](#) .

Añadir nuevo sitio

1. Siga los pasos para ["Agregar un nuevo sitio"](#) .
2. ["Actualizar las subredes"](#) .
3. Implementar nodos de cuadrícula:
 - ["Accesorios"](#)
 - ["VMware"](#)
 - ["Linux"](#)



"Linux" se refiere a una implementación de Red Hat Enterprise Linux, Ubuntu o Debian. Para obtener una lista de las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp \(IMT\)"](#) .

4. ["Realizar la expansión"](#) .
5. ["Configurar el sistema expandido"](#) .

Plan de expansión de StorageGRID

Añadir capacidad de almacenamiento

Pautas para agregar capacidad de objetos

Puede ampliar la capacidad de almacenamiento de objetos de su sistema StorageGRID agregando volúmenes de almacenamiento a los nodos de almacenamiento existentes o agregando nuevos nodos de almacenamiento a los sitios existentes. Debe agregar capacidad de almacenamiento de una manera que cumpla con los requisitos de su

política de gestión del ciclo de vida de la información (ILM).

Pautas para agregar volúmenes de almacenamiento

Antes de agregar volúmenes de almacenamiento a los nodos de almacenamiento existentes, revise las siguientes pautas y limitaciones:

- Debe examinar sus reglas ILM actuales para determinar dónde y cuándo ["agregar volúmenes de almacenamiento"](#) para aumentar el almacenamiento disponible para ["objetos replicados"](#) o ["objetos codificados por borrado"](#).
- No puede aumentar la capacidad de metadatos de su sistema agregando volúmenes de almacenamiento porque los metadatos de los objetos se almacenan solo en el volumen 0.
- Cada nodo de almacenamiento basado en software puede admitir un máximo de 48 volúmenes de almacenamiento. Si necesita agregar capacidad más allá de eso, debe agregar nuevos nodos de almacenamiento.
- Puede agregar uno o dos estantes de expansión a cada electrodoméstico SG6060. Cada estante de expansión agrega 16 volúmenes de almacenamiento. Con ambos estantes de expansión instalados, el SG6060 puede admitir un total de 48 volúmenes de almacenamiento.
- Puede agregar uno o dos estantes de expansión a cada electrodoméstico SG6160. Cada estante de expansión agrega 60 volúmenes de almacenamiento. Con ambos estantes de expansión instalados, el SG6160 puede admitir un total de 180 volúmenes de almacenamiento.
- No puedes agregar volúmenes de almacenamiento a ningún otro dispositivo de almacenamiento.
- No se puede aumentar el tamaño de un volumen de almacenamiento existente.
- No se pueden agregar volúmenes de almacenamiento a un nodo de almacenamiento al mismo tiempo que se realiza una actualización del sistema, una operación de recuperación u otra expansión.

Una vez que haya decidido agregar volúmenes de almacenamiento y haya determinado qué nodos de almacenamiento debe expandir para satisfacer su política de ILM, siga las instrucciones para su tipo de nodo de almacenamiento:

- Para agregar uno o dos estantes de expansión a un dispositivo de almacenamiento SG6060, vaya a ["Agregar estante de expansión al SG6060 implementado"](#).
- Para agregar uno o dos estantes de expansión a un dispositivo de almacenamiento SG6160, vaya a ["Agregar estante de expansión al SG6160 implementado"](#).
- Para un nodo basado en software, siga las instrucciones para ["Agregar volúmenes de almacenamiento a los nodos de almacenamiento"](#).

Pautas para agregar nodos de almacenamiento

Antes de agregar nodos de almacenamiento a sitios existentes, revise las siguientes pautas y limitaciones:

- Debe examinar sus reglas ILM actuales para determinar dónde y cuándo agregar nodos de almacenamiento para aumentar el almacenamiento disponible. ["objetos replicados"](#) o ["objetos codificados por borrado"](#).
- No debe agregar más de 10 nodos de almacenamiento en un solo procedimiento de expansión.
- Puede agregar nodos de almacenamiento a más de un sitio en un solo procedimiento de expansión.
- Puede agregar nodos de almacenamiento y otros tipos de nodos en un solo procedimiento de expansión.
- Antes de iniciar el procedimiento de expansión, debe confirmar que se hayan completado todas las operaciones de reparación de datos realizadas como parte de una recuperación. Ver ["Comprobar trabajos"](#).

[de reparación de datos](#)" .

- Si necesita eliminar nodos de almacenamiento antes o después de realizar una expansión, no debe dismantelar más de 10 nodos de almacenamiento en un solo procedimiento de dismantelamiento de nodos.

Directrices para el servicio ADC en nodos de almacenamiento

Al configurar la expansión, debe elegir si desea incluir el servicio del Controlador de dominio administrativo (ADC) en cada nuevo Nodo de almacenamiento. El servicio ADC realiza un seguimiento de la ubicación y la disponibilidad de los servicios de la red.

- El sistema StorageGRID requiere un ["quórum de servicios de ADC"](#) estar disponible en cada sitio 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. Incluir demasiados servicios ADC puede provocar ralentizaciones debido a la mayor cantidad de comunicación entre nodos.
- Una sola red 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, cuando selecciona la configuración **Servicio ADC** para un nuevo nodo, debe seleccionar **Automático**. Seleccione **Sí** solo si el nuevo nodo reemplazará otro nodo de almacenamiento que incluye el servicio ADC. Dado que no se puede dismantelar un nodo de almacenamiento si quedan muy pocos servicios ADC, esto garantiza que haya un nuevo servicio ADC disponible antes de que se elimine el servicio anterior.
- No se puede agregar el servicio ADC a un nodo después de implementarlo.

Agregar capacidad de almacenamiento para objetos replicados

Si la política de administración del ciclo de vida de la información (ILM) para su implementación incluye una regla que crea copias replicadas de objetos, debe considerar cuánto almacenamiento agregar y dónde agregar los nuevos volúmenes de almacenamiento o nodos de almacenamiento.

Para obtener orientación sobre dónde agregar almacenamiento adicional, examine las reglas de ILM que crean copias replicadas. Si las reglas de ILM crean dos o más copias de objetos, planifique agregar almacenamiento en cada ubicación donde se realicen copias de objetos. Como ejemplo simple, si tiene una cuadrícula de dos sitios y una regla ILM que crea una copia de objeto en cada sitio, debe [añadir almacenamiento](#) a cada sitio para aumentar la capacidad general de objetos de la red. Para obtener información sobre la replicación de objetos, consulte ["¿Qué es la replicación?"](#) .

Por razones de rendimiento, debe intentar mantener la capacidad de almacenamiento y la potencia de procesamiento equilibradas entre los sitios. Entonces, para este ejemplo, debe agregar la misma cantidad de nodos de almacenamiento a cada sitio o volúmenes de almacenamiento adicionales en cada sitio.

Si tiene una política ILM más compleja que incluye reglas que colocan objetos en diferentes ubicaciones según criterios como el nombre del depósito, o reglas que cambian las ubicaciones de los objetos con el tiempo, su análisis de dónde se requiere almacenamiento para la expansión será similar, pero más complejo.

Graficar la velocidad con la que se consume la capacidad de almacenamiento general puede ayudarle a comprender cuánto almacenamiento agregar en la expansión y cuándo será necesario el espacio de almacenamiento adicional. Puede utilizar el Administrador de cuadrícula para ["Capacidad de almacenamiento de monitores y gráficos"](#) .

Al planificar el momento de una expansión, recuerde tener en cuenta cuánto tiempo podría llevar adquirir e instalar almacenamiento adicional.

Añadir capacidad de almacenamiento para objetos con código de borrado

Si su política de ILM incluye una regla que realiza copias con código de borrado, debe planificar dónde y cuándo agregar nuevo almacenamiento. La cantidad de almacenamiento que agregue y el momento de la adición pueden afectar la capacidad de almacenamiento utilizable de la red.

El primer paso para planificar una expansión de almacenamiento es examinar las reglas en su política ILM que crean objetos con código de borrado. Debido a que StorageGRID crea $k+m$ fragmentos para cada objeto con código de borrado y almacena cada fragmento en un nodo de almacenamiento diferente, debe asegurarse de que al menos $k+m$ nodos de almacenamiento tengan espacio para nuevos datos con código de borrado después de la expansión. Si el perfil de codificación de borrado proporciona protección contra pérdida de sitio, debe agregar almacenamiento a cada sitio. Ver "[¿Qué son los esquemas de codificación de borrado?](#)" para obtener información sobre los perfiles de codificación de borrado.

La cantidad de nodos que necesita agregar también depende de qué tan llenos estén los nodos existentes cuando realice la expansión.

Recomendación general para agregar capacidad de almacenamiento para objetos con código de borrado

Si desea evitar cálculos detallados, puede agregar dos nodos de almacenamiento por sitio cuando los nodos de almacenamiento existentes alcancen el 70 % de su capacidad.

Esta recomendación general proporciona resultados razonables en una amplia gama de esquemas de codificación de borrado tanto para redes de un solo sitio como para redes en las que la codificación de borrado proporciona protección contra pérdida de sitios.

Para comprender mejor los factores que llevaron a esta recomendación o para desarrollar un plan más preciso para su sitio, consulte "[Consideraciones para reequilibrar los datos codificados por borrado](#)". Para obtener una recomendación personalizada optimizada para su situación, comuníquese con su consultor de Servicios Profesionales de NetApp .

Consideraciones para reequilibrar los datos codificados por borrado

Si está realizando una expansión para agregar nodos de almacenamiento y usa reglas ILM para borrar datos de código, es posible que deba realizar el procedimiento de reequilibrio de codificación de borrado (EC) si no puede agregar suficientes nodos de almacenamiento para el esquema de codificación de borrado que está usando.

Después de revisar estas consideraciones, realice la expansión y luego vaya a "[Reequilibrar los datos codificados por borrado después de agregar nodos de almacenamiento](#)" para ejecutar el procedimiento.

¿Qué es el reequilibrio CE?

El reequilibrio de EC es un procedimiento de StorageGRID que podría ser necesario después de una expansión de un nodo de almacenamiento. El procedimiento se ejecuta como un script de línea de comandos desde el nodo de administración principal. Cuando ejecuta el procedimiento de reequilibrio de EC, StorageGRID redistribuye los fragmentos codificados por borrado entre los nodos de almacenamiento existentes y los recientemente agregados en un sitio.

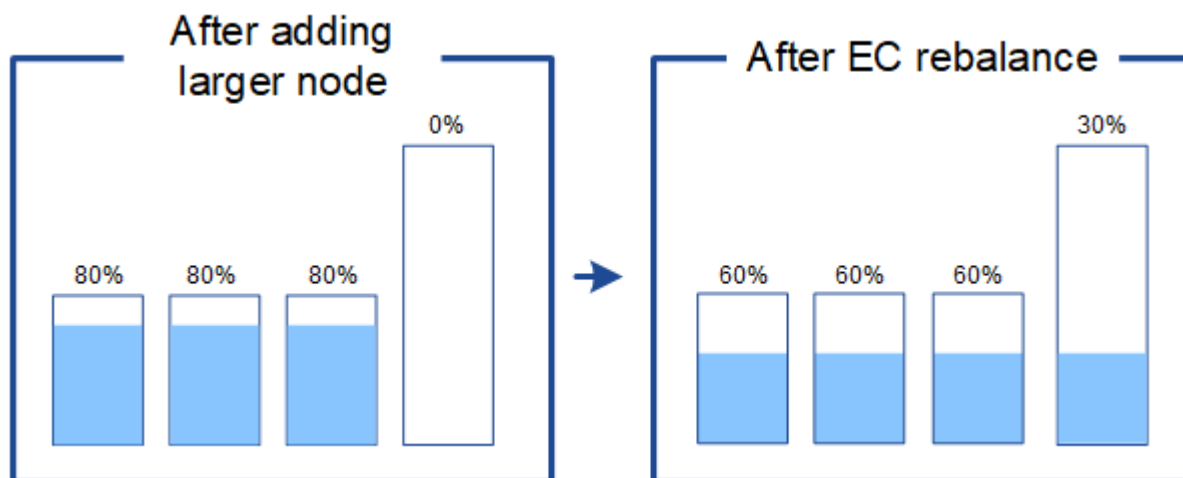
El procedimiento de reequilibrio de la CE:

- Solo mueve datos de objetos codificados por borrado. No mueve datos de objetos replicados.
- Redistribuye los datos dentro de un sitio. No mueve datos entre sitios.
- Redistribuye datos entre todos los nodos de almacenamiento de un sitio. No redistribuye datos dentro de los volúmenes de almacenamiento.
- No tiene en cuenta el uso de datos replicados en cada nodo de almacenamiento al determinar dónde mover los datos codificados por borrado.
- Redistribuye los datos codificados por borrado de manera uniforme entre los nodos de almacenamiento sin tener en cuenta las capacidades relativas de cada nodo.
- No distribuirá datos codificados por borrado a nodos de almacenamiento que estén llenos en más del 80 %.
- Podría disminuir el rendimiento de las operaciones de ILM y de las operaciones del cliente S3 cuando se ejecuta; se requieren recursos adicionales para redistribuir los fragmentos de codificación de borrado.

Una vez completado el procedimiento de reequilibrio de la CE:

- Los datos codificados por borrado se habrán movido de los nodos de almacenamiento con menos espacio disponible a los nodos de almacenamiento con más espacio disponible.
- La protección de datos de los objetos con código de borrado no se verá afectada.
- Los valores usados (%) pueden ser diferentes entre los nodos de almacenamiento por dos motivos:
 - Las copias de objetos replicados continuarán consumiendo espacio en los nodos existentes; el procedimiento de reequilibrio de EC no mueve los datos replicados.
 - Los nodos de mayor capacidad estarán relativamente menos llenos que los de menor capacidad, aunque todos los nodos terminarán con aproximadamente la misma cantidad de datos codificados por borrado.

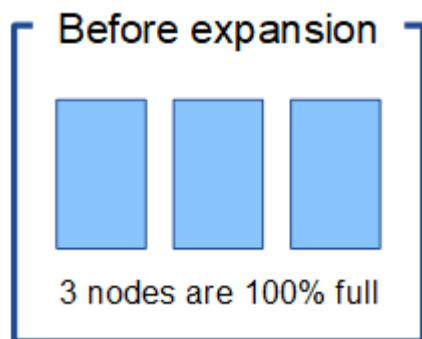
Por ejemplo, supongamos que tres nodos de 200 TB están llenos al 80 % cada uno ($200 \times 0,8 = 160$ TB en cada nodo o 480 TB para el sitio). Si agrega un nodo de 400 TB y ejecuta el procedimiento de reequilibrio, todos los nodos tendrán ahora aproximadamente la misma cantidad de datos de código de borrado ($480/4 = 120$ TB). Sin embargo, el Usado (%) para el nodo más grande será menor que el Usado (%) para los nodos más pequeños.



Cuándo reequilibrar los datos codificados por borrado

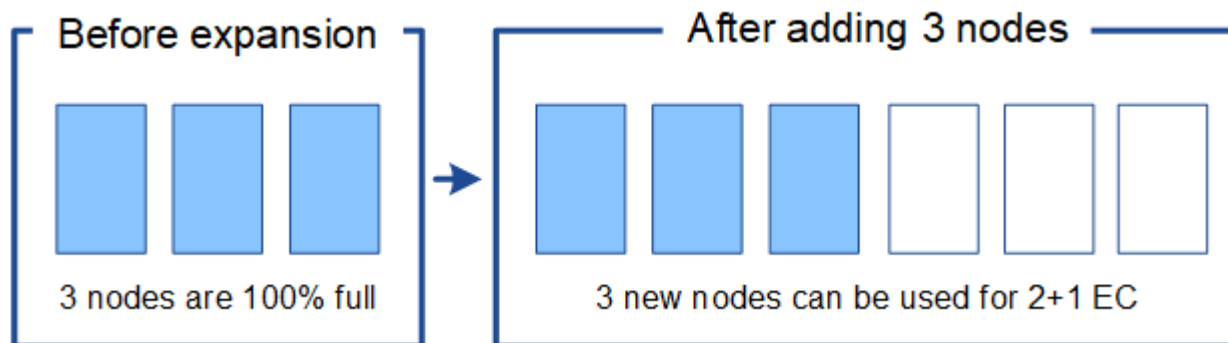
Consideremos el siguiente escenario:

- StorageGRID se ejecuta en un solo sitio, que contiene tres nodos de almacenamiento.
- La política ILM utiliza una regla de codificación de borrado 2+1 para todos los objetos mayores a 1,0 MB y una regla de replicación de 2 copias para objetos más pequeños.
- Todos los nodos de almacenamiento se han llenado completamente. La alerta **Almacenamiento de objetos bajo** se ha activado en el nivel de gravedad mayor.



No es necesario reequilibrar si se agregan suficientes nodos

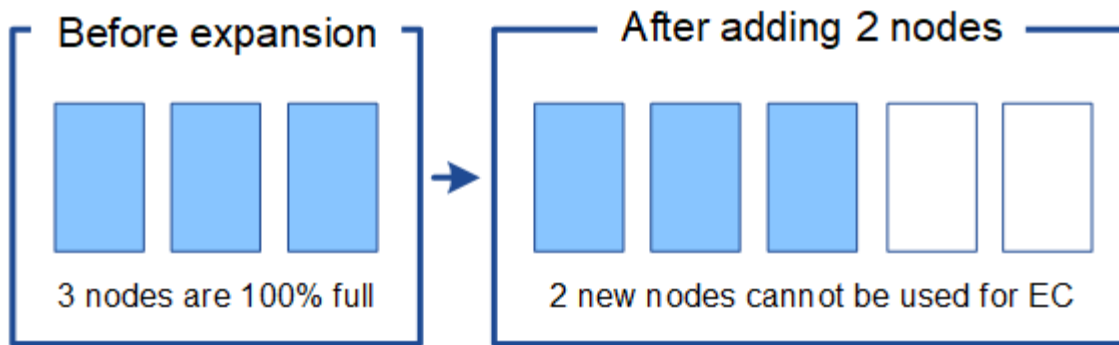
Para comprender cuándo no es necesario reequilibrar EC, supongamos que agregó tres (o más) nodos de almacenamiento nuevos. En este caso, no es necesario realizar un reequilibrio de CE. Los nodos de almacenamiento originales permanecerán llenos, pero los nuevos objetos ahora usarán los tres nuevos nodos para la codificación de borrado 2+1: los dos fragmentos de datos y el fragmento de paridad se pueden almacenar en un nodo diferente.



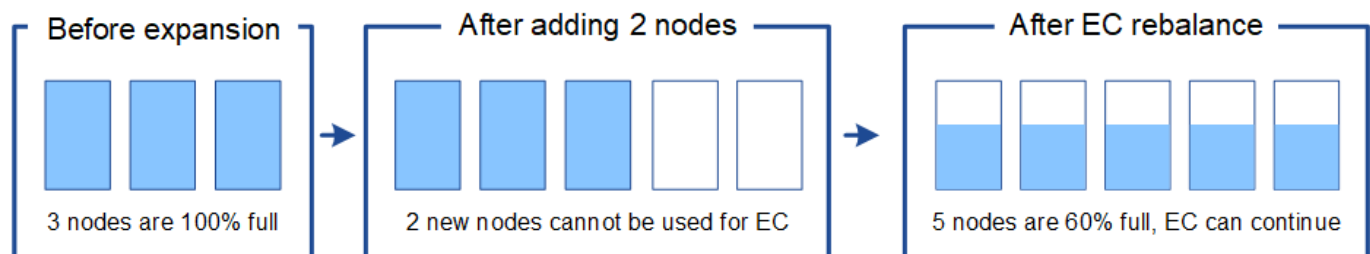
Si bien puede ejecutar el procedimiento de reequilibrio de EC en este caso, mover los datos codificados por borrado existentes disminuirá temporalmente el rendimiento de la red, lo que podría afectar las operaciones del cliente.

Se requiere reequilibrio si no puede agregar suficientes nodos

Para comprender cuándo es necesario reequilibrar la CE, supongamos que solo puede agregar dos nodos de almacenamiento, en lugar de tres. Debido a que el esquema 2+1 requiere que al menos tres nodos de almacenamiento tengan espacio disponible, los nodos vacíos no se pueden usar para nuevos datos codificados por borrado.



Para utilizar los nuevos nodos de almacenamiento, debe ejecutar el procedimiento de reequilibrio de EC. Cuando se ejecuta este procedimiento, StorageGRID redistribuye los datos codificados por borrado y los fragmentos de paridad existentes 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 solo al 60 % de su capacidad y los objetos pueden seguir ingiriéndose en el esquema de codificación de borrado 2+1 en todos los nodos de almacenamiento.



Recomendaciones para el reequilibrio de la CE

NetApp requiere el reequilibrio de EC si *todas* las siguientes afirmaciones son verdaderas:

- Utilice codificación de borrado para los datos de sus objetos.
- Se ha activado la alerta **Almacenamiento de objetos bajo** para uno o más nodos de almacenamiento en un sitio, lo que indica que los nodos están llenos en un 80 % o más.
- No puede agregar suficientes nodos de almacenamiento nuevos para el esquema de codificación de borrado en uso. Ver "[Añadir capacidad de almacenamiento para objetos con código de borrado](#)".
- Sus clientes S3 pueden tolerar un menor rendimiento en sus operaciones de escritura y lectura mientras se ejecuta el procedimiento de reequilibrio de EC.

Opcionalmente, puede ejecutar el procedimiento de reequilibrio de EC si prefiere que los nodos de almacenamiento se llenen a niveles similares y sus clientes S3 puedan tolerar un menor rendimiento para sus operaciones de escritura y lectura mientras se ejecuta el procedimiento de reequilibrio de EC.

Cómo interactúa el procedimiento de reequilibrio de la CE con otras tareas de mantenimiento

No es posible realizar determinados procedimientos de mantenimiento al mismo tiempo que se ejecuta el procedimiento de reequilibrio de CE.

Procedimiento	¿Permitido durante el procedimiento de reequilibrio de la CE?
Procedimientos adicionales de reequilibrio de la CE	No. Solo se puede ejecutar un procedimiento de reequilibrio de CE a la vez.
Procedimiento de desmantelamiento Trabajo de reparación de datos de la CE	No. • No se le permite iniciar un procedimiento de desmantelamiento o una reparación de datos de EC mientras se ejecuta el procedimiento de reequilibrio de EC. • No se le permite iniciar el procedimiento de reequilibrio de EC mientras se está ejecutando un procedimiento de desmantelamiento de un nodo de almacenamiento o una reparación de datos de EC.
Procedimiento de expansión	No. Si necesita agregar nuevos nodos de almacenamiento en una expansión, ejecute el procedimiento de reequilibrio de EC después de agregar todos los nodos nuevos.
Procedimiento de actualización	No. Si necesita actualizar el software StorageGRID , realice el procedimiento de actualización antes o después de ejecutar el procedimiento de reequilibrio de EC. Según sea necesario, puede finalizar el procedimiento de reequilibrio de CE para realizar una actualización de software.
Procedimiento de clonación del nodo del dispositivo	No. Si necesita clonar un nodo de almacenamiento del dispositivo, ejecute el procedimiento de reequilibrio de EC después de agregar el nuevo nodo.
Procedimiento de revisión urgente	Sí. Puede aplicar una revisión de StorageGRID mientras se ejecuta el procedimiento de reequilibrio de EC.
Otros procedimientos de mantenimiento	No. Debe finalizar el procedimiento de reequilibrio de CE antes de ejecutar otros procedimientos de mantenimiento.

Cómo interactúa el procedimiento de reequilibrio de la CE con el ILM

Mientras se ejecuta el procedimiento de reequilibrio de EC, evite realizar cambios en ILM que puedan cambiar la ubicación de los objetos con código de borrado existentes. Por ejemplo, no comience a utilizar una regla ILM que tenga un perfil de codificación de borrado diferente. Si necesita realizar dichos cambios en ILM, debe finalizar el procedimiento de reequilibrio de EC.

Añadir capacidad de metadatos

Para garantizar que haya suficiente espacio disponible para los metadatos de los objetos, es posible que deba realizar un procedimiento de expansión para agregar nuevos nodos de almacenamiento en cada sitio.

StorageGRID reserva espacio para metadatos de objetos en el volumen 0 de cada nodo de almacenamiento. Se mantienen tres copias de todos los metadatos de los objetos en cada sitio, distribuidas uniformemente entre todos los nodos de almacenamiento.

Puede utilizar el Administrador de cuadrícula para supervisar la capacidad de metadatos de los nodos de almacenamiento y para estimar la velocidad con la que se consume dicha capacidad de metadatos. Además, la alerta **Almacenamiento de metadatos bajo** se activa para un nodo de almacenamiento cuando el espacio de metadatos utilizado alcanza ciertos umbrales.

Tenga en cuenta que la capacidad de metadatos de objetos de una cuadrícula puede consumirse más rápido que su capacidad de almacenamiento de objetos, dependiendo de cómo utilice la cuadrícula. Por ejemplo, si normalmente ingiere grandes cantidades de objetos pequeños o agrega grandes cantidades de metadatos de usuario o etiquetas a los objetos, es posible que necesite agregar nodos de almacenamiento para aumentar la capacidad de metadatos incluso aunque todavía quede suficiente capacidad de almacenamiento de objetos.

Para obtener más información, consulte lo siguiente:

- ["Administrar el almacenamiento de metadatos de objetos"](#)
- ["Supervisar la capacidad de metadatos de objetos para cada nodo de almacenamiento"](#)

Directrices para aumentar la capacidad de metadatos

Antes de agregar nodos de almacenamiento para aumentar la capacidad de metadatos, revise las siguientes pautas y limitaciones:

- Suponiendo que hay suficiente capacidad de almacenamiento de objetos disponible, tener más espacio disponible para metadatos de objetos aumenta la cantidad de objetos que puede almacenar en su sistema StorageGRID .
- Puede aumentar la capacidad de metadatos de una red agregando uno o más nodos de almacenamiento a cada sitio.
- El espacio real reservado para los metadatos de objetos en cualquier nodo de almacenamiento determinado depende de la opción de almacenamiento Espacio reservado para metadatos (configuración de todo el sistema), la cantidad de RAM asignada al nodo y el tamaño del volumen del nodo 0.
- No es posible aumentar la capacidad de metadatos agregando volúmenes de almacenamiento a los nodos de almacenamiento existentes, porque los metadatos se almacenan solo en el volumen 0.
- No es posible aumentar la capacidad de metadatos agregando un nuevo sitio.
- StorageGRID mantiene tres copias de todos los metadatos de los objetos en cada sitio. Por este motivo, la capacidad de metadatos de su sistema está limitada por la capacidad de metadatos de su sitio más pequeño.
- Al agregar capacidad de metadatos, debe agregar la misma cantidad de nodos de almacenamiento a cada sitio.

Los nodos de almacenamiento de solo metadatos tienen requisitos de hardware específicos:

- Al utilizar dispositivos StorageGRID , los nodos de solo metadatos se pueden configurar únicamente en

dispositivos SGF6112 con doce unidades de 1,9 TB o doce unidades de 3,8 TB.

- Al utilizar nodos basados en software, los recursos de nodo de solo metadatos deben coincidir con los recursos de los nodos de almacenamiento existentes. Por ejemplo:
 - Si el sitio StorageGRID existente utiliza dispositivos SG6000 o SG6100, los nodos de solo metadatos basados en software deben cumplir los siguientes requisitos mínimos:
 - 128 GB de RAM
 - CPU de 8 núcleos
 - SSD de 8 TB o almacenamiento equivalente para la base de datos Cassandra (rangedb/0)
 - Si el sitio StorageGRID existente usa nodos de almacenamiento virtuales con 24 GB de RAM, CPU de 8 núcleos y 3 TB o 4 TB de almacenamiento de metadatos, los nodos solo de metadatos basados en software deben usar recursos similares (24 GB de RAM, CPU de 8 núcleos y 4 TB de almacenamiento de metadatos (rangedb/0)).
- Al agregar un nuevo sitio StorageGRID , la capacidad total de metadatos del nuevo sitio debe coincidir, como mínimo, con los sitios StorageGRID existentes y los recursos del nuevo sitio deben coincidir con los nodos de almacenamiento de los sitios StorageGRID existentes.

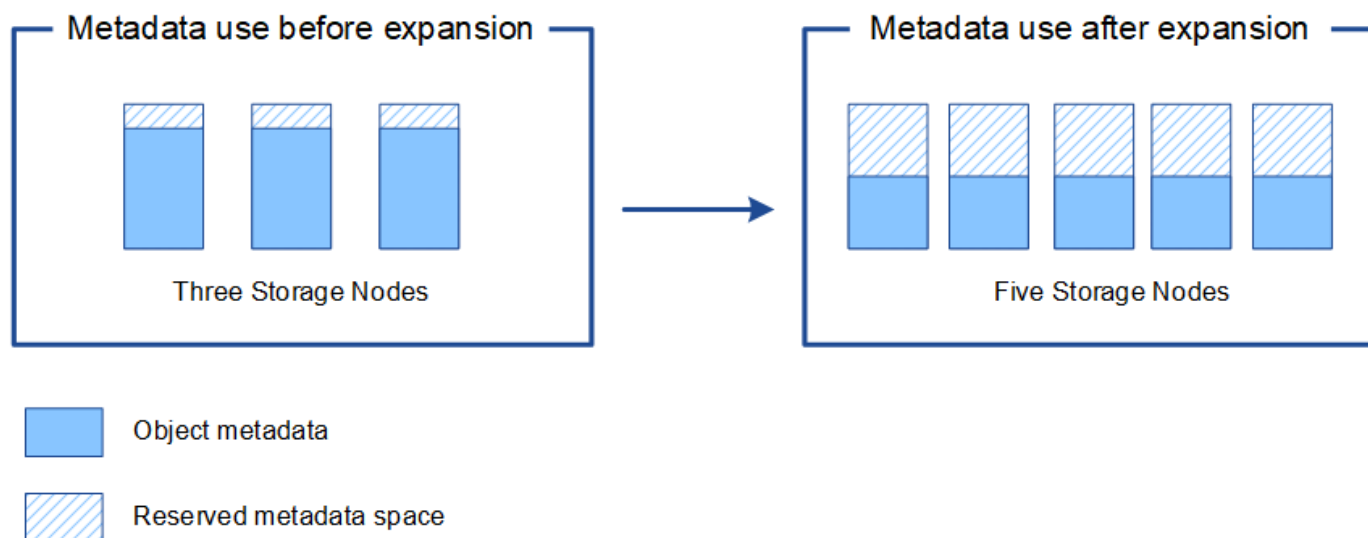
Ver el ["Descripción de qué es el Espacio Reservado de Metadatos"](#) .

Cómo se redistribuyen los metadatos al agregar nodos de almacenamiento

Cuando agrega nodos de almacenamiento en una expansión, StorageGRID redistribuye los metadatos de los objetos existentes a los nuevos nodos en cada sitio, lo que aumenta la capacidad general de metadatos de la red. No se requiere ninguna acción del usuario.

La siguiente figura muestra cómo StorageGRID redistribuye los metadatos de los objetos cuando se agregan nodos de almacenamiento en una expansión. El lado izquierdo de la figura representa el volumen 0 de tres nodos de almacenamiento antes de una expansión. Los metadatos están consumiendo una porción 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 que se agregan 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 el espacio disponible para metadatos ha aumentado.



Agregue nodos de red para agregar capacidades a su sistema

Puede agregar redundancia o capacidades adicionales a un sistema StorageGRID agregando nuevos nodos de red a sitios existentes.

Por ejemplo, puede optar por agregar nodos de puerta de enlace para usar en un grupo de alta disponibilidad (HA), o puede agregar un nodo de administración en un sitio remoto para permitir el monitoreo mediante un nodo local.

Puede agregar uno o más de los siguientes tipos de nodos a uno o más sitios existentes en una sola operación de expansión:

- Nodos de administración no principales
- Nodos de almacenamiento
- Nodos de puerta de enlace

Al prepararse para agregar nodos de cuadrícula, tenga en cuenta las siguientes limitaciones:

- El nodo de administración principal se implementa durante la instalación inicial. No se puede agregar un nodo de administración principal durante una expansión.
- Puede agregar nodos de almacenamiento y otros tipos de nodos en la misma expansión.
- Al agregar nodos de almacenamiento, debe planificar cuidadosamente la cantidad y la ubicación de los nuevos nodos. Ver ["Pautas para agregar capacidad de objetos"](#).
- Si la opción **Establecer nuevo nodo predeterminado** es **No confiable** en la pestaña Redes de cliente no confiables en la página Control de firewall, las aplicaciones cliente que se conectan a nodos de expansión mediante la Red de cliente deben conectarse mediante un puerto de punto final del balanceador de carga (**CONFIGURACIÓN > Seguridad > Control de firewall**). Vea las instrucciones para ["cambiar la configuración de seguridad para el nuevo nodo"](#) y a ["Configurar los puntos finales del balanceador de carga"](#).

Agregar un nuevo sitio

Puede ampliar su sistema StorageGRID agregando un nuevo sitio.

Pautas para agregar un sitio

Antes de agregar un sitio, revise los siguientes requisitos y limitaciones:

- Sólo se puede agregar un sitio por operación de expansión.
- No se pueden agregar nodos de cuadrícula a un sitio existente como parte de la misma expansión.
- Todos los sitios deben incluir al menos tres nodos de almacenamiento.
- Agregar un nuevo sitio no aumenta automáticamente la cantidad de objetos que puede almacenar. La capacidad total de objetos de una red depende de la cantidad de almacenamiento disponible, la política ILM y la capacidad de metadatos en cada sitio.
- Al dimensionar un sitio nuevo, debe asegurarse de que incluya suficiente capacidad de metadatos.

StorageGRID mantiene una copia de todos los metadatos de los objetos en cada sitio. Al agregar un nuevo sitio, debe asegurarse de que incluya suficiente capacidad de metadatos para los metadatos de los objetos existentes y suficiente capacidad de metadatos para el crecimiento.

Para obtener más información, consulte lo siguiente:

- ["Administrar el almacenamiento de metadatos de objetos"](#)
- ["Supervisar la capacidad de metadatos de 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 la red. Las actualizaciones de metadatos se replican continuamente entre sitios incluso si todos los objetos se almacenan solo en el sitio donde se ingieren.
- Dado que su sistema StorageGRID permanece operativo durante la expansión, debe revisar las reglas de ILM antes de iniciar el procedimiento de expansión. Debe asegurarse de que las copias de objetos no se almacenen en el nuevo sitio hasta que se complete el procedimiento de expansión.

Por ejemplo, antes de comenzar la expansión, determine si alguna regla utiliza el grupo de almacenamiento predeterminado (Todos los nodos de almacenamiento). Si es así, debe crear un nuevo grupo de almacenamiento que contenga los nodos de almacenamiento existentes y actualizar sus reglas ILM para usar el nuevo grupo de almacenamiento. De lo contrario, los objetos se copiarán al nuevo sitio tan pronto como el primer nodo de ese sitio se active.

Para obtener más información sobre cómo cambiar ILM al agregar un nuevo sitio, consulte la ["Ejemplo de cambio de una política de ILM"](#).

Reúna los materiales necesarios

Antes de realizar una operación de expansión, reúna los materiales e instale y configure cualquier hardware y redes nuevas.

Artículo	Notas
Archivo de instalación de StorageGRID	Si está agregando nuevos nodos de red o un nuevo sitio, debe descargar y extraer el archivo de instalación de StorageGRID . Debe utilizar la misma versión que se ejecuta actualmente en la red. Para obtener más detalles, consulte las instrucciones para Descargar y extraer los archivos de instalación de StorageGRID . Nota: No es necesario descargar archivos si está agregando nuevos volúmenes de almacenamiento a nodos de almacenamiento existentes o instalando un nuevo dispositivo StorageGRID .
Servicio de computadora portátil	La computadora portátil de servicio tiene lo siguiente: • Puerto de red • Cliente SSH (por ejemplo, PuTTY) • "Navegador web compatible"
`Passwords.txt` archivo	Contiene las contraseñas necesarias para acceder a los nodos de la red en la línea de comando. Incluido en el paquete de recuperación.

Artículo	Notas
Frase de contraseña de aprovisionamiento	La frase de contraseña se crea y se documenta cuando se instala por primera vez el sistema StorageGRID . La frase de contraseña de aprovisionamiento no está en el <code>Passwords.txt</code> archivo.
Documentación de StorageGRID	• "Administrar StorageGRID" • "Notas de la versión" • Instrucciones de instalación para su plataforma ◦ "Instalar StorageGRID en Red Hat Enterprise Linux" ◦ "Instalar StorageGRID en Ubuntu o Debian" ◦ "Instalar StorageGRID en VMware"
Documentación actual para su plataforma	Para conocer las versiones compatibles, consulte la "Herramienta de matriz de interoperabilidad (IMT)" .

Descargue y extraiga los archivos de instalación de StorageGRID

[[descargar y extraer archivos de instalación]]

Antes de poder agregar nuevos nodos de red o un nuevo sitio, debe descargar el archivo de instalación de StorageGRID apropiado y extraer los archivos.

Acerca de esta tarea

Debe realizar operaciones de expansión utilizando la versión de StorageGRID que se esté ejecutando actualmente en la red.

Pasos

1. Ir a ["Descargas de NetApp : StorageGRID"](#) .
2. Seleccione la versión de StorageGRID que se está ejecutando actualmente en la red.
3. Sign in con el nombre de usuario y la contraseña de su cuenta de NetApp .
4. Lea el Acuerdo de licencia de usuario final, seleccione la casilla de verificación y luego seleccione **Aceptar y continuar**.
5. En la columna **Instalar StorageGRID** de la página de descarga, seleccione la opción `.tgz` o `.zip` archivo para su plataforma.

La versión que se muestra en el archivo de instalación debe coincidir con la versión del software que está instalado actualmente.

Utilice el `.zip` archivo si está ejecutando Windows en la computadora portátil de servicio.

Plataforma	Archivo de instalación
Red Hat Enterprise Linux	StorageGRID-Webscale- <i>version</i> -RPM- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -RPM- <i>uniqueID</i> .tgz

Plataforma	Archivo de instalación
Ubuntu o Debian o electrodomésticos	StorageGRID-Webscale- <i>version</i> -DEB- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -DEB- <i>uniqueID</i> .tgz
VMware	StorageGRID-Webscale- <i>version</i> -VMware- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -VMware- <i>uniqueID</i> .tgz
OpenStack/otro hipervisor	Para expandir una implementación existente en OpenStack, debe implementar una máquina virtual que ejecute una de las distribuciones de Linux compatibles enumeradas anteriormente y seguir las instrucciones adecuadas para Linux.

6. Descargue y extraiga el archivo comprimido.
7. Siga el paso apropiado para su plataforma para elegir los archivos que necesita, en función de su plataforma, la topología de red planificada y cómo expandirá su sistema StorageGRID .

Las rutas enumeradas en el paso para cada plataforma son relativas al directorio de nivel superior instalado por el archivo de almacenamiento.

8. Si está ampliando un sistema Red Hat Enterprise Linux, seleccione los archivos adecuados.

Ruta y nombre de archivo	Descripción
	Un 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.
	Paquete RPM para instalar el servicio de host StorageGRID en sus hosts RHEL.
Herramienta de scripting de implementación	Descripción
	Un script de Python utilizado para automatizar la configuración de un sistema StorageGRID .
	Un script de Python utilizado para automatizar la configuración de dispositivos StorageGRID .
	Un archivo de configuración de ejemplo para usar con el <code>configure-storagegrid.py</code> guion.

Ruta y nombre de archivo	Descripción
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único está habilitado. También puede utilizar este script para la integración de Ping Federate.
	Un archivo de configuración en blanco para usar con el <code>configure-storagegrid.py</code> guion.
	Ejemplo de rol y manual de Ansible para configurar hosts RHEL para la implementación de contenedores StorageGRID . Puede personalizar el rol o el libro de jugadas según sea necesario.
	Un ejemplo de secuencia de comandos de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script de ayuda llamado por el compañero <code>storagegrid-ssoauth-azure.py</code> Script de Python para realizar interacciones de SSO con Azure.
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno de StorageGRID que no sea de producción para realizar pruebas de compatibilidad de actualización.

1. Si está expandiendo un sistema Ubuntu o Debian, seleccione los archivos apropiados.

Ruta y nombre de archivo	Descripción
	Un 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 puede utilizar para realizar pruebas e implementaciones de prueba de concepto.
	Paquete DEB para instalar las imágenes del nodo StorageGRID en hosts Ubuntu o Debian.

Ruta y nombre de archivo	Descripción
	Suma de comprobación MD5 del archivo <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .
	Paquete DEB para instalar el servicio de host StorageGRID en hosts Ubuntu o Debian.
Herramienta de scripting de implementación	Descripción
	Un script de Python utilizado para automatizar la configuración de un sistema StorageGRID.
	Un script de Python utilizado para automatizar la configuración de dispositivos StorageGRID.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único está habilitado. También puede utilizar este script para la integración de Ping Federate.
	Un archivo de configuración de ejemplo para usar con el <code>configure-storagegrid.py</code> guion.
	Un archivo de configuración en blanco para usar con el <code>configure-storagegrid.py</code> guion.
	Ejemplo de rol y manual de estrategias de Ansible para configurar hosts Ubuntu o Debian para la implementación de contenedores StorageGRID. Puede personalizar el rol o el libro de jugadas según sea necesario.
	Un ejemplo de secuencia de comandos de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script de ayuda llamado por el compañero <code>storagegrid-ssoauth-azure.py</code> Script de Python para realizar interacciones de SSO con Azure.

Ruta y nombre de archivo	Descripción
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno de StorageGRID que no sea de producción para realizar pruebas de compatibilidad de actualización.

1. Si está expandiendo un sistema VMware, seleccione los archivos apropiados.

Ruta y nombre de archivo	Descripción
	Un 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 la máquina virtual que se utiliza como plantilla para crear máquinas virtuales de nodo de cuadrícula.
	El archivo de plantilla de formato de virtualización abierta(.ovf) y archivo de manifiesto(.mf) para implementar el nodo de administración principal.
	El archivo de plantilla(.ovf) y archivo de manifiesto(.mf) para implementar nodos de administración no principales.
	El archivo de plantilla(.ovf) y archivo de manifiesto(.mf) para implementar nodos de puerta de enlace.
	El archivo de plantilla(.ovf) y archivo de manifiesto(.mf) para implementar nodos de almacenamiento basados en máquinas virtuales.
Herramienta de scripting de implementación	Descripción
	Un script de shell Bash utilizado para automatizar la implementación de nodos de red virtuales.

Ruta y nombre de archivo	Descripción
	Un archivo de configuración de ejemplo para usar con el <code>deploy-vsphere-ovftool.sh</code> guion.
	Un script de Python utilizado para automatizar la configuración de un sistema StorageGRID .
	Un script de Python utilizado para automatizar la configuración de dispositivos StorageGRID .
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único (SSO) está habilitado. También puede utilizar este script para la integración de Ping Federate.
	Un archivo de configuración de ejemplo para usar con el <code>configure-storagegrid.py</code> guion.
	Un archivo de configuración en blanco para usar con el <code>configure-storagegrid.py</code> guion.
	Un ejemplo de secuencia de comandos de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script de ayuda llamado por el compañero <code>storagegrid-ssoauth-azure.py</code> Script de Python para realizar interacciones de SSO con Azure.
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno de StorageGRID que no sea de producción para realizar pruebas de compatibilidad de actualización.

1. Si está expandiendo un sistema basado en un dispositivo StorageGRID , seleccione los archivos apropiados.

Ruta y nombre de archivo	Descripción
	Paquete DEB para instalar las imágenes del nodo StorageGRID en sus dispositivos.
	Suma de comprobación MD5 del archivo /debs/storagegridwebscale- images-version-SHA.deb .



Para la instalación del dispositivo, estos archivos solo son necesarios si necesita evitar el tráfico de red. El dispositivo puede descargar los archivos necesarios desde el nodo de administración principal.

Verificar hardware y redes

Antes de comenzar la expansión de su sistema StorageGRID , asegúrese de lo siguiente:

- Se ha instalado y configurado el hardware necesario para soportar los nuevos nodos de la red o el nuevo sitio.
- Todos los nodos nuevos tienen rutas de comunicación bidireccionales hacia todos los nodos existentes y nuevos (un requisito para la red Grid). En particular, confirme que los siguientes puertos TCP estén abiertos entre los nuevos nodos que está agregando en la expansión y el nodo de administración principal:
 - 1055
 - 7443
 - 8011
 - 10342

Ver "[Comunicaciones internas de los nodos de la red](#)".

- El nodo de administración principal puede comunicarse con todos los servidores de expansión que estén destinados a alojar el sistema StorageGRID .
- Si alguno de los nuevos nodos tiene una dirección IP de red en una subred que no se utilizó anteriormente, ya la ha "[Se agregó la nueva subred](#)" a la lista de subredes de la red Grid. De lo contrario, tendrá que cancelar la expansión, agregar la nueva subred y comenzar el procedimiento nuevamente.
- No está utilizando la traducción de direcciones de red (NAT) en la red Grid entre nodos Grid o entre sitios StorageGRID . Cuando se utilizan direcciones IPv4 privadas para la red de cuadrícula, dichas direcciones deben ser enrutables directamente desde cada nodo de la red en cada sitio. El uso de NAT para unir la red de cuadrícula a través de un segmento de red pública solo es compatible si se utiliza una aplicación de tunelización que sea transparente para todos los nodos de la red, lo que significa que los nodos de la red no requieren conocimiento de direcciones IP públicas.

Esta restricción de NAT es específica para los nodos de la red y la red de la red. Según sea necesario, puede utilizar NAT entre clientes externos y nodos de la red, por ejemplo, para proporcionar una dirección IP pública para un nodo de puerta de enlace.

Agregar volúmenes de almacenamiento

Agregar volúmenes de almacenamiento a los nodos de almacenamiento

Puede ampliar la capacidad de almacenamiento de los nodos de almacenamiento que estén por debajo de la cantidad máxima de volúmenes admitida. Es posible que necesite agregar volúmenes de almacenamiento a más de un nodo de almacenamiento para satisfacer los requisitos de ILM para copias replicadas o codificadas por borrado.

Antes de empezar

Antes de agregar volúmenes de almacenamiento, revise la ["Pautas para agregar capacidad de objetos"](#) para asegurarse de saber dónde agregar volúmenes para cumplir con los requisitos de su política ILM.



Estas instrucciones se aplican únicamente a los nodos de almacenamiento basados en software. Ver ["Agregar estante de expansión al SG6060 implementado"](#) o ["Agregar estante de expansión al SG6160 implementado"](#) para aprender cómo agregar volúmenes de almacenamiento al SG6060 o SG6160 mediante la instalación de estantes de expansión. Los nodos de almacenamiento de otros dispositivos no se pueden expandir.

Acerca de esta tarea

El almacenamiento subyacente de un nodo de almacenamiento se divide en volúmenes de almacenamiento. Los volúmenes de almacenamiento son dispositivos de almacenamiento basados en bloques que son formateados por el sistema StorageGRID y montados para almacenar objetos. Cada nodo de almacenamiento puede admitir hasta 48 volúmenes de almacenamiento, que se denominan *almacenes de objetos* en el Administrador de cuadrícula.



Los metadatos de los 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 a la `/var/local/rangedb/0` punto de montaje.

Antes de agregar nuevos volúmenes de almacenamiento, utilice el Administrador de cuadrícula para ver los almacenes de objetos actuales para cada nodo de almacenamiento, así como los puntos de montaje correspondientes. Puede utilizar esta información al agregar volúmenes de almacenamiento.

Pasos

1. Seleccione **NODOS** > **sitio** > **Nodo de almacenamiento** > **Almacenamiento**.
2. Desplácese hacia abajo para ver las cantidades de almacenamiento disponible para cada volumen y almacén de objetos.

Para los nodos de almacenamiento del dispositivo, el nombre mundial de cada disco coincide con el identificador mundial del volumen (WWID) que aparece cuando se visualizan las propiedades del volumen estándar en SANtricity OS (el software de administración conectado al controlador de almacenamiento del dispositivo).

Para ayudarlo a interpretar las estadísticas de lectura y escritura del disco relacionadas con los puntos de montaje del volumen, la primera parte del nombre que se muestra 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 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 de su plataforma para agregar nuevos volúmenes de almacenamiento al nodo de almacenamiento.
 - ["VMware: Agregar volúmenes de almacenamiento al nodo de almacenamiento"](#)
 - ["Linux: Agregar volúmenes SAN o de conexión directa al nodo de almacenamiento"](#)

VMware: Agregar volúmenes de almacenamiento al nodo de almacenamiento

Si un nodo de almacenamiento incluye menos de 16 volúmenes de almacenamiento, puede aumentar su capacidad utilizando VMware vSphere para agregar volúmenes.

Antes de empezar

- Tiene acceso a las instrucciones para instalar StorageGRID para implementaciones de VMware.
 - ["Instalar StorageGRID en VMware"](#)
- Tú tienes el `Passwords.txt` archivo.
- Tienes ["permisos de acceso específicos"](#).



No intente agregar volúmenes de almacenamiento a un nodo de almacenamiento mientras esté activo una actualización de software, un procedimiento de recuperación u otro procedimiento de expansión.

Acerca de esta tarea

El nodo de almacenamiento no está disponible por un breve tiempo cuando se agregan volúmenes de almacenamiento. Debe realizar este procedimiento en un nodo de almacenamiento a la vez para evitar afectar los servicios de red que miran al cliente.

Pasos

1. Si es necesario, instale nuevo hardware de almacenamiento y cree nuevos almacenes de datos de VMware.
2. Agregue uno o más discos duros a la máquina virtual para usarlos como almacenamiento (almacenes de objetos).
 - a. Abra el cliente VMware vSphere.
 - b. Edite la configuración de la máquina virtual para agregar uno o más discos duros adicionales.

Los discos duros normalmente se configuran como discos de máquina virtual (VMDK). Los VMDK se utilizan con mayor frecuencia y son más fáciles de administrar, mientras que los RDM pueden proporcionar un mejor rendimiento para cargas de trabajo que utilizan tamaños de objetos más grandes (por ejemplo, más de 100 MB). Para obtener más información sobre cómo agregar discos duros a máquinas virtuales, consulte la documentación de VMware vSphere.

3. Reinicie la máquina virtual utilizando la opción **Reiniciar sistema operativo invitado** en VMware vSphere Client, o ingresando el siguiente comando en una sesión ssh en la máquina virtual: `sudo reboot`



No utilice **Apagar** o **Reiniciar** 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 la red:
 - i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`

- ii. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- iii. Introduzca el siguiente comando para cambiar a root: `su -`
- iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo. Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

b. Configurar los nuevos volúmenes de almacenamiento:

```
sudo add_rangedbs.rb
```

Este script encuentra todos los volúmenes de almacenamiento nuevos y le solicita que los formatee.

- c. Introduzca **y** para aceptar el formato.
- d. Si alguno de los volúmenes ha sido formateado previamente, decida si desea reformatearlo.
 - Introduzca **y** para reformatear.
 - Introduzca **n** para omitir el reformateo.

El `setup_rangedbs.sh` El script se ejecuta automáticamente.

5. Compruebe que los servicios se inician correctamente:

- a. Ver una lista del estado de todos los servicios en el servidor:

```
sudo storagegrid-status
```

El estado se actualiza automáticamente.

- a. Espere hasta que todos los servicios estén en ejecución o verificados.
- b. Salir de la pantalla de estado:

```
Ctrl+C
```

6. Verifique que el nodo de almacenamiento esté en línea:

- a. Sign in en Grid Manager usando un ["navegador web compatible"](#).
- b. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
- c. Seleccione **sítio > Nodo de almacenamiento > LDR > Almacenamiento**.
- d. Seleccione la pestaña **Configuración** y luego la pestaña **Principal**.
- e. Si la lista desplegable **Estado de almacenamiento - Deseado** está configurada en Solo lectura o Sin conexión, seleccione **En línea**.
- f. Seleccione **Aplicar cambios**.

7. Para ver los nuevos almacenes de objetos:

- a. Seleccione **NODOS > sitio > Nodo de almacenamiento > Almacenamiento**.
- b. Vea los detalles en la tabla **Almacenes de objetos**.

Resultado

Puede utilizar la capacidad ampliada de los nodos de almacenamiento para guardar datos de objetos.

Linux: Agregar volúmenes SAN o de conexión directa al nodo de almacenamiento

Si un nodo de almacenamiento incluye menos de 48 volúmenes de almacenamiento, puede aumentar su capacidad agregando nuevos dispositivos de almacenamiento en bloque, haciéndolos visibles para los hosts de Linux y agregando las nuevas asignaciones de dispositivos de bloque al archivo de configuración StorageGRID utilizado para el nodo de almacenamiento.

Antes de empezar

- Tiene acceso a las instrucciones para instalar StorageGRID para su plataforma Linux.
 - ["Instalar StorageGRID en Red Hat Enterprise Linux"](#)
 - ["Instalar StorageGRID en Ubuntu o Debian"](#)
- Tú tienes el `Passwords.txt` archivo.
- Tienes ["permisos de acceso específicos"](#) .



No intente agregar volúmenes de almacenamiento a un nodo de almacenamiento mientras esté activo una actualización de software, un procedimiento de recuperación u otro procedimiento de expansión.

Acerca de esta tarea

El nodo de almacenamiento no está disponible por un breve tiempo cuando se agregan volúmenes de almacenamiento. Debe realizar este procedimiento en un nodo de almacenamiento a la vez para evitar afectar los servicios de red que miran 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 bloque de los tamaños deseados.
 - Conecte las nuevas unidades y actualice la configuración del controlador RAID según sea necesario, o asigne los nuevos LUN SAN en las matrices de almacenamiento compartido y permita que el host Linux acceda a ellos.
 - Utilice el mismo esquema de nombres persistente que utilizó para los volúmenes de almacenamiento en el nodo de almacenamiento existente.
 - Si utiliza la función de migración de nodo StorageGRID , haga que los nuevos volúmenes sean visibles para otros hosts Linux que sean destinos de migración para este nodo de almacenamiento. Para obtener más información, consulte las instrucciones para instalar StorageGRID para su plataforma Linux.
3. Inicie sesión en el host Linux que admite el nodo de almacenamiento como root o con una cuenta que tenga permiso sudo.
4. Confirme que los nuevos volúmenes de almacenamiento sean visibles en el host Linux.

Es posible que tengas que volver a buscar dispositivos.

5. Ejecute el siguiente comando para deshabilitar temporalmente el nodo de almacenamiento:

```
sudo storagegrid node stop <node-name>
```

6. Usando un editor de texto como vim o pico, edite el archivo de configuración del nodo de almacenamiento, que se puede encontrar en `/etc/storagegrid/nodes/<node-name>.conf`.
7. Localice la sección del archivo de configuración del nodo que contiene las asignaciones de dispositivos de bloque de almacenamiento de objetos existentes.

En el ejemplo, `BLOCK_DEVICE_RANGEDB_00` a `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. Agregue nuevas asignaciones de dispositivos de bloques de almacenamiento de objetos correspondientes a los volúmenes de almacenamiento de bloques que agregó para este nodo de almacenamiento.

Asegúrate de empezar en el siguiente `BLOCK_DEVICE_RANGEDB_nn`. No dejes ningún espacio

- Basándonos en el ejemplo anterior, comencemos en `BLOCK_DEVICE_RANGEDB_04`.
- En el siguiente ejemplo, se han agregado cuatro nuevos volúmenes de almacenamiento en bloque al nodo: `BLOCK_DEVICE_RANGEDB_04` a `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 de almacenamiento:

```
sudo storagegrid node validate <node-name>
```

Aborde cualquier error o advertencia antes de continuar con el siguiente paso.

Si observa un error similar al siguiente, significa que el archivo de configuración del nodo está intentando mapear el dispositivo de bloque utilizado por <node-name> para <PURPOSE> a lo dado <path-name> en el sistema de archivos de Linux, pero no hay un archivo especial de dispositivo de bloque válido (o un enlace simbólico 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

```

Verifique que haya ingresado la información correcta <path-name> .

10. Ejecute el siguiente comando para reiniciar el nodo con las nuevas asignaciones de dispositivos de bloque en su lugar:

```
sudo storagegrid node start <node-name>
```

11. Inicie sesión en el nodo de almacenamiento como administrador usando la contraseña que aparece en el Passwords.txt archivo.
12. Compruebe que los servicios se inician correctamente:
 - a. Ver una lista del estado de todos los servicios en el servidor:

```
sudo storagegrid-status
```

El estado se actualiza automáticamente.

- b. Espere hasta que todos los servicios estén en ejecución o verificados.
- c. Salir de la pantalla de estado:

```
Ctrl+C
```

13. Configure el nuevo almacenamiento para que lo utilice el nodo de almacenamiento:

- a. Configurar los nuevos volúmenes de almacenamiento:

```
sudo add_rangedbs.rb
```

Este script encuentra todos los volúmenes de almacenamiento nuevos y le solicita que los formatee.

- b. Ingrese **y** para formatear los volúmenes de almacenamiento.
- c. Si alguno de los volúmenes ha sido formateado previamente, decida si desea reformatearlo.
 - Introduzca **y** para reformatear.
 - Introduzca **n** para omitir el reformateo.

El `setup_rangedbs.sh` El script se ejecuta automáticamente.

14. Verifique que el estado de almacenamiento del nodo de almacenamiento esté en línea:

- a. Sign in en Grid Manager usando un ["navegador web compatible"](#).
- b. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
- c. Seleccione **sitio > Nodo de almacenamiento > LDR > Almacenamiento**.
- d. Seleccione la pestaña **Configuración** y luego la pestaña **Principal**.
- e. Si la lista desplegable **Estado de almacenamiento - Deseado** está configurada en Solo lectura o Sin conexión, seleccione **En línea**.
- f. Haga clic en **Aplicar cambios**.

15. Para ver los nuevos almacenes de objetos:

- a. Seleccione **NODOS > sitio > Nodo de almacenamiento > Almacenamiento**.
- b. Vea los detalles en la tabla **Almacenes de objetos**.

Resultado

Ahora puede utilizar la capacidad ampliada de los nodos de almacenamiento para guardar datos de objetos.

Agregar nodos de cuadrícula o sitio

Agregar nodos de cuadrícula a un sitio existente o agregar un sitio nuevo

Siga este procedimiento para agregar nodos de cuadrícula a sitios existentes o para agregar un sitio nuevo. Sólo se puede realizar un tipo de expansión a la vez.

Antes de empezar

- Tú tienes el ["Acceso root o permiso de mantenimiento"](#) .
- Todos los nodos existentes en la red están en funcionamiento en todos los sitios.
- Se han completado todos los procedimientos previos de expansión, actualización, desmantelamiento o recuperación.



No se le permite iniciar una expansión mientras otro procedimiento de expansión, actualización, recuperación o desmantelamiento activo esté en curso. Sin embargo, si es necesario, puede pausar un procedimiento de desmantelamiento para iniciar una expansión.

Pasos

1. ["Actualizar subredes para la red Grid"](#) .
2. ["Implementar nuevos nodos de red"](#) .
3. ["Realizar expansión"](#) .

Actualizar subredes para la red Grid

Cuando agrega nodos de cuadrícula o un nuevo sitio en una expansión, es posible que necesite actualizar o agregar subredes a la red de cuadrícula.

StorageGRID mantiene una lista de las subredes de red utilizadas para comunicarse entre los nodos de la red en la red Grid (eth0). Estas entradas incluyen las subredes utilizadas para la red Grid por cada sitio en su sistema StorageGRID , así como también cualquier subred utilizada para NTP, DNS, LDAP u otros servidores externos a los que se accede a través de la puerta de enlace de la red Grid.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de mantenimiento o acceso root"](#) .
- Tienes la contraseña de aprovisionamiento.
- Tienes las direcciones de red, en notación CIDR, de las subredes que quieres configurar.

Acerca de esta tarea

Si alguno de los nuevos nodos tiene una dirección IP de red Grid en una subred no utilizada anteriormente, debe agregar la nueva subred a la lista de subredes de red Grid antes de comenzar la expansión. De lo contrario, tendrá que cancelar la expansión, agregar la nueva subred y comenzar el procedimiento nuevamente.

No utilice subredes que contengan las siguientes direcciones IPv4 para la red de cuadrícula, la red de administración o la red de cliente de ningún nodo:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4



Por ejemplo, no utilice los siguientes rangos de subred para la red de cuadrícula, la red de administración o la red de cliente de ningún nodo:

- 192.168.130.0/24 porque este rango de subred contiene las direcciones IP 192.168.130.101 y 192.168.130.102
- 192.168.131.0/24 porque este rango de subred contiene las direcciones IP 192.168.131.101 y 192.168.131.102
- 198.51.100.0/24 porque este rango de subred contiene las direcciones IP 198.51.100.2 y 198.51.100.4

Pasos

1. Seleccione **MANTENIMIENTO > Red > Red de cuadrícula**.
2. Seleccione **Agregar otra subred** para agregar una nueva subred en notación CIDR.

Por ejemplo, introduzca 10.96.104.0/22.

3. Ingrese la contraseña de aprovisionamiento y seleccione **Guardar**.
4. Espere hasta que se apliquen los cambios y luego descargue un nuevo paquete de recuperación.
 - a. Seleccione **MANTENIMIENTO > Sistema > Paquete de recuperación**.
 - b. Introduzca la **contraseña de aprovisionamiento**.



El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID. También se utiliza para recuperar el nodo de administración principal.

Las subredes que ha especificado se configuran automáticamente para su sistema StorageGRID.

Implementar nuevos nodos de red

Los pasos para implementar nuevos nodos de red en una expansión son los mismos que los pasos utilizados cuando se instaló la red por primera vez. Debe implementar todos los nuevos nodos de la red antes de poder realizar la expansión.

Al expandir una cuadrícula, los nodos que agregue no tienen que coincidir con los tipos de nodos existentes. Puede agregar nodos VMware, nodos basados en contenedores Linux o nodos de dispositivos.

VMware: Implementar nodos de red

Debe implementar una máquina virtual en VMware vSphere para cada nodo VMware que desee agregar en la expansión.

Pasos

1. ["Implementar el nuevo nodo como máquina virtual"](#) y conectarlo a una o más redes StorageGRID .

Al implementar el nodo, puede opcionalmente reasignar los puertos del nodo o aumentar la configuración de CPU o memoria.

2. Después de haber implementado todos los nuevos nodos de VMware, ["realizar el procedimiento de expansión"](#) .

Linux: Implementar nodos de red

Puede implementar nodos de red en nuevos hosts Linux o en hosts Linux existentes. Si necesita hosts Linux adicionales para soportar los requisitos de CPU, RAM y almacenamiento de los nodos StorageGRID que desea agregar a su red, debe prepararlos de la misma manera que preparó los hosts cuando los instaló por primera vez. Luego, implementa los nodos de expansión de la misma manera que implementaste los nodos de la red durante la instalación.

Antes de empezar

- Tiene las instrucciones para instalar StorageGRID para su versión de Linux y ha revisado los requisitos de hardware y almacenamiento.
 - ["Instalar StorageGRID en Red Hat Enterprise Linux"](#)
 - ["Instalar StorageGRID en Ubuntu o Debian"](#)
- Si planea implementar nuevos nodos de red en hosts existentes, debe confirmar que los hosts existentes tengan suficiente CPU, RAM y capacidad de almacenamiento para los nodos adicionales.
- Tiene un plan para minimizar los dominios de falla. Por ejemplo, no debe implementar todos los nodos de puerta de enlace en un solo host físico.



En una implementación de producción, no ejecute más de un nodo de almacenamiento en un solo host físico o virtual. El uso de un host dedicado para cada nodo de almacenamiento proporciona un dominio de falla aislado.

- Si el nodo StorageGRID usa almacenamiento asignado desde un sistema NetApp ONTAP , confirme que el volumen no tenga habilitada una política de niveles de FabricPool . Deshabilitar la organización en niveles de FabricPool para los volúmenes utilizados con nodos StorageGRID simplifica la resolución de problemas y las operaciones de almacenamiento.

Pasos

1. Si está agregando nuevos hosts, acceda a las instrucciones de instalación para implementar nodos StorageGRID .
2. Para implementar los nuevos hosts, siga las instrucciones para prepararlos.
3. Para crear archivos de configuración de nodos y validar la configuración de StorageGRID , siga las instrucciones para implementar nodos de la red.
4. Si está agregando nodos a un nuevo host Linux, inicie el servicio de host StorageGRID .
5. Si está agregando nodos a un host Linux existente, inicie los nuevos nodos utilizando la CLI del servicio de host storagegrid:
`sudo storagegrid node start [<node name>]`

Después de terminar

Después de implementar todos los nuevos nodos de la red, puede ["realizar la expansión"](#) .

Dispositivos: Implementación de almacenamiento, puerta de enlace o nodos de administración no principales

Para instalar el software StorageGRID en un nodo de dispositivo, utilice el instalador de dispositivo StorageGRID , que está incluido en el dispositivo. En una expansión, 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 no principal. Cualquier dispositivo puede conectarse a la red de red, a la red de administración y a la red de cliente.

Antes de empezar

- El dispositivo se ha instalado en un rack o gabinete, se ha conectado a sus redes y se ha encendido.
- Has completado el ["Configurar el hardware"](#) pasos.

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 reasignar los puertos de red.

- Todas las subredes de la red Grid que aparecen en la página de configuración de IP del instalador del dispositivo StorageGRID se han definido en la lista de subredes de la red Grid en el nodo de administración principal.
- El firmware del instalador del dispositivo StorageGRID en el dispositivo de reemplazo es compatible con la versión del software StorageGRID que se ejecuta actualmente en su red. Si las versiones no son compatibles, debe actualizar el firmware del instalador del dispositivo StorageGRID .
- Tienes una computadora portátil de servicio con una ["navegador web compatible"](#) .
- Conoce una de las direcciones IP asignadas al controlador de cómputo del dispositivo. Puede utilizar 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:

- Usted especifica o confirma la dirección IP del nodo de administración principal y el nombre del nodo del dispositivo.
- Inicia la instalación y espera mientras se configuran los volúmenes y se instala el software.

A mitad de las tareas de instalación del dispositivo, la instalación se detiene. Para reanudar la instalación, inicie sesión en Grid Manager, apruebe todos los nodos de la red y complete el proceso de instalación de StorageGRID .



Si necesita implementar varios nodos de dispositivos al mismo tiempo, puede automatizar el proceso de instalación mediante el uso de `configure-sga.py` Script de instalación del dispositivo.

Pasos

1. Abra un navegador e ingrese una de las direcciones IP del controlador de cómputo del dispositivo.

```
https://Controller_IP:8443
```

Aparece la página de inicio del instalador del dispositivo 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 anteriormente ha instalado otros nodos en este centro de datos, el instalador del dispositivo StorageGRID puede descubrir esta dirección IP automáticamente, suponiendo que el nodo de administración principal, o al menos otro nodo de la red con ADMIN_IP configurado, esté presente en la misma subred.

3. Si esta dirección IP no se muestra o necesita cambiarla, especifique la dirección:

Opción	Descripción
Entrada manual de IP	a. Desmarque la casilla de verificación Habilitar descubrimiento de nodo de administración. b. Introduzca la dirección IP manualmente. c. Haga clic en Guardar. d. Espere a que el estado de la conexión para la nueva dirección IP esté listo.
Descubrimiento automático de todos los nodos de administración principales conectados	a. Seleccione la casilla de verificación Habilitar descubrimiento de nodo de administración. b. Espere a que se muestre la lista de direcciones IP descubiertas. c. Seleccione el nodo de administración principal para la red donde se implementará este nodo de almacenamiento del dispositivo. d. Haga clic en Guardar. e. Espere a que el estado de la conexión para la nueva dirección IP esté listo.

4. En el campo **Nombre del nodo**, ingrese el nombre que desea usar para este nodo del dispositivo y seleccione **Guardar**.

El nombre del nodo se asigna a este nodo del dispositivo en el sistema StorageGRID . Se muestra en la página Nodos (pestaña Descripción general) en el Administrador de cuadrícula. Si es necesario, puede cambiar el nombre cuando apruebe el nodo.

5. En la sección **Instalación**, confirme que el estado actual sea "Listo para iniciar la instalación de *nombre del nodo* en la red con el nodo de administración principal *admin_ip*" y que el botón **Iniciar instalación** esté habilitado.

Si el botón **Iniciar instalación** no está habilitado, es posible que necesite cambiar la configuración de red o la configuración del puerto. Para obtener instrucciones, consulte las instrucciones de mantenimiento de su aparato.

6. Desde la página de inicio del instalador del dispositivo StorageGRID , seleccione **Iniciar instalación**.

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.

Primary Admin Node connection

Enable Admin Node discovery

☐

Primary Admin Node IP

172.16.4.210

Connection state

Connection to 172.16.4.210 ready

Cancel

Save

Node name

Node name

NetApp-SGA

Cancel

Save

Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

Start Installation

El estado actual cambia a "La instalación está en curso" y se muestra la página de instalación del monitor.

7. Si su expansión incluye varios nodos de dispositivo, repita los pasos anteriores para cada dispositivo.



Si necesita implementar varios nodos de almacenamiento del dispositivo al mismo tiempo, puede automatizar el proceso de instalación mediante el script de instalación del dispositivo `configure-sga.py`.

8. Si necesita acceder manualmente a la página de Instalación del Monitor, seleccione **Instalación del Monitor** en la barra de menú.

La página de instalación del monitor muestra el progreso de la instalación.

1. Configure storage			Running
Step	Progress	Status	
Connect to storage controller		Complete	
Clear existing configuration		Complete	
Configure volumes		Creating volume StorageGRID-obj-00	
Configure host settings		Pending	

2. Install OS	Pending
3. Install StorageGRID	Pending
4. Finalize installation	Pending

La barra de estado azul indica qué tarea está actualmente en progreso. Las barras de estado verdes indican tareas que se han completado correctamente.



El instalador garantiza que las tareas completadas en una instalación anterior no se vuelvan a ejecutar. Si está volviendo a ejecutar una instalación, cualquier tarea que no necesite volver a ejecutarse se mostrará con una barra de estado verde y un estado de "Omitido".

9. Revise el progreso de las dos primeras etapas de instalación.

1. Configurar el dispositivo

Durante esta etapa se produce uno de los siguientes procesos:

- Para un dispositivo de almacenamiento, el instalador se conecta al controlador de almacenamiento, borra cualquier configuración existente, se comunica con SANtricity OS para configurar volúmenes y configura los ajustes del host.
- Para un dispositivo de servicios, el instalador borra cualquier configuración existente de las unidades en el controlador de cómputo y configura los ajustes del host.

2. Instalar sistema operativo

Durante esta etapa, el instalador copia la imagen del sistema operativo base de StorageGRID al dispositivo.

10. Continúe monitoreando el progreso de la instalación hasta que aparezca un mensaje en la ventana de la consola que le solicitará que utilice el Administrador de cuadrícula para aprobar el nodo.



Espere hasta que todos los nodos que agregó en esta expansión estén listos para su aprobación antes de ir al Administrador de cuadrícula para aprobar los nodos.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

Realizar expansión

Cuando realiza la expansión, los nuevos nodos de la red se agregan a su implementación de StorageGRID existente.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tienes la contraseña de aprovisionamiento.
- Ha implementado todos los nodos de la red que se están agregando en esta expansión.
- Tú tienes el ["Permiso de mantenimiento o acceso root"](#) .

- Si está agregando nodos de almacenamiento, ha confirmado que todas las operaciones de reparación de datos realizadas como parte de una recuperación están completas. Ver "[Comprobar trabajos de reparación de datos](#)".
- Si está agregando nodos de almacenamiento y desea asignar un grado de almacenamiento personalizado a esos nodos, ya debe "[creó el grado de almacenamiento personalizado](#)". También tienes el permiso de acceso root o los permisos de mantenimiento e ILM.
- Si está agregando un nuevo sitio, habrá revisado y actualizado las reglas de ILM. Debe asegurarse de que las copias de objetos no se almacenen en el nuevo sitio hasta que se complete la expansión. Por ejemplo, si una regla utiliza el grupo de almacenamiento predeterminado (**Todos los nodos de almacenamiento**), debe "[crear un nuevo grupo de almacenamiento](#)" que contiene solo los nodos de almacenamiento existentes y "[actualizar las reglas de ILM](#)" y la política de ILM para utilizar ese nuevo grupo de almacenamiento. De lo contrario, los objetos se copiarán al nuevo sitio tan pronto como el primer nodo de ese sitio se active.

Acerca de esta tarea

La realización de la expansión incluye estas tareas principales del usuario:

1. Configurar la expansión.
2. Iniciar la expansión.
3. Descargue un nuevo archivo de paquete de recuperación.
4. Supervisar los pasos y etapas de expansión hasta que todos los nodos nuevos estén instalados y configurados y todos los servicios se hayan iniciado.



Algunos pasos y etapas de expansión podrían requerir una cantidad significativa de tiempo para ejecutarse en una red grande. Por ejemplo, transmitir Cassandra a un nuevo nodo de almacenamiento puede tomar 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 podría llevar 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 la cuadrícula. La sección Nodos pendientes enumera los nodos que están listos para ser agregados.

Grid Expansion

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Configure Expansion

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve	✕ Remove	Search			
☐	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:a7:7a:c0	rlao-010-096-106-151	Storage Node	VMware VM	10.96.106.151/22
☐	00:50:56:a7:0f:2e	rlao-010-096-106-156	API Gateway Node	VMware VM	10.96.106.156/22

2. Seleccione **Configurar expansión**.

Aparece el cuadro de diálogo Selección del sitio.

3. Selecciona el tipo de expansión que estás iniciando:

- Si está agregando un nuevo sitio, seleccione **Nuevo** e ingrese el nombre del nuevo sitio.
- Si está agregando uno o más nodos a un sitio existente, seleccione **Existente**.

4. Seleccione **Guardar**.

5. Revise la lista **Nodos pendientes** y confirme que muestra todos los nodos de la red que implementó.

Según sea necesario, puede colocar el cursor sobre la **Dirección MAC de la red de cuadrícula** de un nodo para ver detalles sobre ese nodo.

Pending Nodes

Grid nodes are listed as

Approve

Remove

Grid Network MAC Address

00:50:56:a7:7a:c0

00:50:56:a7:0f:2e

Approved Nodes

Storage Node

Network

Grid Network	10.96.106.151/22	10.96.104.1
Admin Network	Name	Type
Client Network		

Hardware

VMware VM

4 CPUs

8 GB RAM

Disks

55 GB

55 GB

55 GB



Si falta un nodo, confirme que se implementó correctamente.

6. De la lista de nodos pendientes, apruebe los nodos que desea agregar en esta expansión.
- a. Seleccione el botón de opción junto al primer nodo de cuadrícula pendiente que desea aprobar.
- b. Seleccione **Aprobar**.

Aparece el formulario de configuración del nodo de la cuadrícula.

- c. Según sea necesario, modifique la configuración general:

Campo	Descripción
Sitio	El nombre del sitio con el que se asociará el nodo de la cuadrícula. Si está agregando varios nodos, asegúrese de seleccionar el sitio correcto para cada nodo. Si está agregando un nuevo sitio, todos los nodos se agregan al nuevo sitio.
Nombre	El nombre del sistema para el nodo. Los nombres de sistema son necesarios para las operaciones internas de StorageGRID y no se pueden cambiar.
Tipo de almacenamiento (solo nodos de almacenamiento)	Datos y metadatos ("combinados"): Nodo de almacenamiento de datos y metadatos de objetos Solo datos: Nodo de almacenamiento que contiene únicamente datos de objetos (sin metadatos) Solo metadatos: Nodo de almacenamiento que contiene solo metadatos (sin datos de objetos)

Campo	Descripción
Rol de NTP	La función del Protocolo de tiempo de red (NTP) del nodo de red: • Seleccione Automático (predeterminado) para asignar automáticamente la función NTP al nodo. El rol principal se asignará a los nodos de administración, nodos de almacenamiento con servicios ADC, nodos de puerta de enlace y cualquier nodo de red que tenga direcciones IP no estáticas. El rol de Cliente se asignará a todos los demás nodos de la red. • Seleccione Principal para asignar manualmente la función NTP principal al nodo. Al menos dos nodos en cada sitio deben tener la función principal para proporcionar acceso redundante al sistema a fuentes de sincronización externas. • Seleccione Cliente para asignar manualmente la función NTP de Cliente al nodo.
Servicio ADC (nodos de almacenamiento combinados o de solo metadatos)	Si este nodo de almacenamiento ejecutará el servicio del controlador de dominio administrativo (ADC). El servicio ADC realiza un seguimiento de la ubicación y la disponibilidad de los servicios de la red. Al menos tres nodos de almacenamiento en cada sitio deben incluir el servicio ADC. No se puede agregar el servicio ADC a un nodo después de implementarlo. • Seleccione Sí si el nodo de almacenamiento que está reemplazando incluye el servicio ADC. Dado que no se puede dismantelar un nodo de almacenamiento si quedan muy pocos servicios ADC, esto garantiza que haya un nuevo servicio ADC disponible antes de que se elimine el servicio anterior. • Seleccione Automático para permitir que el sistema determine si este nodo requiere el servicio ADC. Conozca más sobre el "Cuórum de la ADC" .
Grado de almacenamiento (nodos de almacenamiento combinados o de solo datos)	Utilice el grado de almacenamiento Predeterminado o seleccione el grado de almacenamiento personalizado que desea asignar a este nuevo nodo. Los niveles de almacenamiento son utilizados por los grupos de almacenamiento de ILM, por lo que su selección puede afectar qué objetos se colocarán en el nodo de almacenamiento.

d. Según sea necesario, modifique las configuraciones de la red de cuadrícula, la red de administración y la red de cliente.

- **Dirección IPv4 (CIDR):** La dirección de red CIDR para la interfaz de red. Por ejemplo:
172.16.10.100/24



Si descubre que los nodos tienen direcciones IP duplicadas en la red Grid mientras está aprobando nodos, debe cancelar la expansión, volver a implementar las máquinas virtuales o los dispositivos con una IP no duplicada y reiniciar la expansión.

- **Puerta de enlace:** La puerta de enlace predeterminada del nodo de la red. Por ejemplo: 172.16.10.1
- **Subredes (CIDR):** Una o más subredes para la red de administración.

e. Seleccione **Guardar**.

El nodo de la cuadrícula 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 mover un nodo de cuadrícula aprobado nuevamente a la lista de Nodos pendientes, seleccione su botón de opción y seleccione **Restablecer**.
- Para eliminar permanentemente un nodo de red aprobado, apague el nodo. Luego, seleccione su botón de opción y seleccione **Eliminar**.

f. Repita estos pasos para cada nodo de cuadrícula pendiente que desee aprobar.



Si es posible, debe aprobar todas las notas de la cuadrícula pendientes y realizar una única expansión. Se necesitará más tiempo si realiza varias expansiones pequeñas.

7. Cuando haya aprobado todos los nodos de la red, ingrese la **Frase de contraseña 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 nodos de la red individuales en curso, la sección Estado del nodo de la red muestra el estado actual de cada nodo de la red.



Durante el paso "Instalación de nodos de red" para un nuevo dispositivo, el instalador del dispositivo StorageGRID muestra que la instalación pasa de la Etapa 3 a la Etapa 4, Finalizar instalación. Cuando se completa la Etapa 4, el controlador se reinicia.

Expansion Progress

Lists the status of grid configuration tasks required to change the grid topology. These grid configuration tasks are run automatically by the StorageGRID system.

1. Installing grid nodes

In Progress

Grid Node Status

Lists the installation and configuration status of each grid node included in the expansion.

Search



Name	Site	Grid Network IPv4 Address	Progress	Stage
rleo-010-096-106-151	Data Center 1	10.96.106.151/22		Waiting for Dynamic IP Service peers
rleo-010-096-106-156	Data Center 1	10.96.106.156/22		Waiting for NTP to synchronize

2. Initial configuration

Pending

3. Distributing the new grid node's certificates to the StorageGRID system.

Pending

4. Assigning Storage Nodes to storage grade

Pending

5. Starting services on the new grid nodes

Pending

6. Starting background process to clean up unused Cassandra keys

Pending



Una expansión del sitio incluye una tarea adicional para configurar Cassandra para el nuevo sitio.

8. Tan pronto como aparezca el enlace **Descargar paquete de recuperación**, descargue el archivo del paquete de recuperación.

Debe descargar una copia actualizada del archivo del paquete de recuperación lo antes posible después de realizar cambios en la topología de la red en el sistema StorageGRID . El archivo del paquete de recuperación le permite restaurar el sistema si ocurre una falla.

- a. Seleccione el enlace de descarga.
- b. Ingrese la contraseña de aprovisionamiento y seleccione **Iniciar descarga**.
- c. Cuando se complete la descarga, abra el `.zip` archivo y confirme que puede acceder al contenido, incluido el `Passwords.txt` archivo.
- d. Copie el archivo del paquete de recuperación descargado(`.zip`) a dos lugares seguros, protegidos y separados.



El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

9. Si está agregando nodos de almacenamiento a un sitio existente o agregando un sitio, supervise las etapas de Cassandra, que ocurren cuando se inician los servicios en los nuevos nodos de la red.



No reinicie ningún nodo de almacenamiento durante las etapas de "Expansión del clúster Cassandra" o "Inicio de Cassandra y transmisión de datos". Estas etapas pueden tardar muchas horas en completarse para cada nuevo nodo de almacenamiento, especialmente si los nodos de almacenamiento existentes contienen una gran cantidad de metadatos de objetos.

Agregar nodos de almacenamiento

Si está agregando nodos de almacenamiento a un sitio existente, revise el porcentaje que se muestra en el mensaje de estado "Iniciando Cassandra y transmitiendo datos".

5. Starting services on the new grid nodes

In Progress

Grid Node Status

Lists the installation and configuration status of each grid node included in the expansion.

⚠

Do not reboot any Storage Nodes during Step 4. The "Starting Cassandra and streaming data" stage might take hours, especially if existing Storage Nodes contain a large amount of object metadata.

Search

Q

Name	Site	Grid Network IPv4 Address	Progress	Stage
rleo-010-096-106-151	Data Center 1	10.96.106.151/22		Starting Cassandra and streaming data (20.4% streamed)
rleo-010-096-106-156	Data Center 1	10.96.106.156/22		Starting services

Este porcentaje estima qué tan completa está la operación de transmisión de Cassandra, en función de la cantidad total de datos de Cassandra disponibles y la cantidad que ya se ha escrito en el nuevo nodo.

Agregar sitio

Si está agregando un nuevo sitio, utilice `nodetool status` para monitorear el progreso de la transmisión de Cassandra y ver cuántos metadatos se han copiado al nuevo sitio durante la etapa de "Expansión del clúster Cassandra". La carga total de datos en el nuevo sitio debe ser aproximadamente el 20% del total del sitio actual.

- Continúe monitoreando la expansión hasta que se completen todas las tareas y vuelva a aparecer el botón **Configurar expansión**.

Después de terminar

Dependiendo de los tipos de nodos de red que haya agregado, realice pasos de integración y configuración adicionales. Ver ["Pasos de configuración después de la expansión"](#).

Configurar el sistema expandido

Pasos de configuración después de la expansión

Después de completar una expansión, debe realizar pasos de integración y configuración

adicionales.

Acerca de esta tarea

Debe completar las tareas de configuración que se enumeran a continuación para los nodos de la red o los sitios que está agregando en su expansión. Algunas tareas pueden ser opcionales, dependiendo de las opciones seleccionadas al instalar y administrar su sistema, y de cómo desea configurar los nodos y sitios agregados durante la expansión.

Pasos

1. Si agregó un sitio:

- ["Crear un grupo de almacenamiento"](#) para el sitio y cada grado de almacenamiento que seleccionó para los nuevos nodos de almacenamiento.
- Confirmar que la política de ILM cumple con los nuevos requisitos. Si se requieren cambios en las reglas, ["crear nuevas reglas"](#) y ["actualizar la política de ILM"](#) . Si las reglas ya son correctas, ["activar una nueva política"](#) sin cambios de reglas para garantizar que StorageGRID utilice los nuevos nodos.
- Confirme que los servidores de Protocolo de tiempo de red (NTP) sean accesibles desde ese sitio. Ver ["Administrar servidores NTP"](#) .



Asegúrese de que al menos dos nodos en cada sitio puedan acceder al menos a cuatro fuentes NTP externas. Si solo un nodo en un sitio puede acceder a las fuentes NTP, se producirán problemas de sincronización si ese nodo deja de funcionar. Además, designar dos nodos por sitio como fuentes NTP primarias garantiza una sincronización precisa si un sitio está aislado del resto de la red.

2. Si agregó uno o más nodos de almacenamiento a un sitio existente:

- ["Ver detalles del grupo de almacenamiento"](#) para confirmar que cada nodo que agregó esté incluido en los grupos de almacenamiento esperados y se use en las reglas ILM esperadas.
- Confirmar que la política de ILM cumple con los nuevos requisitos. Si se requieren cambios en las reglas, ["crear nuevas reglas"](#) y ["actualizar la política de ILM"](#) . Si las reglas ya son correctas, ["activar una nueva política"](#) sin cambios de reglas para garantizar que StorageGRID utilice los nuevos nodos.
- ["Verifique que el nodo de almacenamiento esté activo"](#) y capaz de ingerir objetos.
- Si no pudo agregar la cantidad recomendada de nodos de almacenamiento, reequilibre los datos codificados por borrado. Ver ["Reequilibrar los datos codificados por borrado después de agregar nodos de almacenamiento"](#) .

3. Si agregó un nodo de puerta de enlace:

- Si se utilizan grupos de alta disponibilidad (HA) para conexiones de clientes, agregue opcionalmente el nodo de puerta de enlace a un grupo de HA. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad** para revisar la lista de grupos de alta disponibilidad existentes y agregar el nuevo nodo. Ver ["Configurar grupos de alta disponibilidad"](#) .

4. Si agregó un nodo de administración:

- a. Si el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID , cree una relación de confianza de usuario autenticado para el nuevo nodo de administración. No puedes iniciar sesión en el nodo hasta que crees esta confianza de parte autenticada. Ver ["Configurar el inicio de sesión único"](#) .
- b. Si planea utilizar el servicio Load Balancer en nodos de administración, opcionalmente agregue el nuevo nodo de administración a un grupo de alta disponibilidad. Seleccione **CONFIGURACIÓN > Red > Grupos de alta disponibilidad** para revisar la lista de grupos de alta disponibilidad existentes y agregar el nuevo nodo. Ver ["Configurar grupos de alta disponibilidad"](#) .

- c. De manera opcional, copie la base de datos del nodo de administración del nodo de administración principal al nodo de administración de expansión si desea mantener la información de atributos y auditoría consistente en cada nodo de administración. Ver "[Copiar la base de datos del nodo de administración](#)".
 - d. De manera opcional, copie la base de datos de Prometheus del nodo de administración principal al nodo de administración de expansión si desea mantener las métricas históricas consistentes en cada nodo de administración. Ver "[Copiar métricas de Prometheus](#)".
 - e. De manera opcional, copie los registros de auditoría existentes del nodo de administración principal al nodo de administración de expansión si desea mantener la información del registro histórico consistente en cada nodo de administración. Ver "[Copiar registros de auditoría](#)".
5. Para verificar si se agregaron nodos de expansión con una red de cliente no confiable o para cambiar si la red de cliente de un nodo es confiable o no confiable, vaya a **CONFIGURACIÓN > Seguridad > Control de firewall**.

Si la red del cliente en el nodo de expansión no es confiable, las conexiones al nodo en la red del cliente se deben realizar mediante un punto final del equilibrador de carga. Ver "[Configurar los puntos finales del balanceador de carga](#)" y "[Administrar los controles del firewall](#)".

6. Configurar el DNS.

Si ha estado especificando configuraciones de DNS por separado para cada nodo de la red, debe agregar configuraciones de DNS personalizadas por nodo para los nuevos nodos. Ver "[Modificar la configuración de DNS para un solo nodo de red](#)".

Para garantizar un funcionamiento correcto, especifique dos o tres servidores DNS. Si especifica más de tres, es posible que solo se utilicen tres debido a las limitaciones conocidas del sistema operativo en algunas plataformas. Si tiene restricciones de enrutamiento en su entorno, puede "[personalizar la lista de servidores DNS](#)" para que los nodos individuales (normalmente todos los nodos de un sitio) utilicen un conjunto diferente de hasta tres servidores DNS.

Si es posible, utilice servidores DNS a los que cada sitio pueda acceder localmente para garantizar que un sitio aislado pueda resolver los FQDN para destinos externos.

Verificar que el nodo de almacenamiento esté activo

Una vez completada una operación de expansión que agrega nuevos nodos de almacenamiento, el sistema StorageGRID debería comenzar a utilizar automáticamente los nuevos nodos de almacenamiento. Debe utilizar el sistema StorageGRID para verificar que el nuevo nodo de almacenamiento esté activo.

Pasos

1. Sign in en Grid Manager usando un "[navegador web compatible](#)".
2. Seleccione **NODOS > Nodo de almacenamiento de expansión > Almacenamiento**.
3. Coloque el cursor sobre el gráfico **Almacenamiento utilizado - Datos de objetos** para ver el valor de **Usado**, que es la cantidad de espacio utilizable total que se ha utilizado para los datos de objetos.
4. Verifique que el valor de **Usado** aumente a medida que mueve el cursor hacia la derecha en el gráfico.

Copiar la base de datos del nodo de administración

Al agregar nodos de administración a través de un procedimiento de expansión, puede copiar opcionalmente la base de datos del nodo de administración principal al nuevo nodo de administración. Copiar la base de datos le permite conservar información histórica sobre atributos, alertas y avisos.

Antes de empezar

- Ha completado los pasos de expansión necesarios para agregar un nodo de administración.
- Tú tienes el `Passwords.txt` archivo.
- Tienes la contraseña 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 de los servidores y servicios que actualmente forman parte del sistema o se agregan más adelante. Esta base de datos del nodo de administración incluye la siguiente información:

- Historial de alertas
- Datos de atributos históricos, que se utilizan en gráficos de estilo heredado en la página Nodos

Para garantizar que la base de datos del nodo de administración sea coherente entre los nodos, puede copiar la base de datos del nodo de administración principal al nodo de administración de expansión.



Copiar la base de datos del nodo de administración principal (el *nodo de administración de origen*) a un nodo de administración de expansión puede tardar varias horas en completarse. Durante este período, el Administrador de red no estará accesible.

Utilice 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 administración:
 - i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - iii. Introduzca el siguiente comando para cambiar a root: `su -`
 - iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - b. Ejecute el siguiente comando: `recover-access-points`
 - c. Introduzca la contraseña de aprovisionamiento.
 - d. Detener el servicio MI: `service mi stop`
 - e. Detener el servicio de interfaz de programación de aplicaciones de administración (mgmt-api):
`service mgmt-api stop`
2. Complete los siguientes pasos en el nodo de administración de expansión:
 - a. Inicie sesión en el nodo de administración de expansión:

- i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - iii. Introduzca el siguiente comando para cambiar a root: `su -`
 - iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- b. Detener el servicio MI: `service mi stop`
 - c. Detener el servicio mgmt-api: `service mgmt-api stop`
 - d. Agregue la clave privada SSH al agente SSH. Ingresar: `ssh-add`
 - e. Ingrese la contraseña de acceso SSH que aparece en el `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 al nodo de administración de expansión. Una vez finalizada la operación de copia, el script inicia la expansión del nodo de administración.

- h. Cuando ya no necesite acceso sin contraseña a otros servidores, elimine la clave privada del agente SSH. Ingresar: `ssh-add -D`

3. Reinicie los servicios en el nodo de administración principal: `service servermanager start`

Copiar métricas de Prometheus

Después de agregar un nuevo nodo de administración, puede copiar opcionalmente las métricas históricas mantenidas por Prometheus desde el nodo de administración principal al nuevo nodo de administración. Copiar las métricas garantiza que las métricas históricas sean consistentes entre los nodos de administración.

Antes de empezar

- El nuevo nodo de administración está instalado y funcionando.
- Tú tienes el `Passwords.txt` archivo.
- Tienes la contraseña de aprovisionamiento.

Acerca de esta tarea

Cuando agrega un nodo de administración, el proceso de instalación del software crea una nueva base de datos de Prometheus. Puede mantener las métricas históricas consistentes entre los nodos copiando la base de datos de Prometheus desde el nodo de administración principal (el *nodo de administración de origen*) al nuevo nodo de administración.



Copiar la base de datos de Prometheus podría tardar una hora o más. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios estén detenidos en el nodo de administración de origen.

Pasos

1. Inicie sesión en el nodo de administración de origen:

- a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
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 administración:
 - a. Inicie sesión en el nuevo nodo de administración:
 - i. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - iii. Introduzca el siguiente comando para cambiar a root: `su -`
 - iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - b. Detener el servicio Prometheus: `service prometheus stop`
 - c. Agregue la clave privada SSH al agente SSH. Ingresar: `ssh-add`
 - d. Ingrese la contraseña de acceso SSH que aparece en el `Passwords.txt` archivo.
 - e. Copie la base de datos de Prometheus del nodo de administración de origen al nuevo nodo de administración: `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
 - f. Cuando se le solicite, presione **Enter** para confirmar que desea destruir la nueva base de datos de Prometheus en el nuevo nodo de administración.

La base de datos original de Prometheus y sus datos históricos se copian al nuevo nodo de administración. Cuando se realiza 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 acceso sin contraseña a otros servidores, elimine la clave privada del agente SSH. Ingresar:

```
ssh-add -D
```

4. Reinicie el servicio Prometheus en el nodo de administración de origen.

```
service prometheus start
```

Copiar registros de auditoría

Cuando se agrega un nuevo nodo de administración a través de un procedimiento de expansión, su servicio AMS solo registra los eventos y acciones que ocurren después de que se une al sistema. Según sea necesario, puede copiar registros de auditoría de un nodo de administración previamente instalado al nuevo nodo de administración de expansión para que esté sincronizado con el resto del sistema StorageGRID .

Antes de empezar

- Ha completado los pasos de expansión necesarios para agregar un nodo de administración.
- Tú tienes el `Passwords.txt` archivo.

Acerca de esta tarea

Para que los mensajes de auditoría históricos estén disponibles en un nuevo nodo de administración, debe copiar manualmente los archivos de registro de auditoría desde un nodo de administración existente al nodo de administración de expansión.



De forma predeterminada, la información de auditoría se envía al registro de auditoría en los nodos de administración. Puede omitir estos pasos si se aplica alguna de las siguientes situaciones:

- Configuró un servidor syslog externo y los registros de auditoría ahora se envían al servidor syslog en lugar de a los nodos de administración.
- Usted especificó explícitamente que los mensajes de auditoría deben guardarse solo en los nodos locales que los generaron.

Ver ["Configurar mensajes de auditoría y destinos de registro"](#) Para 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 el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Detenga el servicio AMS para evitar que cree un nuevo archivo: `service ams stop`

3. Navegue hasta el directorio de exportación de auditoría:

```
cd /var/local/log
```

4. Cambiar el nombre de la fuente `audit.log` archivo para asegurarse de que no sobrescriba el archivo en el nodo de administración de expansión al que lo está copiando:

```
ls -l
mv audit.log _new_name_.txt
```

5. Copie todos los archivos de registro de auditoría a la ubicación de destino en el nodo de administración de expansión:

```
scp -p * IP_address:/var/local/log
```

6. Si se le solicita la contraseña para `/root/.ssh/id_rsa`, ingrese la contraseña de acceso SSH para el nodo de administración principal que aparece en la `Passwords.txt` archivo.

7. Restaurar el original `audit.log` archivo:

```
mv new_name.txt audit.log
```

8. Iniciar el servicio AMS:

```
service ams start
```

9. Cerrar sesión en el servidor:

```
exit
```

10. Inicie sesión en el nodo de administración de expansión:

- Introduzca el siguiente comando: `ssh admin@expansion_Admin_Node_IP`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- Introduzca el siguiente comando para cambiar a root: `su -`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

11. Actualice la configuración de usuario y grupo para los archivos de registro de auditoría:

```
cd /var/local/log  
  
chown ams-user:bycast *
```

12. Cerrar sesión en el servidor:

```
exit
```

Reequilibrar los datos codificados por borrado después de agregar nodos de almacenamiento

Después de agregar nodos de almacenamiento, puede utilizar el procedimiento de reequilibrio de codificación de borrado (EC) para redistribuir los fragmentos codificados de borrado entre los nodos de almacenamiento existentes y nuevos.

Antes de empezar

- Ha completado los pasos de expansión para agregar los nuevos nodos de almacenamiento.
- Usted ha revisado el ["Consideraciones para reequilibrar los datos codificados por borrado"](#).
- Usted comprende que los datos de objetos replicados no se moverán mediante este procedimiento y que el procedimiento de reequilibrio de EC no considera el uso de datos replicados en cada nodo de almacenamiento al determinar dónde mover los datos codificados por borrado.
- Tú tienes el `Passwords.txt` archivo.

¿Qué sucede cuando se ejecuta este procedimiento?

Antes de iniciar el procedimiento, tenga en cuenta lo siguiente:

- El procedimiento de reequilibrio de EC no se iniciará si uno o más volúmenes están fuera de línea (desmontados) o si están en línea (montados) pero en un estado de error.
- El procedimiento de reequilibrio de la CE reserva temporalmente una gran cantidad de almacenamiento. Es posible que se activen alertas de almacenamiento, pero se resolverán cuando se complete el reequilibrio. Si no hay suficiente almacenamiento para la reserva, el procedimiento de reequilibrio de EC fallará. Las reservas de almacenamiento se liberan cuando se completa el procedimiento de reequilibrio de EC, independientemente de si el procedimiento falló o tuvo éxito.
- Si un volumen se desconecta mientras el procedimiento de reequilibrio de EC está en proceso, el procedimiento de reequilibrio finalizará. Cualquier fragmento de datos que ya se haya movido permanecerá en sus nuevas ubicaciones y no se perderá ningún dato.

Puede volver a ejecutar el procedimiento después de que todos los volúmenes vuelvan a estar en línea.

- Cuando se ejecuta el procedimiento de reequilibrio de EC, el rendimiento de las operaciones de ILM y de las operaciones del cliente S3 podría verse afectado.



Las operaciones de la API S3 para cargar objetos (o partes de objetos) pueden fallar durante el procedimiento de reequilibrio de EC si requieren más de 24 horas para completarse. Las operaciones PUT de larga duración fallarán si la regla ILM aplicable utiliza ubicación equilibrada o estricta en la ingesta. Se informará el siguiente error: 500 Internal Server Error.

- Durante este procedimiento, todos los nodos tienen un límite de capacidad de almacenamiento del 80%. Los nodos que exceden este límite, pero aún almacenan por debajo de la partición de datos de destino, quedan excluidos de:
 - El valor del desequilibrio del sitio
 - Cualquier condición de finalización del trabajo



La partición de datos de destino se calcula dividiendo los datos totales de un sitio por la cantidad de nodos.

- **Condiciones de finalización del trabajo.** El procedimiento de reequilibrio de la CE se considera completo cuando se cumple cualquiera de las siguientes condiciones:
 - No se pueden mover más datos codificados por borrado.
 - Los datos de todos los nodos están dentro de una desviación del 5 % de la partición de datos de destino.
 - El procedimiento lleva 30 días en marcha.

Pasos

1. Revise los detalles de almacenamiento de objetos actuales para el sitio que planea reequilibrar.
 - a. Seleccione **NODOS**.
 - b. Seleccione el primer nodo de almacenamiento en el sitio.
 - c. Seleccione la pestaña **Almacenamiento**.
 - d. Coloque el cursor sobre el gráfico Almacenamiento utilizado - Datos de objeto para ver la cantidad actual de datos replicados y datos codificados por borrado en el nodo de almacenamiento.
 - e. Repita estos pasos para ver los otros nodos de almacenamiento en el 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 el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de \$ a # .

3. Iniciar el procedimiento:

```
`rebalance-data start --site "nombre-del-sitio"
```

Para "*site-name*", especifique el primer sitio donde agregó nuevos nodos de almacenamiento. Encerrar *site-name* entre comillas.

Se inicia el procedimiento de reequilibrio de CE y se devuelve un ID de trabajo.

4. Copiar el ID del trabajo.

5. Supervisar el estado del procedimiento de reequilibrio de la CE.

- Para ver el estado de un solo procedimiento de reequilibrio de CE:

```
rebalance-data status --job-id job-id
```

Para *job-id*, especifique el ID que se devolvió cuando inició el procedimiento.

- Para ver el estado del procedimiento actual de reequilibrio de CE y cualquier procedimiento completado anteriormente:

```
rebalance-data status
```



Para obtener ayuda sobre el comando `rebalance-data`:

```
rebalance-data --help
```

6. Realice pasos adicionales, según el estado devuelto:

- Si `State` es `In progress` La operación de reequilibrio de la CE todavía está en curso. Debes supervisar periódicamente el procedimiento hasta que se complete.

Utilice el `Site Imbalance` Valor para evaluar qué tan desequilibrado está el uso de datos de código de borrado en los nodos de almacenamiento del sitio. Este valor puede variar de 1,0 a 0, donde 0 indica que el uso de datos de codificación de borrado está completamente equilibrado entre todos los nodos de almacenamiento del sitio.

El trabajo de reequilibrio de EC se considera completo y se detendrá cuando los datos en todos los nodos estén dentro de una desviación del 5 % de la partición de datos de destino.

- Si `State` es `Success`, opcionalmente [revisar el almacenamiento de objetos](#) para ver los detalles actualizados del sitio.

Los datos codificados por borrado ahora deberían estar más equilibrados entre los nodos de

almacenamiento del sitio.

° Si State es Failure :

- i. Confirme que todos los nodos de almacenamiento en el sitio estén conectados a la red.
- ii. Verifique y resuelva cualquier alerta que pueda estar afectando a estos nodos de almacenamiento.
- iii. Reinicie el procedimiento de reequilibrio de CE:

```
rebalance-data start --job-id job-id
```

- iv. [Ver el estado](#) del nuevo procedimiento. Si State todavía está Failure , póngase en contacto con el soporte técnico.

7. Si el procedimiento de reequilibrio de EC genera demasiada carga (por ejemplo, las operaciones de ingesta se ven afectadas), pause 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), ingrese lo siguiente:

```
rebalance-data terminate --job-id job-id
```



Cuando finaliza un procedimiento de reequilibrio de EC, todos los fragmentos de datos que ya se hayan movido permanecerán en sus nuevas ubicaciones. Los datos no se mueven de nuevo a la ubicación original.

9. Si está utilizando codificación de borrado en más de un sitio, ejecute este procedimiento para todos los demás sitios afectados.

Solucionar problemas de expansión

Si encuentra errores durante el proceso de expansión de la red que no puede resolver, o si una tarea de la red falla, recopile los archivos de registro y comuníquese con el soporte técnico.

Antes de contactar con el soporte técnico, recopile los archivos de registro necesarios para ayudar en la resolución de problemas.

Pasos

1. Conectarse al nodo de expansión que ha experimentado fallas:

- 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 de contenedor que ejecuta StorageGRID.

- b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Después de iniciar sesión como root, el mensaje cambia de \$ a # .

2. Dependiendo de la etapa en la que se encuentre la instalación, recupere cualquiera de los siguientes registros que estén disponibles en el nodo de la red:

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 fallido) • /var/log/storagegrid/nodes/<node-name>.log(para cada nodo fallido; podría no existir)

Mantener un sistema StorageGRID

Mantenimiento de la red

Las tareas de mantenimiento de la red incluyen el desmantelamiento de un nodo o sitio, el cambio de nombre de una red, un nodo o un sitio y el mantenimiento de redes. También puede realizar procedimientos de host y middleware y procedimientos de nodo de red.



En estas instrucciones, "Linux" se refiere a una implementación de Red Hat® Enterprise Linux®, Ubuntu® o Debian®. Para obtener una lista de las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp"](#).

Antes de empezar

- Tiene un amplio conocimiento del sistema StorageGRID.
- Ha revisado la topología de su sistema StorageGRID y comprende la configuración de la red.
- Usted comprende que debe seguir todas las instrucciones exactamente y prestar atención a todas las advertencias.
- Usted comprende que los procedimientos de mantenimiento no descritos no son compatibles o requieren una contratación de servicios.

Procedimientos de mantenimiento de electrodomésticos

Para conocer los procedimientos de hardware, consulte la ["Instrucciones de mantenimiento para su dispositivo StorageGRID"](#).

Descargar paquete de recuperación

El archivo del paquete de recuperación le permite restaurar el sistema StorageGRID si ocurre una falla.

Antes de empezar

- Desde el nodo de administración principal, inicia sesión en el administrador de cuadrícula mediante un ["navegador web compatible"](#).
- Tienes la contraseña de aprovisionamiento.
- Tienes ["permisos de acceso específicos"](#).

Descargue el archivo del paquete de recuperación actual antes de realizar cambios en la topología de la red en el sistema StorageGRID o antes de actualizar el software. Luego, descargue una nueva copia del paquete de recuperación después de realizar cambios en la topología de la red o después de actualizar el software.

Pasos

1. Seleccione **MANTENIMIENTO > Sistema > Paquete de recuperación**.
2. Ingrese la contraseña de aprovisionamiento y seleccione **Iniciar descarga**.

La descarga comienza inmediatamente.

3. Cuando se complete la descarga, abra el `.zip` archivo y confirme que puede acceder al contenido, incluido el `Passwords.txt` archivo.
4. Copie el archivo del paquete de recuperación descargado(`.zip`) a dos lugares seguros, protegidos y separados.



El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

Desmantelar nodos o sitios

Nodo o sitio de desmantelamiento

Puede realizar un procedimiento de desmantelamiento para eliminar de forma permanente los nodos de la red o un sitio completo del sistema StorageGRID .

Para eliminar un nodo de la red o un sitio, realice uno de los siguientes procedimientos de desmantelamiento:

- Realizar una "[Desmantelamiento de nodos de red](#)" para eliminar uno o más ganglios, que pueden estar en uno o más sitios. Los nodos que elimine pueden estar en línea y conectados al sistema StorageGRID o pueden estar fuera de línea y desconectados.
- Realizar una "[desmantelamiento del sitio](#)" para eliminar un sitio. Se realiza una **desactivación del sitio conectado** si todos los nodos están conectados a StorageGRID. Se realiza una **desconexión del sitio desconectado** si todos los nodos están desconectados de StorageGRID. Si el sitio contiene una mezcla de nodos conectados y desconectados, deberá volver a poner en línea todos los nodos fuera de línea.



Antes de realizar la desconexión de un sitio desconectado, comuníquese con su representante de cuenta de NetApp . NetApp revisará sus requisitos antes de habilitar todos los pasos en el asistente de desmantelamiento del sitio. No debe intentar desmantelar un sitio desconectado si cree que es posible recuperar el sitio o recuperar datos de objetos del sitio.

Nodos de desmantelamiento

Desmantelamiento de nodos de red

Puede utilizar el procedimiento de desmantelamiento de nodos para eliminar uno o más nodos de la red en uno o más sitios. No puedes desmantelar el nodo de administración principal.

Cuándo desmantelar un nodo

Utilice el procedimiento de desmantelamiento de nodo cuando se cumpla alguna de las siguientes condiciones:

- Agregó un nodo de almacenamiento más grande en una expansión y desea eliminar uno o más nodos de almacenamiento más pequeños, al mismo tiempo que conserva los objetos.



Si desea reemplazar un electrodoméstico antiguo por uno más nuevo, considere ["clonar el nodo del dispositivo"](#) en lugar de agregar un nuevo electrodoméstico en una expansión y luego desmantelar el electrodoméstico antiguo.

- Necesita menos almacenamiento total.
- Ya no necesitas un nodo de enlace.
- Ya no necesitas un nodo de administración no principal.
- Su red incluye un nodo desconectado que no puede recuperar ni volver a poner en funcionamiento.
- Su cuadrícula incluye un nodo de archivo.

Cómo desmantelar un nodo

Puede desmantelar nodos de red conectados o desconectados.

Desmantelar nodos conectados

En general, debe desmantelar los nodos de la red solo cuando estén conectados al sistema StorageGRID y solo cuando todos los nodos tengan un estado normal (tengan íconos verdes en las páginas **NODOS** y en la página **Desmantelar nodos**).

Para obtener instrucciones, consulte ["Desmantelar nodos de red conectados"](#).

Desmantelar nodos desconectados

En algunos casos, es posible que necesites desmantelar un nodo de la red que no esté conectado actualmente a la red (uno cuyo estado de salud sea desconocido o esté administrativamente inactivo).

Para obtener instrucciones, consulte ["Desmantelar nodos de red desconectados"](#).

Qué tener en cuenta antes de desmantelar un nodo

Antes de realizar cualquiera de los procedimientos, revise las consideraciones para cada tipo de nodo:

- ["Consideraciones para el desmantelamiento del nodo de administración o de puerta de enlace"](#)
- ["Consideraciones para el desmantelamiento del nodo de almacenamiento"](#)

Consideraciones para el desmantelamiento de nodos de administración o de puerta de enlace

Revise las consideraciones para dar de baja un nodo de administración o un nodo de puerta de enlace.

Consideraciones para el nodo de administración

- No puedes desmantelar el nodo de administración principal.
- No se puede desmantelar un nodo de administración si una de sus interfaces de red es parte de un grupo de alta disponibilidad (HA). Primero debe eliminar las interfaces de red del grupo HA. Vea las instrucciones para ["gestión de grupos de alta disponibilidad"](#).
- Según sea necesario, puede cambiar de forma segura las políticas de ILM mientras desmantela un nodo de administración.
- Si desmantela un nodo de administración y el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID, debe recordar quitar la confianza de usuario autenticado del nodo de los Servicios de federación de Active Directory (AD FS).

- Si utilizas ["federación de red"](#) Asegúrese de que la dirección IP del nodo que está desmantelando no se haya especificado para una conexión de federación de red.
- Cuando desmantela un nodo de administración desconectado, perderá los registros de auditoría de ese nodo; sin embargo, estos registros también deben existir en el nodo de administración principal.

Consideraciones para el nodo de enlace

- No se puede desmantelar un nodo de puerta de enlace si una de sus interfaces de red es parte de un grupo de alta disponibilidad (HA). Primero debe eliminar las interfaces de red del grupo HA. Vea las instrucciones para ["gestión de grupos de alta disponibilidad"](#) .
- Según sea necesario, puede cambiar de forma segura las políticas de ILM mientras desmantela un nodo de puerta de enlace.
- Si utilizas ["federación de red"](#) Asegúrese de que la dirección IP del nodo que está desmantelando no se haya especificado para una conexión de federación de red.
- Puede desmantelar de forma segura un nodo de puerta de enlace mientras esté desconectado.

Consideraciones para los nodos de almacenamiento

Consideraciones para el desmantelamiento de nodos de almacenamiento

Antes de desmantelar un nodo de almacenamiento, considere si puede clonar el nodo. Luego, si decide desmantelar el nodo, revise cómo StorageGRID administra los objetos y metadatos durante el procedimiento de desmantelamiento.

Cuándo clonar un nodo en lugar de desmantelarlo

Si desea reemplazar un nodo de almacenamiento de un dispositivo antiguo por un dispositivo más nuevo o más grande, considere clonar el nodo del dispositivo en lugar de agregar un nuevo dispositivo en una expansión y luego desmantelar el dispositivo antiguo.

La clonación de nodos de dispositivos le permite reemplazar fácilmente un nodo de dispositivo existente con un dispositivo compatible en el mismo sitio de StorageGRID . El proceso de clonación transfiere todos los datos al nuevo dispositivo, lo pone en servicio y deja el antiguo en un estado previo a la instalación.

Puede clonar un nodo de dispositivo si necesita:

- Reemplazar un aparato que esté llegando al final de su vida útil.
- Actualice un nodo existente para aprovechar la tecnología mejorada del dispositivo.
- Aumente la capacidad de almacenamiento de la red sin cambiar la cantidad de nodos de almacenamiento en su sistema StorageGRID .
- Mejore la eficiencia del almacenamiento, por ejemplo, cambiando el modo RAID.

Ver ["Clonación de nodos de dispositivos"](#) Para más detalles.

Consideraciones para los nodos de almacenamiento conectados

Revise las consideraciones para el desmantelamiento de un nodo de almacenamiento conectado.

- No debe desmantelar más de 10 nodos de almacenamiento en un solo procedimiento de desmantelamiento de nodo.

- El sistema debe incluir en todo momento suficientes nodos de almacenamiento para satisfacer los requisitos operativos, incluidos los ["Cuórum de la ADC"](#) y el activo ["Política de ILM"](#) . Para satisfacer esta restricción, es posible que necesite agregar un nuevo nodo de almacenamiento en una operación de expansión antes de poder dismantelar un nodo de almacenamiento existente.

Tenga cuidado al dismantelar nodos de almacenamiento en una red que contenga nodos solo de metadatos basados en software. Si dismantela todos los nodos configurados para almacenar *tanto* objetos como metadatos, se elimina la capacidad de almacenar objetos de la red. Ver ["Tipos de nodos de almacenamiento"](#) para obtener más información sobre los nodos de almacenamiento de solo metadatos.

- Cuando se elimina un nodo de almacenamiento, se transfieren grandes volúmenes de datos de objetos a través de la red. Aunque estas transferencias no deberían afectar las operaciones normales del sistema, pueden afectar la cantidad total de ancho de banda de red consumido por el sistema StorageGRID .
- Las tareas asociadas con el dismantelamiento del nodo de almacenamiento reciben una prioridad menor que las tareas asociadas con las operaciones normales del sistema. Esto significa que el dismantelamiento no interfiere con las operaciones normales del sistema StorageGRID y no necesita programarse para un período de inactividad del sistema. Dado que el dismantelamiento se realiza en segundo plano, es difícil estimar cuánto tiempo tardará en completarse el proceso. En general, el dismantelamiento finaliza más rápidamente cuando el sistema está en silencio o si solo se elimina un nodo de almacenamiento a la vez.
- Podrían necesitarse días o semanas para dismantelar un nodo de almacenamiento. Planifique este procedimiento en consecuencia. Si bien el proceso de dismantelamiento está diseñado para no afectar las operaciones del sistema, puede limitar otros procedimientos. En general, debe realizar cualquier actualización o expansión planificada del sistema antes de eliminar los nodos de la red.
- Si necesita realizar otro procedimiento de mantenimiento mientras se eliminan los nodos de almacenamiento, puede ["pausar el procedimiento de dismantelamiento"](#) y reanudarlo después de que se complete el otro procedimiento.



El botón **Pausa** se habilita solo cuando se alcanzan las etapas de evaluación de ILM o de dismantelamiento de datos codificados por borrado; sin embargo, la evaluación de ILM (migración de datos) continuará ejecutándose en segundo plano.

- No se pueden ejecutar operaciones de reparación de datos en ningún nodo de la red cuando se está ejecutando una tarea de dismantelamiento.
- No debe realizar ningún cambio en una política ILM mientras se dismantela un nodo de almacenamiento.
- Para eliminar datos de forma permanente y segura, debe borrar las unidades del nodo de almacenamiento una vez completado el procedimiento de dismantelamiento.

Consideraciones para nodos de almacenamiento desconectados

Revise las consideraciones para dar de baja un nodo de almacenamiento desconectado.

- Nunca desactive un nodo desconectado a menos que esté seguro de que no se puede volver a poner en línea ni recuperar.



No realice este procedimiento si cree que es posible recuperar datos del objeto del nodo. En su lugar, comuníquese con el soporte técnico para determinar si es posible recuperar el nodo.

- Cuando se dismantela un nodo de almacenamiento desconectado, StorageGRID utiliza datos de otros nodos de almacenamiento para reconstruir los datos de objetos y metadatos que estaban en el nodo

desconectado.

- Podría producirse una pérdida de datos si desconecta más de un nodo de almacenamiento desconectado. Es posible que el sistema no pueda reconstruir datos si no quedan suficientes copias de objetos, fragmentos codificados por borrado o metadatos de objetos disponibles. Al dismantelar nodos de almacenamiento en una red con nodos solo de metadatos basados en software, al dismantelar todos los nodos configurados para almacenar objetos y metadatos se elimina todo el almacenamiento de objetos de la red. Ver "[Tipos de nodos de almacenamiento](#)" para obtener más información sobre los nodos de almacenamiento de solo metadatos.



Si tiene más de un nodo de almacenamiento desconectado que no puede recuperar, comuníquese con el soporte técnico para determinar el mejor curso de acción.

- Cuando se dismantela un nodo de almacenamiento desconectado, StorageGRID inicia trabajos de reparación de datos al final del proceso de dismantelamiento. Estos trabajos intentan reconstruir los datos y metadatos del objeto que se almacenaron en el nodo desconectado.
- Cuando se dismantela un nodo de almacenamiento desconectado, el procedimiento de dismantelamiento se completa relativamente rápido. Sin embargo, los trabajos de reparación de datos pueden tardar días o semanas en ejecutarse y no son monitoreados por el procedimiento de dismantelamiento. Debe supervisar manualmente estos trabajos y reiniciarlos según sea necesario. Ver "[Comprobar trabajos de reparación de datos](#)".
- Si dismantela un nodo de almacenamiento desconectado que contiene la única copia de un objeto, dicho objeto se perderá. Los trabajos de reparación de datos solo pueden reconstruir y recuperar objetos si existe al menos una copia replicada o suficientes fragmentos codificados de borrado en los nodos de almacenamiento que están conectados actualmente.

¿Qué es el quórum de la ADC?

Es posible que no pueda dismantelar ciertos nodos de almacenamiento en un sitio si quedan muy pocos servicios de controlador de dominio administrativo (ADC) después del dismantelamiento.

El servicio ADC, que se encuentra en algunos nodos de almacenamiento, mantiene la información de topología de la red y proporciona servicios de configuración a la red. El sistema StorageGRID requiere que haya un quórum de servicios ADC disponibles en cada sitio y en todo momento.

No se puede dismantelar un nodo de almacenamiento si al eliminarlo se produce que ya no se cumpla el quórum del ADC. Para satisfacer el quórum de ADC durante un dismantelamiento, un mínimo de tres nodos de almacenamiento en cada sitio deben tener el servicio ADC. Si un sitio tiene más de tres nodos de almacenamiento con el servicio ADC, una mayoría simple de esos nodos debe permanecer disponible después del dismantelamiento: $((0.5 * \text{Storage Nodes with ADC}) + 1)$



Tenga cuidado al dismantelar nodos de almacenamiento en una red que contenga nodos solo de metadatos basados en software. Si dismantela todos los nodos configurados para almacenar *tanto* objetos como metadatos, se elimina la capacidad de almacenar objetos de la red. Ver "[Tipos de nodos de almacenamiento](#)" para obtener más información sobre los nodos de almacenamiento de solo metadatos.

Por ejemplo, supongamos que un sitio actualmente incluye seis nodos de almacenamiento con servicios de ADC y desea dismantelar tres nodos de almacenamiento. Debido al requisito de quórum de ADC, debe completar dos procedimientos de dismantelamiento, como se indica a continuación:

- En el primer procedimiento de desmantelamiento, debe asegurarse de que cuatro nodos de almacenamiento con servicios ADC permanezcan disponibles: $((0.5 * 6) + 1)$. Esto significa que inicialmente solo puedes desmantelar dos nodos de almacenamiento.
- En el segundo procedimiento de desmantelamiento, puede eliminar el tercer nodo de almacenamiento porque el quórum de ADC ahora solo requiere que tres servicios de ADC permanezcan disponibles: $((0.5 * 4) + 1)$.

Si necesita desmantelar un nodo de almacenamiento pero no puede hacerlo debido al requisito de quórum de ADC, agregue un nuevo nodo de almacenamiento en un "expansión" y especifique que debe tener un servicio ADC. A continuación, desmantele el nodo de almacenamiento existente.

Revisar la política de ILM y la configuración de almacenamiento

Si planea desmantelar un nodo de almacenamiento, debe revisar la política ILM de su sistema StorageGRID antes de comenzar el proceso de desmantelamiento.

Durante el desmantelamiento, todos los datos de los objetos se migran desde el nodo de almacenamiento desmantelado a otros nodos de almacenamiento.



La política ILM que tenga *durante* la baja será la que utilice *después* de la baja. Debe asegurarse de que esta política cumpla con sus requisitos de datos tanto antes de comenzar el desmantelamiento como después de que este se complete.

Debes revisar las reglas en cada uno "política ILM activa" para garantizar que el sistema StorageGRID seguirá teniendo suficiente capacidad del tipo correcto y en las ubicaciones correctas para 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 manera que se cumplan las reglas de ILM?
- ¿Qué sucede si un sitio deja de estar disponible temporalmente mientras se lleva a cabo el desmantelamiento? ¿Se pueden realizar copias adicionales en una ubicación alternativa?
- ¿Cómo afectará el proceso de desmantelamiento a la distribución final de contenidos? Como se describe en "Consolidar nodos de almacenamiento", debería "agregar nuevos nodos de almacenamiento" Antes de desmantelar los antiguos. Si agrega un nodo de almacenamiento de reemplazo más grande después de desmantelar un nodo de almacenamiento más pequeño, los nodos de almacenamiento antiguos podrían estar cerca de su capacidad máxima y el nuevo nodo de almacenamiento podría no tener casi contenido. La mayoría de las operaciones de escritura de nuevos datos de objetos se dirigirían al nuevo nodo de almacenamiento, lo que reduciría la eficiencia general de las operaciones del sistema.
- ¿El sistema incluirá en todo momento suficientes nodos de almacenamiento para satisfacer las políticas ILM activas?



Una política ILM que no se pueda cumplir generará retrasos y alertas y podría detener el funcionamiento del sistema StorageGRID.

Verifique que la topología propuesta que resultará del proceso de desmantelamiento satisfaga la política ILM evaluando las áreas enumeradas en la tabla.

Área a evaluar	Qué tener en cuenta
Capacidad disponible	¿Habrá suficiente capacidad de almacenamiento para acomodar todos los datos de objetos almacenados en el sistema StorageGRID , incluidas las copias permanentes de los datos de objetos actualmente almacenados en el nodo de almacenamiento que se desmantelarán? ¿Habrá suficiente capacidad para manejar el crecimiento previsto en los datos de objetos almacenados durante un intervalo de tiempo razonable una vez que se complete el desmantelamiento?
Ubicación del almacenamiento	Si queda suficiente capacidad en el sistema StorageGRID en su conjunto, ¿está la capacidad en las ubicaciones correctas para satisfacer las reglas comerciales del sistema StorageGRID ?
Tipo de almacenamiento	¿Habrá suficiente almacenamiento del tipo apropiado una vez completado el desmantelamiento? Por ejemplo, las reglas ILM podrían mover contenido de un tipo de almacenamiento a otro a medida que el contenido envejece. En este caso, debe asegurarse de que haya suficiente almacenamiento del tipo apropiado disponible en la configuración final del sistema StorageGRID .

Consolidar nodos de almacenamiento

Puede consolidar nodos de almacenamiento para reducir la cantidad de nodos de almacenamiento de un sitio o una implementación y, al mismo tiempo, aumentar la capacidad de almacenamiento.

Cuando consolida nodos de almacenamiento, ["ampliar el sistema StorageGRID"](#) agregando nodos de almacenamiento nuevos, de mayor capacidad, y luego desmantelando los nodos de almacenamiento antiguos, de menor capacidad. Durante el procedimiento de desmantelamiento, los objetos se migran de los antiguos nodos de almacenamiento a los nuevos nodos de almacenamiento.



Si está consolidando electrodomésticos más antiguos y pequeños con modelos nuevos o electrodomésticos de mayor capacidad, considere ["clonar el nodo del dispositivo"](#) (o utilice la clonación de nodos del dispositivo y el procedimiento de desmantelamiento si no está realizando un reemplazo uno a uno).

Por ejemplo, puede agregar dos nodos de almacenamiento nuevos y de mayor capacidad para reemplazar tres nodos de almacenamiento más antiguos. Primero deberá utilizar el procedimiento de expansión para agregar los dos nodos de almacenamiento nuevos y más grandes, y luego deberá utilizar el procedimiento de desmantelamiento para eliminar los tres nodos de almacenamiento antiguos y de menor capacidad.

Al agregar nueva capacidad antes de eliminar los nodos de almacenamiento existentes, se garantiza una distribución de datos más equilibrada en todo el sistema StorageGRID . También reduce la posibilidad de que un nodo de almacenamiento existente pueda ser empujado más allá del nivel de marca de agua de almacenamiento.

Si necesita eliminar más de un nodo de almacenamiento, puede desmantelarlos de forma secuencial o en paralelo.



Tenga cuidado al desmantelar nodos de almacenamiento en una red que contenga nodos solo de metadatos basados en software. Si desmantela todos los nodos configurados para almacenar *tanto* objetos como metadatos, se elimina la capacidad de almacenar objetos de la red. Ver "[Tipos de nodos de almacenamiento](#)" para obtener más información sobre los nodos de almacenamiento de solo metadatos.

- Si desmantela nodos de almacenamiento de forma secuencial, debe esperar a que el primer nodo de almacenamiento complete el desmantelamiento antes de comenzar a desmantelar el siguiente nodo de almacenamiento.
- Si desmantela nodos de almacenamiento en paralelo, estos procesarán simultáneamente tareas de desmantelamiento para todos los nodos de almacenamiento que se desmantelan. Esto puede generar una situación en la que todas las copias permanentes de un archivo se marquen como "solo lectura", lo que deshabilita temporalmente la eliminación en las cuadrículas donde esta funcionalidad está habilitada.

Comprobar trabajos de reparación de datos

Antes de desmantelar un nodo de la red, debe confirmar que no haya trabajos de reparación de datos activos. Si alguna reparación ha fallado, debe reiniciarla y dejar que se complete antes de realizar el procedimiento de desmantelamiento.

Acerca de esta tarea

Si necesita desmantelar un nodo de almacenamiento desconectado, también deberá completar estos pasos una vez finalizado el procedimiento de desmantelamiento para garantizar que el trabajo de reparación de datos se haya completado exitosamente. Debe asegurarse de que todos los fragmentos con código de borrado que estaban en el nodo eliminado se hayan restaurado correctamente.

Estos pasos solo se aplican a sistemas que tienen objetos con código de borrado.

Pasos

1. Inicie sesión en el nodo de administración principal:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Comprobar si hay reparaciones en curso: `repair-data show-ec-repair-status`
 - Si nunca ha ejecutado un trabajo de reparación de datos, el resultado 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.

Repair ID	Affected Nodes / Volumes	Start Time	End Time	State	Estimated Bytes Affected	Bytes Repaired	Percentage
4216507958013005550	DC1-S1-0-182 (Volumes: 2)	2022-08-17T21:37:30.051543	2022-08-17T21:37:37.320998	Completed	1015788876	0	0
18214680851049518682	DC1-S1-0-182 (Volumes: 1)	2022-08-17T20:37:58.869362	2022-08-17T20:38:45.299688	Completed	0	0	100
7962734388032289010	DC1-S1-0-182 (Volumes: 0)	2022-08-17T20:42:29.578740		Stopped			Unknown



Opcionalmente, puede utilizar el Administrador de cuadrícula para supervisar los procesos de restauración en curso y mostrar un historial de restauración. Ver ["Restaurar datos de objetos mediante Grid Manager"](#).

3. Si el Estado se hace cargo de todas las reparaciones `Completed`, no es necesario reiniciar ningún trabajo de reparación.
4. Si el Estado por cualquier reparación es `Stopped`, debes reiniciar esa reparación.
 - a. Obtenga el ID de reparación para la reparación fallida a partir de la salida.
 - b. Ejecutar el `repair-data start-ec-node-repair dominio`.

Utilice el `--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. Continuar el seguimiento del estado de las reparaciones de datos de la CE hasta que se determine el estado de todas las reparaciones. `Completed`.

Reúna los materiales necesarios

Antes de realizar el desmantelamiento de un nodo de la red, debe obtener la siguiente información.

Artículo	Notas
Paquete de recuperación .zip archivo	Usted debe "Descargue el paquete de recuperación más reciente" .zip archivo(<code>sgws-recovery-package-id-revision.zip</code>). Puede utilizar el archivo del paquete de recuperación para restaurar el sistema si ocurre una falla.
`Passwords.txt` archivo	Este archivo contiene las contraseñas necesarias para acceder a los nodos de la red en la línea de comandos y está incluido en el paquete de recuperación.
Frase de contraseña de aprovisionamiento	La frase de contraseña se crea y se documenta cuando se instala por primera vez el sistema StorageGRID . La frase de contraseña de aprovisionamiento no está en el <code>Passwords.txt</code> archivo.
Descripción de la topología del sistema StorageGRID antes del desmantelamiento	Si está disponible, obtenga cualquier documentación que describa la topología actual del sistema.

Información relacionada

["Requisitos del navegador web"](#)

Acceder a la página de nodos de desmantelamiento

Cuando accede a la página Nodos de desmantelamiento en el Administrador de red, puede ver de un vistazo qué nodos se pueden desmantelar.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"Permiso de mantenimiento o acceso root" .



Tenga cuidado al desmantelar nodos de almacenamiento en una red que contenga nodos solo de metadatos basados en software. Si desmantela todos los nodos configurados para almacenar *tanto* objetos como metadatos, se elimina la capacidad de almacenar objetos de la red. Ver"Tipos de nodos de almacenamiento" para obtener más información sobre los nodos de almacenamiento de solo metadatos.

Pasos

1. Seleccione **MANTENIMIENTO > Tareas > Desmantelamiento**.
2. Seleccione **Nodos de desmantelamiento**.

Aparece la página Nodos de desmantelamiento. Desde esta página, puedes:

- Determinar qué nodos de la red se pueden desmantelar actualmente.
- Ver el estado de todos los nodos de la red
- Ordene la lista en orden ascendente o descendente por **Nombre, Sitio, Tipo o Tiene ADC**.
- Introduzca términos de búsqueda para encontrar rápidamente nodos específicos.

En este ejemplo, la columna Desactivación posible indica que puede desactivar el nodo de puerta de enlace y uno de los cuatro nodos de almacenamiento.

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-		No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC1-ARC1	Data Center 1	Archive Node	-		No, you can't decommission an Archive Node unless the node is disconnected.
☐ DC1-G1	Data Center 1	API Gateway Node	-		
DC1-S1	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S2	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S3	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
☐ DC1-S4	Data Center 1	Storage Node	No		

3. Revise la columna **Desactivación posible** para cada nodo que desee desactivar.

Si se puede desmantelar un nodo de la red, esta columna incluye una marca de verificación verde y la columna izquierda incluye una casilla de verificación. Si no se puede desmantelar un nodo, esta columna describe el problema. Si hay más de un motivo por el cual no se puede desmantelar un nodo, se muestra el motivo más crítico.

Desmantelamiento Posible motivo	Descripción	Pasos para resolver
No, no se admite el desmantelamiento del <i>tipo de nodo</i> .	No puedes desmantelar el nodo de administración principal.	Ninguno.
No, al menos un nodo de la red está desconectado. Nota: Este mensaje se muestra únicamente para los nodos de la red conectados.	No es posible desmantelar un nodo de red conectado si algún nodo de red está desconectado. La columna Salud incluye uno de estos íconos para los nodos de la red que están desconectados:  (gris): Administrativamente caído  (azul): Desconocido	Debe volver a poner en línea todos los nodos desconectados o " Desmantelar todos los nodos desconectados " antes de poder eliminar un nodo conectado. Nota: Si su red contiene varios nodos desconectados, el software requiere que los desactive todos al mismo tiempo, lo que aumenta la posibilidad de que se produzcan resultados inesperados.
No, uno o más nodos requeridos están actualmente desconectados y deben recuperarse. Nota: Este mensaje se muestra únicamente para los nodos de la red desconectados.	No se puede desmantelar un nodo de red desconectado si uno o más nodos requeridos también están desconectados (por ejemplo, un nodo de almacenamiento que es necesario para el quórum de ADC).	- Revise los mensajes de posible desconexión para todos los nodos desconectados. - Determinar qué nodos no se pueden desmantelar porque son necesarios. - Si la salud de un nodo requerido está administrativamente inactiva, vuelva a poner el nodo en línea. - Si el estado de salud de un nodo requerido es desconocido, realice un procedimiento de recuperación de nodo para recuperarlo.
No, miembro del grupo(s) de HA: <i>nombre del grupo</i> . Antes de poder desmantelar este nodo, debe eliminarlo de todos los grupos de alta disponibilidad.	No se puede desmantelar un nodo de administración o un nodo de puerta de enlace si una interfaz de nodo pertenece a un grupo de alta disponibilidad (HA).	Edite el grupo HA para eliminar la interfaz del nodo o eliminar todo el grupo HA. Ver " Configurar grupos de alta disponibilidad ".

Desmantelamiento Posible motivo	Descripción	Pasos para resolver
No, el sitio x requiere un mínimo de n nodos de almacenamiento con servicios ADC.	Solo nodos de almacenamiento. No se puede dismantelar un nodo de almacenamiento si no quedan suficientes nodos en el sitio para cumplir con los requisitos de quórum de ADC.	Realizar una expansión. Agregue un nuevo nodo de almacenamiento al sitio y especifique que debe tener un servicio ADC. Ver información sobre el "Cuórum de la ADC" .
No, uno o más perfiles de codificación de borrado necesitan al menos n nodos de almacenamiento. Si el perfil no se utiliza en una regla ILM, puede desactivarlo.	Solo nodos de almacenamiento. No se puede dismantelar un nodo de almacenamiento a menos que queden suficientes nodos para los perfiles de codificación de borrado existentes. Por ejemplo, si existe un perfil de codificación de borrado para codificación de borrado 4+2, deben permanecer al menos 6 nodos de almacenamiento.	Para cada perfil de codificación de borrado afectado, realice uno de los siguientes pasos, según cómo se utilice el perfil: • Se utiliza en políticas ILM activas: Realizar una expansión. Agregue suficientes nodos de almacenamiento nuevos para permitir que la codificación de borrado continúe. Vea las instrucciones para "expandiendo su red". • Se usa en una regla ILM pero no en políticas ILM activas: edite o elimine la regla y luego desactive el perfil de codificación de borrado. • No se utiliza en ninguna regla ILM: Desactivar el perfil de codificación de borrado. Nota: Aparece un mensaje de error si intenta desactivar un perfil de codificación de borrado y los datos del objeto aún están asociados con el perfil. Es posible que tengas que esperar varias semanas antes de intentar nuevamente el proceso de desactivación. Conozca más sobre "Desactivar un perfil de codificación de borrado".

Desmantelamiento Posible motivo	Descripción	Pasos para resolver
No, no puedes dismantlar un nodo de archivo a menos que el nodo esté desconectado.	Si un nodo de archivo aún está conectado, no podrás eliminarlo.	Nota: Se ha eliminado el soporte para nodos de archivo. Si necesita dismantlar un nodo de archivo, consulte "Desmantelamiento de nodos de red (sitio de documentación de StorageGRID 11.8)"

Desmantelar nodos de red desconectados

Es posible que necesites dismantlar un nodo que actualmente no esté conectado a la red (uno cuyo estado de salud sea desconocido o esté administrativamente inactivo).

Antes de empezar

- Entiendes las consideraciones para el dismantlamiento ["Nodos de administración y de puerta de enlace"](#) y las consideraciones para el dismantlamiento ["Nodos de almacenamiento"](#).
- Has obtenido todos los elementos necesarios.
- Se ha asegurado de que no haya trabajos de reparación de datos activos. Ver ["Comprobar trabajos de reparación de datos"](#).
- Ha confirmado que la recuperación del nodo de almacenamiento no está en progreso en ningún lugar de la red. Si es así, deberá esperar hasta que se complete la reconstrucción de Cassandra realizada como parte de la recuperación. Luego puedes proceder al dismantlamiento.
- Se ha asegurado de que no se ejecutarán otros procedimientos de mantenimiento mientras se ejecuta el procedimiento de dismantlamiento del nodo, a menos que dicho procedimiento esté en pausa.
- La columna **Posible dismantlamiento** para el nodo o los nodos desconectados que desea dismantlar incluye una marca de verificación verde.
- Tienes la contraseña de aprovisionamiento.

Acerca de esta tarea

Puede identificar los nodos desconectados buscando el ícono azul Desconocido  o el ícono gris Administrativamente inactivo  en la columna **Salud**.

Antes de dismantlar cualquier nodo desconectado, tenga en cuenta lo siguiente:

- Este procedimiento está destinado principalmente a eliminar un solo nodo desconectado. Si su red contiene varios nodos desconectados, el software requiere que los desactive todos al mismo tiempo, lo que aumenta la posibilidad de que se produzcan resultados inesperados.



Podría producirse una pérdida de datos si desconecta más de un nodo de almacenamiento desconectado a la vez. Ver ["Consideraciones para nodos de almacenamiento desconectados"](#).



Tenga cuidado al dismantlar nodos de almacenamiento en una red que contenga nodos solo de metadatos basados en software. Si dismantla todos los nodos configurados para almacenar *tanto* objetos como metadatos, se elimina la capacidad de almacenar objetos de la red. Ver "[Tipos de nodos de almacenamiento](#)" para obtener más información sobre los nodos de almacenamiento de solo metadatos.

- Si no se puede eliminar un nodo desconectado (por ejemplo, un nodo de almacenamiento que se requiere para el quórum de ADC), no se podrá eliminar ningún otro nodo desconectado.

Pasos

1. A menos que esté dismantlando un nodo de archivo (que debe estar desconectado), intente volver a poner en línea todos los nodos de red desconectados o recuperarlos.

Ver "[Procedimientos de recuperación de nodos de red](#)" para obtener instrucciones.

2. Si no puede recuperar un nodo de red desconectado y desea dismantlarlo mientras está desconectado, seleccione la casilla de verificación de ese nodo.



Si su red contiene varios nodos desconectados, el software requiere que los desactive todos al mismo tiempo, lo que aumenta la posibilidad de que se produzcan resultados inesperados.



Tenga cuidado al elegir dismantlar más de un nodo de red desconectado a la vez, especialmente si está seleccionando varios nodos de almacenamiento desconectados. Si tiene más de un nodo de almacenamiento desconectado que no puede recuperar, comuníquese con el soporte técnico para determinar el mejor curso de acción.

3. Introduzca la contraseña de aprovisionamiento.

El botón **Iniciar dismantelamiento** está habilitado.

4. Haga clic en **Iniciar dismantelamiento**.

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 dismantelamiento y se muestra el progreso para cada nodo. Durante el procedimiento, se genera un nuevo paquete de recuperación que contiene el cambio de configuración de la red.

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 del paquete de recuperación. Luego, descargue el .zip archivo.

Vea las instrucciones para "[descargando el paquete de recuperación](#)".



Descargue el paquete de recuperación lo antes posible para asegurarse de poder recuperar su red si algo sale mal durante el procedimiento de dismantelamiento.



El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

7. Supervise periódicamente la página de Desmantelamiento para asegurarse de que todos los nodos seleccionados se desmantelen correctamente.

Los nodos de almacenamiento pueden tardar días o semanas en desmantelarse. Cuando se completan todas las tareas, la lista de selección de nodos se vuelve a mostrar con un mensaje de éxito. Si desactivó un nodo de almacenamiento desconectado, un mensaje de información indica que se han iniciado los trabajos de reparación.

8. Una vez que los nodos se hayan apagado automáticamente como parte del procedimiento de desmantelamiento, elimine cualquier máquina virtual u otros recursos restantes que estén asociados con el nodo desmantelado.



No realice este paso hasta que los nodos se hayan apagado automáticamente.

9. Si está desmantelando 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 desmantelamiento.

Datos replicados

- Para obtener un porcentaje estimado de finalización de la reparación replicada, agregue el `show-replicated-repair-status` Opción para el comando `reparar-datos`.

```
repair-data show-replicated-repair-status
```

- Para determinar si las reparaciones están completas:
 - a. Seleccione **NODOS > Nodo de almacenamiento en reparación > ILM**.
 - b. Revise los atributos en la sección Evaluación. Cuando se completan las reparaciones, el atributo **En espera - Todo** indica 0 objetos.
- Para supervisar la reparación con más detalle:
 - a. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
 - b. Seleccione **grid > Nodo de almacenamiento en reparación > LDR > Almacén de datos**.
 - c. Utilice una combinación de los siguientes atributos para determinar, lo mejor posible, si las reparaciones replicadas están completas.



Pueden existir inconsistencias en Cassandra y no se realiza un seguimiento de las reparaciones fallidas.

- **Reparaciones intentadas (XRPA)**: utilice este atributo para rastrear el 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 escaneo actual (proporcionado por el atributo **Período de escaneo – Estimado**), significa que el escaneo ILM no encontró objetos de alto riesgo que necesiten reparación en ningún nodo.



Los objetos de alto riesgo son objetos que corren el riesgo de perderse por completo. Esto no incluye objetos que no satisfacen su configuración ILM.

- **Período de escaneo estimado (XSCM)**: utilice este atributo para estimar cuándo se aplicará un cambio de política a los objetos ingeridos previamente. Si el atributo **Reparaciones intentadas** no aumenta durante un período más largo que el período de escaneo actual, es probable que se realicen reparaciones replicadas. Tenga en cuenta que el período de escaneo puede cambiar. El atributo **Período de escaneo estimado (XSCM)** se aplica a toda la cuadrícula y es el máximo de todos los períodos de escaneo de nodos. Puede consultar el historial de atributos **Período de escaneo – Estimado** de la cuadrícula para determinar un período de tiempo apropiado.

Datos codificados por borrado (EC)

Para supervisar la reparación de datos codificados por borrado y volver a intentar cualquier solicitud que pueda haber fallado:

1. Determinar el estado de las reparaciones de datos codificados por borrado:
 - Seleccione **SOPORTE > Herramientas > Métricas** para ver el tiempo estimado de finalización y el porcentaje de finalización del trabajo actual. Luego, seleccione **Descripción general de EC** en la sección Grafana. Consulte los paneles **Tiempo estimado de finalización del trabajo de Grid EC** 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
```

La salida enumera información, incluyendo `repair ID`, para todas las reparaciones realizadas anteriormente y actualmente en curso.

2. Si la salida muestra que la operación de reparación falló, utilice el `--repair-id` Opción para reintentar la reparación.

Este comando vuelve a intentar una reparación de nodo fallida, utilizando el ID de reparación 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando vuelve a intentar una reparación de volumen fallida, utilizando el ID de reparación 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Después de terminar

Una vez que se hayan desconectado los nodos y se hayan completado todos los trabajos de reparación de datos, puede desconectar cualquier nodo de red conectado según sea necesario.

Luego, complete estos pasos después de completar el procedimiento de desmantelamiento:

- Asegúrese de que las unidades del nodo de red fuera de servicio estén limpias. Utilice una herramienta o servicio de borrado de datos disponible comercialmente para eliminar datos de las unidades de forma permanente y segura.
- Si desactivó un nodo del dispositivo y los datos del dispositivo estaban protegidos mediante el cifrado del nodo, utilice el instalador del dispositivo StorageGRID para borrar la configuración del servidor de administración de claves (Borrar KMS). Debe borrar la configuración de KMS si desea agregar el dispositivo a otra red. Para obtener instrucciones, consulte ["Monitorizar el cifrado del nodo en modo de mantenimiento"](#).

Desmantelar nodos de red conectados

Puede desmantelar y eliminar de forma permanente los nodos que estén conectados a la red.

Antes de empezar

- Entiendes las consideraciones para el desmantelamiento ["Nodos de administración y de puerta de enlace"](#) y las consideraciones para el desmantelamiento ["Nodos de almacenamiento"](#).
- Has reunido todos los materiales necesarios.
- Se ha asegurado de que no haya trabajos de reparación de datos activos.
- Ha confirmado que la recuperación del nodo de almacenamiento no está en progreso en ningún lugar de

la red. Si es así, espere hasta que se complete la reconstrucción de Cassandra realizada como parte de la recuperación. Luego puedes proceder al desmantelamiento.

- Se ha asegurado de que no se ejecutarán otros procedimientos de mantenimiento mientras se ejecuta el procedimiento de desmantelamiento del nodo, a menos que dicho procedimiento esté en pausa.
- Tienes la contraseña de aprovisionamiento.
- Los nodos de la red están conectados.
- La columna **Posible desmantelamiento** para el nodo o los nodos que desea desmantelar incluye una marca de verificación verde.



La desactivación no se iniciará si uno o más volúmenes están fuera de línea (desmontados) o si están en línea (montados) pero en un estado de error.



Si uno o más volúmenes se desconectan mientras se lleva a cabo un desmantelamiento, el proceso de desmantelamiento se completa después de que estos volúmenes vuelvan a estar en línea.

- Todos los nodos de la red tienen una salud normal (verde) . Si ve uno de estos íconos en la columna **Salud**, debe intentar resolver el problema:

Icono	Color	Gravedad
	Amarillo	Aviso
	Naranja claro	Menor
	naranja oscuro	Importante
	Rojo	Crítico

- Si anteriormente desactivó un nodo de almacenamiento desconectado, todos los trabajos de reparación de datos se completaron correctamente. Ver "[Comprobar trabajos de reparación de datos](#)".



No elimine la máquina virtual ni otros recursos de un nodo de la red hasta que se le indique hacerlo en este procedimiento.



Tenga cuidado al desmantelar nodos de almacenamiento en una red que contenga nodos solo de metadatos basados en software. Si desmantela todos los nodos configurados para almacenar *tanto* objetos como metadatos, se elimina la capacidad de almacenar objetos de la red. Ver "[Tipos de nodos de almacenamiento](#)" para obtener más información sobre los nodos de almacenamiento de solo metadatos.

Acerca de esta tarea

Cuando se da de baja un nodo, sus servicios se desactivan y el nodo se apaga automáticamente.

Pasos

1. Desde la página Nodos de desmantelamiento, seleccione la casilla de verificación para cada nodo de la red que desee desmantelar.
2. Introduzca la contraseña de aprovisionamiento.

El botón **Iniciar desmantelamiento** está habilitado.

3. Seleccione **Iniciar desmantelamiento**.
4. Revise la lista de nodos en el cuadro de diálogo de confirmación y seleccione **Aceptar**.

Se inicia el procedimiento de desmantelamiento del nodo y se muestra el progreso para cada nodo.



No desconecte un nodo de almacenamiento una vez iniciado el procedimiento de desmantelamiento. Cambiar el estado podría provocar que parte del contenido no se copie a otras ubicaciones.

5. Tan pronto como el nuevo paquete de recuperación esté disponible, seleccione el enlace Paquete de recuperación en el banner o seleccione **MANTENIMIENTO > Sistema > Paquete de recuperación** para acceder a la página Paquete de recuperación. Luego, descargue el .zip archivo.

Ver "[descargando el paquete de recuperación](#)".



Descargue el paquete de recuperación lo antes posible para asegurarse de poder recuperar su red si algo sale mal durante el procedimiento de desmantelamiento.

6. Supervise periódicamente la página Nodos de desmantelamiento para asegurarse de que todos los nodos seleccionados se desmantelen correctamente.



Los nodos de almacenamiento pueden tardar días o semanas en desmantelarse.

Cuando se completan todas las tareas, la lista de selección de nodos se vuelve a mostrar con un mensaje de éxito.

Después de terminar

Complete estos pasos después de completar el procedimiento de desmantelamiento del nodo:

1. Siga el paso apropiado para su plataforma. Por ejemplo:
 - **Linux:** Es posible que desee separar los volúmenes y eliminar los archivos de configuración de nodo que creaste durante la instalación. Ver "[Instalar StorageGRID en Red Hat Enterprise Linux](#)" y "[Instalar StorageGRID en Ubuntu o Debian](#)".
 - **VMware:** Es posible que desee utilizar la opción "Eliminar del disco" de vCenter para eliminar la máquina virtual. Es posible que también sea necesario eliminar cualquier disco de datos que sea independiente de la máquina virtual.
 - ***Dispositivo StorageGRID*:** el nodo del dispositivo vuelve automáticamente a un estado no implementado donde puede acceder al instalador del dispositivo StorageGRID. Puede apagar el dispositivo o agregarlo a otro sistema StorageGRID.
2. Asegúrese de que las unidades del nodo de red fuera de servicio estén limpias. Utilice una herramienta o servicio de borrado de datos disponible comercialmente para eliminar datos de las unidades de forma permanente y segura.
3. Si desactivó un nodo del dispositivo y los datos del dispositivo estaban protegidos mediante el cifrado del

nodo, utilice el instalador del dispositivo StorageGRID para borrar la configuración del servidor de administración de claves (Borrar KMS). Debe borrar la configuración de KMS si desea agregar el dispositivo a otra red. Para obtener instrucciones, consulte "[Monitorizar el cifrado del nodo en modo de mantenimiento](#)".

Pausar y reanudar el proceso de desmantelamiento de nodos de almacenamiento

Si necesita realizar un segundo procedimiento de mantenimiento, puede pausar el procedimiento de desmantelamiento de un nodo de almacenamiento durante ciertas etapas. Una vez finalizado el resto del procedimiento, puedes reanudar el desmantelamiento.



El botón **Pausa** se habilita solo cuando se alcanzan las etapas de evaluación de ILM o de desmantelamiento de datos codificados por borrado; sin embargo, la evaluación de ILM (migración de datos) continuará ejecutándose en segundo plano.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tú tienes el "[Permiso de mantenimiento o acceso root](#)".

Pasos

1. Seleccione **MANTENIMIENTO > Tareas > Desmantelamiento**.

Aparece la página de Desmantelamiento.

2. Seleccione **Nodos de desmantelamiento**.

Aparece la página Nodos de desmantelamiento. Cuando el procedimiento de desmantelamiento llega a cualquiera de las siguientes etapas, se habilita el botón **Pausa**.

- Evaluación de ILM
- Desmantelamiento de datos codificados por borrado

3. Seleccione **Pausa** para suspender el procedimiento.

La etapa actual está en pausa y el botón **Reanudar** está habilitado.

 A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.

 Decommissioning procedure has been paused. Click 'Resume' to resume the procedure.

The progress for each node is displayed while the decommission procedure is running. When all tasks are complete, the node selection list is redisplayed.

Search 				
Name 	Type 	Progress 	Stage 	
DC1-S5	Storage Node		Evaluating ILM	

Pause

Resume

- Una vez finalizado el resto del procedimiento de mantenimiento, seleccione **Reanudar** para continuar con el desmantelamiento.

Sitio de desmantelamiento

Consideraciones para eliminar un sitio

Antes de utilizar el procedimiento de desmantelamiento del sitio para eliminar un sitio, debe revisar las consideraciones.

¿Qué sucede cuando se desmantela un sitio?

Cuando se desmantela un sitio, StorageGRID elimina de forma permanente todos los nodos del sitio y el sitio en sí del sistema StorageGRID .

Una vez finalizado el procedimiento de desmantelamiento del sitio:

- Ya no puede usar StorageGRID para ver o acceder al sitio ni a ninguno de los nodos del sitio.
- Ya no podrás utilizar ningún grupo de almacenamiento ni perfiles de codificación de borrado que hicieran referencia al sitio. Cuando StorageGRID desmantela un sitio, elimina automáticamente estos grupos de almacenamiento y desactiva estos perfiles de codificación de borrado.

Diferencias entre los procedimientos de desmantelamiento de sitios conectados y desconectados

Puede utilizar el procedimiento de desmantelamiento del sitio para eliminar un sitio en el que todos los nodos están conectados a StorageGRID (lo que se denomina desmantelamiento de sitio conectado) o para eliminar un sitio en el que todos los nodos están desconectados de StorageGRID (lo que se denomina desmantelamiento de sitio desconectado). Antes de comenzar, debes comprender las diferencias entre estos procedimientos.



Si un sitio contiene una mezcla de elementos conectados () y nodos desconectados ( o ) , debes volver a poner en línea todos los nodos fuera de línea.

- La desactivación de un sitio conectado le permite eliminar un sitio operativo del sistema StorageGRID .

Por ejemplo, puede realizar una desactivación de un sitio conectado para eliminar un sitio que es funcional pero que ya no es necesario.

- Cuando StorageGRID elimina un sitio conectado, utiliza ILM para administrar los datos de los objetos en el sitio. Antes de poder iniciar la desactivación de un sitio conectado, debe eliminar el sitio de todas las reglas de ILM y activar una nueva política de ILM. Los procesos ILM para migrar datos de objetos y los procesos internos para eliminar un sitio pueden ocurrir al mismo tiempo, pero la mejor práctica es permitir que los pasos ILM se completen antes de comenzar el procedimiento de desmantelamiento real.
- La desactivación de un sitio desconectado le permite eliminar un sitio fallido del sistema StorageGRID . Por ejemplo, puede realizar una desconexión del sitio para eliminar un sitio que haya sido destruido por un incendio o una inundación.

Cuando StorageGRID elimina un sitio desconectado, considera que todos los nodos son irrecuperables y no intenta preservar los datos. Sin embargo, antes de poder iniciar la desactivación de un sitio desconectado, debe eliminar el sitio de todas las reglas de ILM y activar una nueva política de ILM.



Antes de realizar un procedimiento de desconexión de un sitio, debe comunicarse con su representante de cuenta de NetApp . NetApp revisará sus requisitos antes de habilitar todos los pasos en el asistente de desmantelamiento del sitio. No debe intentar desmantelar un sitio desconectado si cree que es posible recuperar el sitio o recuperar datos de objetos del sitio.

Requisitos generales para eliminar un sitio conectado o desconectado

Antes de eliminar un sitio conectado o desconectado, debes tener en cuenta los siguientes requisitos:

- No se puede desmantelar un sitio que incluya el nodo de administración principal.
- No se puede desmantelar un sitio si alguno de los nodos tiene una interfaz que pertenece a un grupo de alta disponibilidad (HA). Debe editar el grupo HA para eliminar la interfaz del nodo o eliminar todo el grupo HA.
- No se puede desmantelar un sitio si contiene una mezcla de elementos conectados () y desconectado ( o ) nodos.
- No se puede desmantelar un sitio si algún nodo en cualquier otro sitio está desconectado ( o ).
- No se puede iniciar el procedimiento de desmantelamiento del sitio si hay una operación de reparación de nodo en curso. Ver "[Comprobar trabajos de reparación de datos](#)" para realizar un seguimiento de las reparaciones de datos codificados por borrado.
- Mientras se ejecuta el procedimiento de desmantelamiento del sitio:
 - No se pueden crear reglas ILM que hagan referencia al sitio que se va a desmantelar. Tampoco puedes editar una regla 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 el desmantelamiento de un sitio conectado, puede "[Pausar el procedimiento mientras se eliminan los nodos de almacenamiento](#)". El botón **Pausa** se habilita solo cuando se alcanzan las etapas de evaluación de ILM o de desmantelamiento de datos codificados por 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 desmantelamiento.

- Si necesita recuperar algún nodo después de iniciar el procedimiento de desmantelamiento del sitio, debe comunicarse con el soporte.
- No es posible desmantelar 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 su sistema StorageGRID, debe eliminar todas las relaciones de confianza de usuario autenticado para el 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 su configuración de ILM. El asistente de desmantelamiento del sitio lo guía a través de una serie de pasos previos necesarios para garantizar lo siguiente:

- El sitio no está referenciado por ninguna política de ILM. Si es así, debe editar las políticas o crear y activar políticas con nuevas reglas ILM.
- Ninguna regla de ILM se refiere al sitio, incluso si esas reglas no se utilizan en ninguna política. Debes eliminar o editar todas las reglas que hacen referencia al sitio.

Cuando StorageGRID desmantele el sitio, desactivará automáticamente todos los perfiles de codificación de borrado no utilizados que hagan referencia al sitio y eliminará automáticamente todos los grupos de almacenamiento no utilizados que hagan referencia al sitio. Si existe el grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores), se elimina porque utiliza todos los sitios.



Antes de poder eliminar un sitio, es posible que deba crear nuevas reglas ILM y activar una nueva política ILM. Estas instrucciones suponen que usted tiene un buen conocimiento de cómo funciona ILM y que está familiarizado con la creación de grupos de almacenamiento, perfiles de codificación de borrado, reglas de ILM y la simulación y activación de una política de ILM. Ver "[Administrar objetos con ILM](#)".

Consideraciones sobre los datos de objetos en un sitio conectado

Si está realizando una desactivación de un sitio conectado, debe decidir qué hacer con los datos de objetos existentes en el sitio cuando crea nuevas reglas ILM y una nueva política ILM. Puede realizar una o ambas de las siguientes acciones:

- Mueva datos de objetos del sitio seleccionado a uno o más sitios en su cuadrícula.

Ejemplo de movimiento de datos: Supongamos que desea desmantelar un sitio en Raleigh porque agregó un nuevo sitio en Sunnyvale. En este ejemplo, desea mover todos los datos de objetos del sitio antiguo al nuevo sitio. Antes de actualizar sus reglas y políticas de ILM, debe revisar la capacidad en ambos sitios. Debe asegurarse de que el sitio de Sunnyvale tenga suficiente capacidad para acomodar los datos de objetos del sitio de Raleigh y que permanezca en Sunnyvale la capacidad adecuada para el crecimiento futuro.



Para garantizar que haya suficiente capacidad disponible, es posible que necesite: "[expandir una cuadrícula](#)" agregando volúmenes de almacenamiento o nodos de almacenamiento a un sitio existente o agregando un nuevo sitio antes de realizar este procedimiento.

- Eliminar copias de objetos del sitio seleccionado.

Ejemplo de eliminación de datos: supongamos que actualmente utiliza una regla ILM de 3 copias para replicar datos de objetos en tres sitios. Antes de desmantelar un sitio, puede crear una regla ILM de 2 copias equivalente para almacenar datos en solo dos sitios. Cuando se activa una nueva política ILM que

utiliza la regla de 2 copias, StorageGRID elimina las copias del tercer sitio porque ya no satisfacen los requisitos de ILM. Sin embargo, los datos de los objetos seguirán protegidos y la capacidad de los dos sitios restantes seguirá siendo la misma.



Nunca cree una regla ILM de copia única para acomodar la eliminación de un sitio. Una regla ILM que crea solo una copia replicada por cada período de tiempo pone los datos en riesgo de pérdida permanente. Si solo existe una copia replicada de un objeto, ese objeto se pierde si un nodo de almacenamiento falla o tiene un error significativo. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como actualizaciones.

Requisitos adicionales para el desmantelamiento de un sitio conectado

Antes de que StorageGRID pueda eliminar un sitio conectado, debe asegurarse de lo siguiente:

- Todos los nodos de su sistema StorageGRID deben tener un estado de conexión de **Conectado** (); sin embargo, los nodos pueden tener alertas activas.



Puede completar los pasos 1 a 4 del asistente de desmantelamiento del sitio si uno o más nodos están desconectados. Sin embargo, no puede completar el Paso 5 del asistente, que inicia el proceso de desmantelamiento, a menos que todos los nodos estén conectados.

- Si el sitio que planea eliminar contiene un nodo de puerta de enlace o un nodo de administración que se utiliza para equilibrar la carga, es posible que deba [expandir una cuadrícula](#) para agregar un nuevo nodo equivalente en otro sitio. Asegúrese de que los clientes puedan conectarse al nodo de reemplazo antes de iniciar el procedimiento de desmantelamiento del sitio.
- Si el sitio que planea eliminar contiene algún nodo de puerta de enlace o nodos de administración que estén en un grupo de alta disponibilidad (HA), puede completar los pasos 1 a 4 del asistente de desmantelamiento del sitio. Sin embargo, no podrá completar el Paso 5 del asistente, que inicia el proceso de desmantelamiento, hasta que elimine estos nodos de todos los grupos de HA. Si los clientes existentes se conectan a un grupo de alta disponibilidad que incluye nodos del sitio, debe asegurarse de que puedan seguir conectándose a StorageGRID después de que se elimine el sitio.
- Si los clientes se conectan directamente a los nodos de almacenamiento en el sitio que planea eliminar, debe asegurarse de que puedan conectarse a los nodos de almacenamiento en otros sitios antes de comenzar el procedimiento de desmantelamiento del sitio.
- Debe proporcionar espacio suficiente en los sitios restantes para acomodar cualquier dato de objeto que se moverá debido a cambios en cualquier política ILM activa. En algunos casos, es posible que necesites [expandir una cuadrícula](#) agregando nodos de almacenamiento, volúmenes de almacenamiento o nuevos sitios antes de poder completar el desmantelamiento de un sitio conectado.
- Debe permitir tiempo suficiente para que se complete el procedimiento de desmantelamiento. Los procesos ILM de StorageGRID pueden tardar días, semanas o incluso meses en mover o eliminar datos de objetos del sitio antes de que este pueda desmantelarse.



Mover o eliminar datos de objetos de un sitio puede llevar días, semanas o incluso meses, dependiendo de la cantidad de datos en el sitio, la carga en su sistema, las latencias de la red y la naturaleza de los cambios ILM requeridos.

- Siempre que sea posible, debe completar los pasos 1 a 4 del asistente de desmantelamiento del sitio lo antes posible. El procedimiento de desmantelamiento se completará más rápidamente y con menos interrupciones e impactos en el rendimiento si permite que los datos se muevan del sitio antes de

comenzar el procedimiento de desmantelamiento real (seleccionando **Iniciar desmantelamiento** en el Paso 5 del asistente).

Requisitos adicionales para el desmantelamiento de un sitio desconectado

Antes de que StorageGRID pueda eliminar un sitio desconectado, debe asegurarse de lo siguiente:

- Se ha comunicado con su representante de cuenta de NetApp . NetApp revisará sus requisitos antes de habilitar todos los pasos en el asistente de desmantelamiento del sitio.



No debe intentar desmantelar un sitio desconectado si cree que es posible recuperar el sitio o recuperar algún dato de objeto del sitio. Ver "[Cómo el soporte técnico recupera un sitio](#)".

- Todos los nodos del sitio deben tener un estado de conexión de uno de los siguientes:
 - **Desconocido** (🌀): Por una razón desconocida, un nodo se desconecta o los servicios en el nodo dejan de funcionar inesperadamente. Por ejemplo, es posible que se haya detenido un servicio en el nodo o que el nodo haya perdido su conexión a la red debido a un corte de energía o una interrupción inesperada.
 - **Administrativamente caído** (🌑): El nodo no está conectado a la red por una razón esperada. Por ejemplo, el nodo o los servicios en el nodo se han apagado correctamente.
- Todos los nodos en todos los demás sitios deben tener un estado de conexión de **Conectado** (✅); sin embargo, estos otros nodos pueden tener alertas activas.
- Debe comprender que ya no podrá utilizar StorageGRID para ver ni recuperar ningún dato de objeto almacenado en el sitio. Cuando StorageGRID realiza este procedimiento, no intenta conservar ningún dato del sitio desconectado.



Si sus reglas y políticas de ILM fueron diseñadas para proteger contra la pérdida de un solo sitio, aún existen copias de sus objetos en los sitios restantes.

- Debes comprender que si el sitio contiene la única copia de un objeto, éste se pierde y no se puede recuperar.

Consideraciones para la coherencia al eliminar un sitio

La consistencia de un bucket S3 determina si StorageGRID replica completamente los metadatos del objeto en todos los nodos y sitios antes de informar a un cliente que la ingesta del objeto fue exitosa. La consistencia proporciona un equilibrio entre la disponibilidad de los objetos y la consistencia de esos objetos en diferentes nodos de almacenamiento y sitios.

Cuando StorageGRID elimina un sitio, debe asegurarse de que no se escriban datos en el sitio que se va a eliminar. Como resultado, anula temporalmente la consistencia de cada depósito o contenedor. Después de iniciar el proceso de desmantelamiento del sitio, StorageGRID utiliza temporalmente una consistencia de sitio fuerte para evitar que se escriban metadatos de objetos en el sitio que se está eliminando.

Como resultado de esta anulación temporal, tenga en cuenta que cualquier operación de escritura, actualización y eliminación de cliente que ocurra durante el desmantelamiento de un sitio puede fallar si varios nodos dejan de estar disponibles en los sitios restantes.

Reúna los materiales necesarios

Antes de desmantelar un sitio, debe obtener los siguientes materiales.

Artículo	Notas
Paquete de recuperación .zip archivo	Debes descargar el paquete de recuperación más reciente .zip archivo(<code>sgws-recovery-package-id-revision.zip</code>). Puede utilizar el archivo del paquete de recuperación para restaurar el sistema si ocurre una falla. "Descargar el paquete de recuperación"
`Passwords.txt` archivo	Este archivo contiene las contraseñas necesarias para acceder a los nodos de la red en la línea de comandos y está incluido en el paquete de recuperación.
Frase de contraseña de aprovisionamiento	La frase de contraseña se crea y se documenta cuando se instala por primera vez el sistema StorageGRID . La frase de contraseña de aprovisionamiento no está en el <code>Passwords.txt</code> archivo.
Descripción de la topología del sistema StorageGRID antes del desmantelamiento	Si está disponible, obtenga cualquier documentación que describa la topología actual del sistema.

Información relacionada

["Requisitos del navegador web"](#)

Paso 1: Seleccionar el sitio

Para determinar si un sitio puede ser desmantelado, comience accediendo al asistente de Desmantelamiento de Sitio.

Antes de empezar

- Has obtenido todos los materiales necesarios.
- Has revisado las consideraciones para eliminar un sitio.
- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de acceso root o permisos de Mantenimiento e ILM"](#) .

Pasos

1. Seleccione **MANTENIMIENTO > Tareas > Desmantelamiento**.
2. Seleccione **Sitio de desmantelamiento**.

Aparece el paso 1 (Seleccionar sitio) del asistente de desmantelamiento del sitio. Este paso incluye una lista alfabética de los sitios en su sistema StorageGRID .

Decommission Site

1

2

3

4

5

6

Select Site

View Details

Revise ILM Policy

Remove ILM References

Resolve Node Conflicts

Monitor Decommission

When you decommission a site, all nodes at the site and the site itself are permanently removed from the StorageGRID system.

Review the table for the site you want to remove. If Decommission Possible is Yes, select the site. Then, select **Next** to ensure that the site is not referred to by ILM and that all StorageGRID nodes are in the correct state.

You might not be able to remove certain sites. For example, you cannot decommission the site that contains the primary Admin Node or a site that contains an Archive Node.

Sites

	Site Name	Used Storage Capacity	Decommission Possible
☐	Raleigh	3.93 MB	
☐	Sunnyvale	3.97 MB	
	Vancouver	3.90 MB	No. This site contains the primary Admin Node.

Next

3. Vea los valores en la columna **Capacidad de almacenamiento utilizada** para determinar cuánto almacenamiento se está utilizando actualmente para los datos de objetos en cada sitio.

La capacidad de almacenamiento utilizada es una estimación. Si los nodos están fuera de línea, la capacidad de almacenamiento utilizada es el último valor conocido para el sitio.

- Para el desmantelamiento de un sitio conectado, este valor representa la cantidad de datos de objetos que será necesario mover a otros sitios o eliminar por ILM antes de poder desmantelar este sitio de manera segura.
- En el caso de la desconexión de un sitio, este valor representa la cantidad de almacenamiento de datos de su sistema que quedará inaccesible cuando desactive este sitio.



Si su política ILM fue diseñada para proteger contra la pérdida de un solo sitio, aún deberían existir copias de los datos de sus objetos en los sitios restantes.

4. Revise los motivos en la columna **Posible desmantelamiento** para determinar qué sitios se pueden desmantelar actualmente.



Si hay más de un motivo por el cual no se puede desmantelar un sitio, se muestra el motivo más crítico.

Desmantelamiento Posible motivo	Descripción	Siguiente paso
Marca de verificación verde ()	Puedes deshabilitar este sitio.	Vaya a el siguiente paso .

Desmantelamiento Posible motivo	Descripción	Siguiente paso
No. Este sitio contiene el nodo de administración principal.	No se puede desmantelar un sitio que contenga el nodo de administración principal.	Ninguno. No puedes realizar este procedimiento.
No. Este sitio contiene uno o más nodos de archivo.	No se puede desmantelar un sitio que contenga un nodo de archivo.	Ninguno. No puedes realizar este procedimiento.
No. Todos los nodos de este sitio están desconectados. Comuníquese con su representante de cuenta de NetApp .	No se puede realizar la desactivación de un sitio conectado a menos que todos los nodos del sitio estén conectados ().	Si desea realizar una desconexión de un sitio desconectado, debe comunicarse con su representante de cuenta de NetApp , quien revisará sus requisitos y habilitará el resto del asistente de desconexión de sitio. IMPORTANTE: Nunca desconectes nodos en línea para poder eliminar un sitio. Perderás 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 desmantelar esos sitios. Sin embargo, no puedes desmantelar el sitio de Vancouver porque contiene el nodo de administración principal.

1. Si es posible desmantelar el sitio, seleccione el botón de opción correspondiente.

El botón **Siguiente** está habilitado.

2. Seleccione **Siguiente**.

Aparece el paso 2 (Ver detalles).

Paso 2: Ver detalles

Desde el Paso 2 (Ver detalles) del asistente de desmantelamiento del sitio, 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 su red.

Antes de empezar

Antes de desmantelar un sitio, debe revisar cuántos datos de objetos existen en el sitio.

- Si está realizando una desactivación de un sitio conectado, debe comprender cuántos datos de objetos existen actualmente en el sitio antes de actualizar ILM. Según las capacidades del sitio y sus necesidades de protección de datos, puede crear nuevas reglas ILM para mover datos a otros sitios o eliminar datos de objetos del sitio.
- Realice cualquier expansión de nodo de almacenamiento necesaria antes de iniciar el procedimiento de

desmantelamiento, si es posible.

- Si está realizando una desactivación de un sitio desconectado, debe comprender cuántos datos de objetos quedarán permanentemente inaccesibles cuando elimine el sitio.

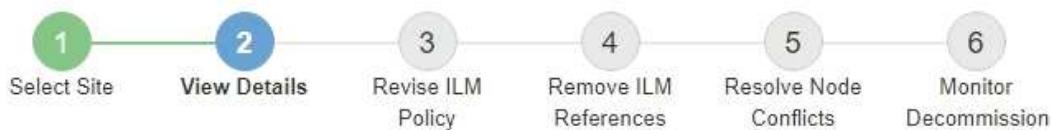


Si está realizando una desactivación de un sitio desconectado, ILM no puede mover ni eliminar datos de objetos. Cualquier dato que permanezca en el sitio se perderá. Sin embargo, si su política ILM fue diseñada para proteger contra la pérdida de un solo sitio, aún existen copias de los datos de sus objetos en los sitios restantes. Ver "[Habilitar la protección contra pérdida de sitios](#)".

Pasos

1. Desde el Paso 2 (Ver detalles), revise todas las advertencias relacionadas con el sitio que seleccionó eliminar.

Decommission Site



Data Center 2 Details

⚠ This site includes a Gateway Node. If clients are currently connecting to this node, you must configure an equivalent node at another site. Be sure clients can connect to the replacement node before starting the decommission procedure.

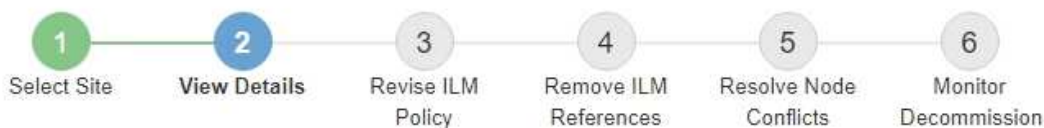
⚠ This site contains a mixture of connected and disconnected nodes. Before you can remove this site, you must bring all offline (blue or gray) nodes back online. Contact technical support if you need assistance.

En estos casos aparece una advertencia:

- El sitio incluye un nodo de enlace. Si los clientes S3 se están conectando actualmente a este nodo, debe configurar un nodo equivalente en otro sitio. Asegúrese de que los clientes puedan conectarse al nodo de reemplazo antes de continuar con el procedimiento de desmantelamiento.
- El sitio contiene una mezcla de (✅) y nodos desconectados (🌑 o 🔄). Antes de poder eliminar este sitio, debes volver a poner en línea todos los nodos fuera de línea.

2. Revise los detalles sobre el sitio que seleccionó eliminar.

Decommission Site



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	Connection 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](#)

La siguiente información se incluye para el sitio seleccionado:

- Número de nodos
- El espacio total utilizado, el espacio libre y la capacidad de todos los nodos de almacenamiento en el sitio.
 - Para el desmantelamiento de un sitio conectado, el valor **Espacio utilizado** representa la cantidad de datos de objetos que se deben mover a otros sitios o eliminar con ILM.
 - En el caso de la desactivación de un sitio desconectado, el valor **Espacio utilizado** indica la cantidad de datos de objetos que se volverán inaccesibles cuando se elimine el sitio.
- Nombres de nodos, tipos y estados de conexión:
 -  (Conectado)
 -  (Administrativamente caído)
 -  (Desconocido)
- Detalles sobre cada nodo:
 - Para cada nodo de almacenamiento, la cantidad de espacio que se ha utilizado para los datos del

objeto.

- Para los nodos de administración y los nodos de puerta de enlace, si el nodo se utiliza actualmente en un grupo de alta disponibilidad (HA). No se puede dismantelar un nodo de administración o un nodo de puerta de enlace que se utilice en un grupo de alta disponibilidad. Antes de comenzar el dismantelamiento, edite los grupos de HA para eliminar todos los nodos del sitio o elimine el grupo de HA si solo incluye nodos de este sitio. Para obtener instrucciones, consulte "[Administrar grupos de alta disponibilidad \(HA\)](#)".

3. En la sección Detalles de otros sitios de la página, evalúe cuánto espacio está disponible en los otros sitios de su 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 está realizando una desactivación de un sitio conectado y planea usar ILM para mover datos de objetos del sitio seleccionado (en lugar de simplemente eliminarlos), debe asegurarse de que los otros sitios tengan suficiente capacidad para acomodar los datos movidos y que quede capacidad adecuada para el crecimiento futuro.



Aparece una advertencia si el **Espacio utilizado** del sitio que desea eliminar es mayor que el **Espacio libre total para otros sitios**. Para garantizar que haya capacidad de almacenamiento adecuada disponible después de eliminar el sitio, es posible que deba realizar una expansión antes de realizar este procedimiento.

4. Seleccione **Siguiente**.

Aparece el paso 3 (Revisar la política de ILM).

Paso 3: Revisar las políticas de ILM

Desde el Paso 3 (Revisar políticas de ILM) del asistente de dismantelamiento de sitio, puede determinar si el sitio está referenciado por alguna política de ILM.

Antes de empezar

Tienes una buena comprensión de cómo "[gestionar objetos con ILM](#)". Está familiarizado con la creación de grupos de almacenamiento y reglas ILM y con la simulación y activación de una política ILM.

Acerca de esta tarea

StorageGRID no puede dar de baja un sitio si alguna regla ILM en cualquier política (activa o inactiva) hace referencia a ese sitio.

Si alguna política de ILM hace referencia al sitio que desea dismantelar, debe eliminar esas políticas o editarlas para que cumplan con estos requisitos:

- Proteja completamente todos los datos de los objetos.
- No haga referencia al sitio que estás desmantelando.
- No utilice grupos de almacenamiento que hagan referencia al sitio ni utilice la opción Todos los sitios.
- No utilice perfiles de codificación de borrado que hagan referencia al sitio.
- No utilice la regla Hacer 2 copias de StorageGRID 11.6 o instalaciones anteriores.



Nunca cree una regla ILM de copia única para acomodar la eliminación de un sitio. Una regla ILM que crea solo una copia replicada por cada período de tiempo pone los datos en riesgo de pérdida permanente. Si solo existe una copia replicada de un objeto, ese objeto se pierde si un nodo de almacenamiento falla o tiene un error significativo. También perderá temporalmente el acceso al objeto durante procedimientos de mantenimiento, como actualizaciones.



Si está realizando una *desactivación de un sitio conectado*, debe considerar cómo StorageGRID debe administrar los datos de los objetos que se encuentran actualmente en el sitio que desea eliminar. Dependiendo de sus requisitos de protección de datos, las nuevas reglas pueden mover datos de objetos existentes a diferentes sitios o pueden eliminar cualquier copia de objetos adicional que ya no sea necesaria.

Comuníquese con el soporte técnico si necesita ayuda para diseñar una nueva política.

Pasos

1. En el Paso 3 (Revisar las políticas de ILM), determine si alguna política de ILM se refiere al sitio que seleccionó desmantelar.
2. Si no se enumeran políticas, seleccione **Siguiente** para ir a "[Paso 4: Eliminar referencias ILM](#)".
3. Si se enumeran una o más políticas ILM *activas*, clone cada política existente o cree nuevas políticas que no hagan referencia al sitio que se va a desmantelar:
 - a. Seleccione el enlace de la política en la columna Nombre de la política.

La página de detalles de la política ILM aparece en una nueva pestaña del navegador. La página del Sitio de Desmantelamiento permanecerá abierta en la otra pestaña.

- b. Siga estas pautas e instrucciones según sea necesario:

- Trabajar con reglas ILM:
 - "[Crear uno o más grupos de almacenamiento](#)" que no hagan referencia al sitio.
 - "[Editar o reemplazar reglas](#)" que hacen referencia al sitio.



No seleccione la regla **Hacer 2 copias** porque esa regla utiliza el grupo de almacenamiento **Todos los nodos de almacenamiento**, lo cual no está permitido.

- Trabajar con las políticas de ILM:
 - "[Clonar una política ILM existente](#)" o "[crear una nueva política ILM](#)".
 - Asegúrese de que la regla predeterminada y otras reglas no hagan referencia al sitio.



Debes confirmar que las reglas de ILM estén en el orden correcto. Cuando se activa la política, los objetos nuevos y existentes se evalúan mediante las reglas en el orden enumerado, comenzando desde arriba.

c. Ingera objetos de prueba y simule la política para garantizar que se apliquen las reglas correctas.



Los errores en una política ILM pueden provocar una pérdida de datos irrecuperable. Revise cuidadosamente y simule la política antes de activarla para confirmar que funcionará según lo previsto.



Cuando activa una nueva política ILM, StorageGRID la utiliza para administrar todos los objetos, incluidos los objetos existentes y los objetos recientemente ingeridos. Antes de activar una nueva política ILM, revise cualquier cambio en la ubicación de los objetos replicados y codificados por borrado existentes. Cambiar la ubicación de un objeto existente podría generar problemas de recursos temporales cuando se evalúen e implementen las nuevas ubicaciones.

d. Active las nuevas políticas y asegúrese de que las políticas antiguas ahora estén inactivas.

Si desea activar varias políticas, ["Siga los pasos para crear etiquetas de política ILM"](#).

Si está realizando una desactivación de un sitio conectado, StorageGRID comienza a eliminar datos de objetos del sitio seleccionado tan pronto como activa la nueva política ILM. Mover o eliminar todas las copias de objetos podría llevar semanas. Si bien puede iniciar de forma segura el desmantelamiento de un sitio mientras aún existen datos de objetos en el sitio, el procedimiento de desmantelamiento se completará más rápidamente y con menos interrupciones e impactos en el rendimiento si permite que los datos se muevan del sitio antes de iniciar el procedimiento de desmantelamiento real (seleccionando **Iniciar desmantelamiento** en el Paso 5 del asistente).

4. Para cada política *inactiva*, edítela o elimínela seleccionando primero el enlace para cada política como se describe en los pasos anteriores.
 - ["Editar la política"](#) por lo que no se refiere al sitio que se va a desmantelar.
 - ["Eliminar una política"](#).
5. Cuando termine de realizar cambios en las reglas y políticas de ILM, no debería haber más políticas enumeradas en el Paso 3 (Revisar políticas de ILM). Seleccione **Siguiente**.

Aparece el paso 4 (Eliminar referencias ILM).

Paso 4: Eliminar referencias ILM

Desde el Paso 4 (Eliminar referencias ILM) del asistente de desmantelamiento del sitio, debe eliminar o editar cualquier regla ILM no utilizada que haga referencia al sitio, incluso si las reglas no se utilizan en ninguna política ILM.

Pasos

1. Determinar si alguna regla ILM no utilizada hace referencia al sitio.

Si se enumeran reglas de ILM, esas reglas aún hacen referencia al sitio pero no se utilizan en ninguna política.



Cuando StorageGRID desmantele el sitio, desactivará automáticamente todos los perfiles de codificación de borrado no utilizados que hagan referencia al sitio y eliminará automáticamente todos los grupos de almacenamiento no utilizados que hagan referencia al sitio. El grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores) se elimina porque utiliza el sitio Todos los sitios.

2. Editar o eliminar cada regla no utilizada:

- Para editar una regla, vaya a la página de reglas de ILM y actualice todas las ubicaciones que usan un perfil de codificación de borrado o un grupo de almacenamiento que hace referencia al sitio. Luego, regrese al **Paso 4 (Eliminar referencias ILM)**.
- Para eliminar una regla, seleccione el icono de la papelera  y seleccione **OK**.



Debes eliminar la regla **Hacer 2 copias** antes de poder dar de baja un sitio.

3. Confirme que no haya reglas ILM no utilizadas que hagan referencia al sitio y que el botón **Siguiente** esté habilitado.

4. Seleccione **Siguiente**.



Cualquier grupo de almacenamiento restante y perfil de codificación de borrado que haga referencia al sitio dejarán de ser válidos cuando se elimine el sitio. Cuando StorageGRID desmantele el sitio, desactivará automáticamente todos los perfiles de codificación de borrado no utilizados que hagan referencia al sitio y eliminará automáticamente todos los grupos de almacenamiento no utilizados que hagan referencia al sitio. El grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores) se elimina porque utiliza el sitio Todos los sitios.

Aparece el paso 5 (Resolver conflictos de nodos).

Paso 5: Resolver los conflictos de nodos (y comenzar el desmantelamiento)

Desde el Paso 5 (Resolver conflictos de nodos) del Asistente para desmantelar el sitio, puede determinar si algún nodo en su sistema StorageGRID está desconectado o si algún nodo en el sitio seleccionado pertenece a un grupo de alta disponibilidad (HA). Una vez resueltos los conflictos de nodos, puede iniciar el procedimiento de desmantelamiento desde esta página.

Antes de empezar

Debe asegurarse de que todos los nodos de su sistema StorageGRID estén en el estado correcto, de la siguiente manera:

- Todos los nodos de su sistema StorageGRID deben estar conectados ().



Si está realizando una desconexión de un sitio desconectado, todos los nodos del sitio que está eliminando deben estar desconectados y todos los nodos de todos los demás sitios deben estar conectados.



La desactivación no se iniciará si uno o más volúmenes están fuera de línea (desmontados) o si están en línea (montados) pero en un estado de error.



Si uno o más volúmenes se desconectan mientras se lleva a cabo un desmantelamiento, el proceso de desmantelamiento se completa después de que estos volúmenes vuelvan a estar en línea.

- Ningún nodo del sitio que está eliminando puede tener una interfaz que pertenezca a un grupo de alta disponibilidad (HA).

Acerca de esta tarea

Si algún nodo aparece en la lista del Paso 5 (Resolver conflictos de nodos), debe corregir el problema antes de poder comenzar el desmantelamiento.

Antes de iniciar el procedimiento de desmantelamiento del sitio desde esta página, revise las siguientes consideraciones:

- Debe permitir tiempo suficiente para que se complete el procedimiento de desmantelamiento.



Mover o eliminar datos de objetos de un sitio puede llevar días, semanas o incluso meses, dependiendo de la cantidad de datos en el sitio, la carga en su sistema, las latencias de la red y la naturaleza de los cambios ILM requeridos.

- Mientras se ejecuta el procedimiento de desmantelamiento del sitio:
 - No se pueden crear reglas ILM que hagan referencia al sitio que se va a desmantelar. Tampoco puedes editar una regla 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 el desmantelamiento de un sitio conectado, puede pausar el procedimiento mientras se eliminan los nodos de almacenamiento. El botón **Pausa** está habilitado durante la etapa de "Desmantelamiento de datos replicados y codificados por borrado".

- Si necesita recuperar algún nodo después de iniciar el procedimiento de desmantelamiento del sitio, debe comunicarse con el soporte.

Pasos

1. Revise la sección de nodos desconectados del Paso 5 (Resolver conflictos de nodos) para determinar si algún nodo en su sistema StorageGRID tiene un estado de conexión desconocido () o Administrativamente Inactivo () .

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

1 disconnected node in the grid

The following nodes have a Connection State of Unknown (blue) or Administratively Down (gray). You must bring these disconnected nodes back online.

For help bringing nodes back online, see the instructions for [monitoring and troubleshooting StorageGRID](#) and the [recovery and maintenance](#) instructions.

Node Name	Connection State	Site	Type
DC1-S3-99-193	Administratively Down	Data Center 1	Storage Node

1 node in the selected site belongs to an HA group

Passphrase

Provisioning Passphrase

Previous

Start Decommission

2. Si algún nodo está desconectado, vuelva a ponerlo en línea.

Ver el "[Procedimientos de nodo](#)". Comuníquese con el soporte técnico si necesita ayuda.

3. Cuando todos los nodos desconectados se hayan vuelto a poner en línea, revise la sección Grupos de alta disponibilidad del Paso 5 (Resolver conflictos de nodos).

Esta tabla enumera todos los nodos en el sitio seleccionado que pertenecen a un grupo de alta disponibilidad (HA).

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue:

All grid nodes are connected

1 node in the selected site belongs to an HA group

The following nodes in the selected site belong to a high availability (HA) group. You must either edit the HA group to remove the node's interface or remove the entire HA group.

[Go to HA Groups page.](#)

For information about HA groups, see the instructions for [administering StorageGRID](#)

HA Group Name	Node Name	Node Type
HA group	DC1-GW1-99-190	API Gateway Node

Passphrase

Provisioning Passphrase ?

Previous

Start Decommission

4. Si hay nodos enumerados, realice una de las siguientes acciones:

- Edite cada grupo de HA afectado para eliminar la interfaz del nodo.
- Eliminar un grupo de HA que solo incluya nodos de este sitio. Consulte las instrucciones para administrar StorageGRID.

Si todos los nodos están conectados y ningún nodo en el sitio seleccionado se utiliza en un grupo de alta disponibilidad, se habilita el campo **Frase de contraseña de aprovisionamiento**.

5. Introduzca la contraseña de aprovisionamiento.

Se habilita el botón **Iniciar desmantelamiento**.

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be offline.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

All grid nodes are connected

No nodes in the selected site belong to an HA group

Passphrase

Provisioning Passphrase ?

.....|

Previous

Start Decommission

6. Si está listo para iniciar el procedimiento de desmantelamiento del sitio, seleccione **Iniciar desmantelamiento**.

Una advertencia enumera el sitio y los nodos que se eliminarán. Se le recuerda que podría tomar días, semanas o incluso meses eliminar el sitio por completo.

Warning

The following site and its nodes have been selected for decommissioning and will be permanently removed from the StorageGRID system:

Data Center 3

- DC3-S1
- DC3-S2
- DC3-S3

When StorageGRID removes a site, it temporarily uses strong-site consistency to prevent object metadata from being written to the site being removed. Client write and delete operations can fail if multiple nodes become unavailable at the remaining sites.

This procedure might take days, weeks, or even months to complete. Select **Maintenance > Decommission** to monitor the decommission progress.

Do you want to continue?

Cancel

OK

7. Revise la advertencia. Si está listo para comenzar, seleccione **Aceptar**.

Aparece un mensaje a medida que se genera la nueva configuración de la cuadrícula. Este proceso puede llevar algún tiempo, dependiendo del tipo y número de nodos de red dados de baja.

Passphrase

Provisioning Passphrase 

 Generating grid configuration. This may take some time depending on the type and the number of decommissioned grid nodes.

Previous

Start Decommission 

Una vez generada la nueva configuración de la red, aparece el Paso 6 (Desmantelamiento del monitor).



El botón **Anterior** permanecerá deshabilitado hasta que se complete el desmantelamiento.

Paso 6: Supervisar el desmantelamiento

Desde el Paso 6 (Monitorear Desmantelamiento) del asistente de página de Desmantelamiento del Sitio, puede monitorear el progreso a medida que se elimina el sitio.

Acerca de esta tarea

Cuando StorageGRID elimina un sitio conectado, elimina los nodos en este orden:

1. Nodos de puerta de enlace
2. Nodos de administración
3. Nodos de almacenamiento

Cuando StorageGRID elimina un sitio desconectado, elimina los nodos en este 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 administración solo requiera unos minutos o una hora para eliminarse; sin embargo, los nodos de almacenamiento pueden demorar días o semanas.

Pasos

1. Tan pronto como se haya generado un nuevo paquete de recuperación, descargue el archivo.

Decommission Site



i A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.



Descargue el paquete de recuperación lo antes posible para asegurarse de poder recuperar su red si algo sale mal durante el procedimiento de desmantelamiento.

- a. Seleccione el enlace en el mensaje o seleccione **MANTENIMIENTO > Sistema > Paquete de recuperación**.
- b. Descargar el .zip archivo.

Vea las instrucciones para ["descargando el paquete de recuperación"](#) .

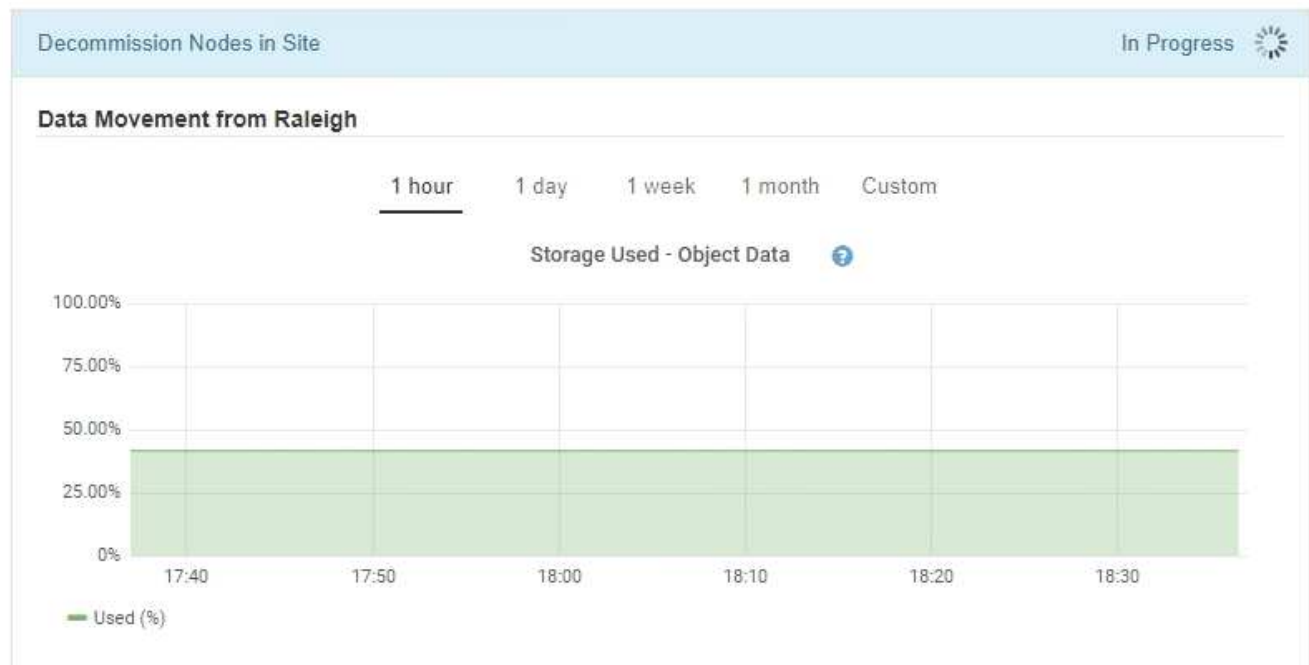


El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

2. Utilizando el gráfico de movimiento de datos, monitoree el movimiento de datos de objetos desde este sitio a otros sitios.

El movimiento de datos comenzó cuando activó la nueva política ILM en el Paso 3 (Revisar la política ILM). El movimiento de datos se producirá durante todo el procedimiento de desmantelamiento.

Decommission Site Progress



3. En la sección Progreso del nodo de la página, supervise el progreso del procedimiento de desmantelamiento a medida que se eliminan los nodos.

Cuando se elimina un nodo de almacenamiento, cada nodo pasa por una serie de etapas. Aunque la mayoría de estas etapas ocurren rápidamente o incluso de manera imperceptible, es posible que tengas que esperar días o incluso semanas para que se completen otras etapas, según la cantidad de datos que deban trasladarse. Se requiere tiempo adicional para gestionar los datos codificados por borrado y reevaluar ILM.

Node Progress

 Depending on the number of objects stored, Storage Nodes might take significantly longer to decommission. Extra time is needed to manage erasure coded data and re-evaluate ILM.

The progress for each node is displayed while the decommission procedure is running. If you need to perform another maintenance procedure, select **Pause** to suspend the decommission (only allowed during certain stages).

Pause **Resume**

Search 				
Name 	Type 	Progress 	Stage 	
RAL-S1-101-196	Storage Node		Decommissioning Replicated and Erasure Coded Data	
RAL-S2-101-197	Storage Node		Decommissioning Replicated and Erasure Coded Data	
RAL-S3-101-198	Storage Node		Decommissioning Replicated and Erasure Coded Data	

Si está supervisando el progreso de la desactivación de un sitio conectado, consulte esta tabla para comprender las etapas de desactivación de un nodo de almacenamiento:

Escenario	Duración estimada
Pending	Minuto o menos
Esperar a que se bloqueen	Minutos
Preparar tarea	Minuto o menos
Marcando LDR Desmantelado	Minutos
Desmantelamiento de datos replicados y codificados por borrado	Horas, días o semanas según la cantidad de datos Nota: Si necesita realizar otras actividades de mantenimiento, puede pausar el desmantelamiento del sitio durante esta etapa.
Estado del conjunto LDR	Minutos
Vaciar colas de auditoría	Minutos a horas, según la cantidad de mensajes y la latencia de la red.
Completo	Minutos

Si está supervisando el progreso de la desconexión de un sitio desconectado, consulte esta tabla para comprender las etapas de desconexión de un nodo de almacenamiento:

Escenario	Duración estimada
Pending	Minuto o menos
Esperar a que se bloqueen	Minutos
Preparar tarea	Minuto o menos
Deshabilitar servicios externos	Minutos
Revocación de certificado	Minutos
Anular registro de nodo	Minutos
Cancelar registro de grado de almacenamiento	Minutos
Eliminación del grupo de almacenamiento	Minutos
Eliminación de entidades	Minutos

Escenario	Duración estimada
Completo	Minutos

4. Una vez que todos los nodos hayan alcanzado la etapa Completado, espere a que se completen las operaciones de desmantelamiento del sitio restantes.
 - Durante el paso **Reparar Cassandra**, StorageGRID realiza todas las reparaciones necesarias en los clústeres de Cassandra que permanecen en su red. Estas reparaciones pueden tardar varios días o más, dependiendo de cuántos nodos de almacenamiento queden en su red.

Decommission Site Progress

Decommission Nodes in Site	Completed
Repair Cassandra	In Progress 
StorageGRID is repairing the remaining Cassandra clusters after removing the site. This might take several days or more, depending on how many Storage Nodes remain in your grid.	
Overall Progress	0%
Deactivate EC Profiles & Delete Storage Pools	Pending
Remove Configurations	Pending

- Durante el paso **Desactivar perfiles EC y eliminar grupos de almacenamiento**, se realizan los siguientes cambios en ILM:
 - Se desactivan todos los perfiles con codificación de borrado que remiten al sitio.
 - Se eliminan todos los grupos de almacenamiento que hacen referencia al sitio.



El grupo de almacenamiento Todos los nodos de almacenamiento (StorageGRID 11.6 y anteriores) también se elimina porque utiliza el sitio Todos los sitios.

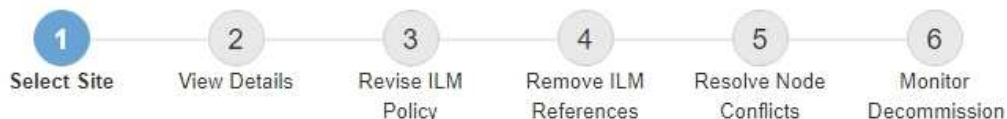
- Finalmente, durante el paso **Eliminar configuración**, cualquier referencia restante al sitio y sus nodos se eliminan del resto de la cuadrícula.

Decommission Site Progress

Decommission Nodes in Site	Completed
Repair Cassandra	Completed
Deactivate EC Profiles & Delete Storage Pools	Completed
Remove Configurations	In Progress 
StorageGRID is removing the site and node configurations from the rest of the grid.	

5. Una vez completado el procedimiento de desmantelamiento, la página del sitio de desmantelamiento muestra un mensaje de éxito y el sitio eliminado ya no se muestra.

Decommission Site



The previous decommission procedure completed successfully at 2021-01-12 14:28:32 MST.

When you decommission a site, all nodes at the site and the site itself are permanently removed from the StorageGRID system.

Review the table for the site you want to remove. If Decommission Possible is Yes, select the site. Then, select **Next** to ensure that the site is not referred to by ILM and that all StorageGRID nodes are in the correct state.

You might not be able to remove certain sites. For example, you cannot decommission the site that contains the primary Admin Node or a site that contains an Archive Node.

Sites

	Site Name	Used Storage Capacity ?	Decommission Possible
☒	Sunnyvale	4.79 MB	✓
☐	Vancouver	4.90 MB	No. This site contains the primary Admin Node.

Next

Después de terminar

Complete estas tareas después de completar el procedimiento de desmantelamiento del sitio:

- Asegúrese de que las unidades de todos los nodos de almacenamiento en el sitio fuera de servicio estén limpias. Utilice una herramienta o servicio de borrado de datos disponible comercialmente para eliminar datos de las unidades de forma permanente y segura.
- Si el sitio incluía uno o más nodos de administración y el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID, elimine todas las relaciones de confianza de usuario autenticado para el sitio de los Servicios de federación de Active Directory (AD FS).
- Una vez que los nodos se hayan apagado automáticamente como parte del procedimiento de desmantelamiento del sitio conectado, elimine las máquinas virtuales asociadas.

Cambiar el nombre de la cuadrícula, el sitio o el nodo

Utilice el procedimiento de cambio de nombre

Según sea necesario, puede cambiar los nombres para mostrar que se muestran en todo el Administrador de cuadrícula para toda la cuadrícula, cada sitio y cada nodo. Puede actualizar los nombres para mostrar de forma segura y cuando lo necesite.

¿Cuál es el procedimiento de cambio de nombre?

Cuando instala StorageGRID inicialmente, especifica un nombre para la red, cada sitio y cada nodo. Estos nombres iniciales se conocen como *nombres del sistema* y son los nombres que se muestran inicialmente en StorageGRID.

Los nombres de sistema son necesarios para las operaciones internas de StorageGRID y no se pueden cambiar. Sin embargo, puede utilizar el procedimiento de cambio de nombre para definir nuevos *nombres para mostrar* para la cuadrícula, cada sitio y cada nodo. Estos nombres para mostrar aparecen en varias ubicaciones de StorageGRID en lugar de (o en algunos casos, además de) los nombres del sistema subyacente.

Utilice el procedimiento de cambio de nombre para corregir errores tipográficos, implementar una convención de nomenclatura diferente o indicar que un sitio y todos sus nodos han sido reubicados. A diferencia de los nombres de sistema, los nombres para mostrar se pueden actualizar cuando sea necesario y sin afectar las operaciones de StorageGRID .

¿Dónde aparecen los nombres del sistema y de la pantalla?

La siguiente tabla resume dónde se muestran los nombres del sistema y los nombres para mostrar en la interfaz de usuario de StorageGRID y en los archivos de StorageGRID .

Ubicación	Nombre del sistema	Nombre para mostrar
Páginas del administrador de cuadrícula	Se muestra a menos que se cambie el nombre del elemento	Si se cambia el nombre de un elemento, se muestra en lugar del nombre del sistema en estas ubicaciones: • Consola • Página de nodos • Páginas de configuración para grupos de alta disponibilidad, puntos finales de balanceador de carga, interfaces VLAN, servidores de administración de claves, contraseñas de red y control de firewall • Alertas • Definiciones de grupos de almacenamiento • Página de búsqueda de metadatos de objetos • Páginas relacionadas con los procedimientos de mantenimiento, incluidas actualizaciones, revisiones, actualizaciones del sistema operativo SANtricity , desmantelamiento, expansión, recuperación y verificación de existencia de objetos. • Páginas de soporte (registros y diagnósticos) • Página de inicio de sesión único, junto al nombre de host del nodo de administración en la tabla de detalles del nodo de administración
NODOS > Pestaña Descripción general de un nodo	Siempre mostrado	Se muestra solo si se cambia el nombre del elemento
Páginas heredadas en el Administrador de cuadrícula (por ejemplo, SOPORTE > Topología de cuadrícula)	Mostrado	No se muestra
API de salud del nodo	Siempre regresaba	Se devuelve solo si se cambia el nombre del artículo

Ubicación	Nombre del sistema	Nombre para mostrar
Aviso al usar SSH para acceder a un nodo	Se muestra como nombre principal a menos que se haya cambiado el nombre del elemento: <pre>admin@SYSTEM-NAME: ~ \$</pre> Incluido entre paréntesis cuando se cambia el nombre del elemento: <pre>admin@DISPLAY-NAME (SYSTEM-NAME) :~ \$</pre>	Se muestra como nombre principal cuando se cambia el nombre del elemento: <pre>admin@DISPLAY-NAME (SYSTEM-NAME) :~ \$</pre>
`Passwords.txt` archivo en el paquete de recuperación	Se muestra como Server Name	Se muestra como Display Name
`/etc/hosts` archivo en todos los nodos Por ejemplo: <pre>10.96.99.128 SYSTEM-NAME 28989c59-a2c3-4d30-bb09-6879adf2437f DISPLAY-NAME localhost-grid # storagegrid-gen-host</pre>	Siempre se muestra en la segunda columna	Cuando se cambia el nombre del elemento, se muestra en la cuarta columna
topology-display-names.json, incluido con los datos de AutoSupport	No incluido	Vacío a menos que se hayan cambiado el nombre de los elementos; de lo contrario, asigna los identificadores de cuadrícula, sitio y nodo a sus nombres para mostrar.

Requisitos del nombre para mostrar

Antes de utilizar este procedimiento, revise los requisitos para los nombres para mostrar.

Nombres para mostrar de los nodos

Los nombres para mostrar de los nodos deben seguir estas reglas:

- Debe ser único en todo el sistema StorageGRID .
- No puede ser el mismo que el nombre del sistema de ningún otro elemento en su sistema StorageGRID .
- Debe contener al menos 1 y no más de 32 caracteres.
- Puede contener números, guiones (-) y letras mayúsculas y minúsculas.
- Puede comenzar o terminar con una letra o un número, pero no puede comenzar o terminar con un guion.

- No pueden ser todos números.
- No distinguen entre mayúsculas y minúsculas. Por ejemplo, DC1-ADM y dc1-adm se consideran duplicados.

Puede cambiar el nombre de un nodo con un nombre para mostrar que haya sido utilizado previamente por un nodo diferente, siempre y cuando el cambio de nombre no genere un nombre para mostrar o un nombre de sistema duplicados.

Nombres para mostrar en la cuadrícula y los sitios

Los nombres para mostrar de la cuadrícula y los sitios siguen las mismas reglas con estas excepciones:

- Puede incluir espacios.
- Puede incluir estos caracteres especiales: = - _ : , . @ !
- Puede comenzar y terminar con caracteres especiales, incluidos guiones.
- Pueden ser todos números o caracteres especiales.

Prácticas recomendadas para nombres para mostrar

Si planea cambiar el nombre de varios elementos, documente su esquema de nombres general antes de utilizar este procedimiento. Piense en un sistema que garantice que los nombres sean únicos, consistentes y fáciles de entender a simple vista.

Puede utilizar cualquier convención de nomenclatura que se ajuste a los requisitos de su organización. Tenga en cuenta estas sugerencias básicas de qué incluir:

- **Indicador de sitio:** si tiene varios sitios, agregue un código de sitio a cada nombre de nodo.
- **Tipo de nodo:** Los nombres de los nodos generalmente indican el tipo del nodo. Puedes utilizar abreviaturas como s , adm , y gw (Nodo de almacenamiento, Nodo de administración y Nodo de puerta de enlace).
- **Número de nodo:** si un sitio contiene más de un nodo de un tipo particular, agregue un número único al nombre de cada nodo.

Piénselo dos veces antes de agregar detalles específicos a los nombres que probablemente cambiarán con el tiempo. Por ejemplo, no incluya direcciones IP en los nombres de los nodos porque estas direcciones pueden cambiarse. De manera similar, las ubicaciones de los racks o los números de modelo de los dispositivos pueden cambiar si usted mueve el equipo o actualiza el hardware.

Ejemplos de nombres para mostrar

Supongamos que su sistema StorageGRID tiene tres centros de datos y nodos de diferentes tipos en cada centro de datos. Tus nombres para mostrar podrían ser tan simples como estos:

- **Red:** StorageGRID Deployment
- **Primer sitio:** Data Center 1
 - dc1-adm1
 - dc1-s1
 - dc1-s2
 - dc1-s3

- dc1-gw1

- **Segundo sitio:** Data Center 2

- dc2-adm2

- dc2-s1

- dc2-s2

- dc2-s3

- **Tercer sitio:** Data Center 3

- dc3-s1

- dc3-s2

- dc3-s3

Agregar o actualizar nombres para mostrar

Puede utilizar este procedimiento para agregar o actualizar los nombres para mostrar utilizados para su cuadrícula, sitios y nodos. Puede cambiar el nombre de un solo elemento, de varios elementos o incluso de todos los elementos al mismo tiempo. Definir o actualizar un nombre para mostrar no afecta las operaciones de StorageGRID de ninguna manera.

Antes de empezar

- Desde el **Nodo de administración principal**, inicia sesión en el Administrador de cuadrícula mediante un ["navegador web compatible"](#).



Puede agregar o actualizar nombres para mostrar desde un nodo de administración que no sea el principal, pero debe iniciar sesión en el nodo de administración principal para descargar un paquete de recuperación.

- Tú tienes el ["Permiso de mantenimiento o acceso root"](#).
- Tienes la contraseña de aprovisionamiento.
- Comprende los requisitos y las mejores prácticas para los nombres para mostrar. Ver ["Cambiar el nombre de la cuadrícula, los sitios y los nodos"](#).

Cómo cambiar el nombre de una cuadrícula, sitios o nodos

Puede cambiar el nombre de su sistema StorageGRID, uno o más sitios, o uno o más nodos.

Puede utilizar un nombre para mostrar que haya sido usado previamente por un nodo diferente, siempre y cuando el cambio de nombre no genere un nombre para mostrar o un nombre de sistema duplicados.

Seleccionar elementos para cambiar el nombre

Para comenzar, seleccione los elementos que desea cambiar de nombre.

Pasos

1. Seleccione **MANTENIMIENTO > Tareas > Cambiar el nombre de la cuadrícula, los sitios y los nodos**.

2. Para el paso **Seleccionar nombres**, seleccione los elementos que desea cambiar de nombre.

Elemento a cambiar	Instrucción
Nombres de todo (o casi todo) en su sistema	a. Seleccionar Seleccionar todo . b. Opcionalmente, borre cualquier elemento que no desee cambiar de nombre.
Nombre de la cuadrícula	Seleccione la casilla de verificación de la cuadrícula.
Nombre de un sitio y algunos o todos sus nodos	a. Seleccione la casilla de verificación en el encabezado de la tabla para el sitio. b. Opcionalmente, borre todos los nodos que no desee cambiar de nombre.
Nombre de un sitio	Seleccione la casilla de verificación del sitio.
Nombre de un nodo	Seleccione la casilla de verificación del nodo.

3. Seleccione **Continuar**.

4. Revise la tabla, que incluye los elementos que seleccionó.

- La columna **Nombre para mostrar** muestra el nombre actual de cada elemento. Si el elemento nunca ha sido renombrado, su nombre para mostrar será el mismo que su nombre de sistema.
- La columna **Nombre del sistema** muestra el nombre que ingresó para cada elemento durante la instalación. Los nombres del sistema se utilizan para operaciones internas de StorageGRID y no se pueden cambiar. Por ejemplo, el nombre del sistema para un nodo podría ser su nombre de host.
- La columna **Tipo** indica el tipo de elemento: Cuadrícula, Sitio o el tipo específico de nodo.

Proponer nuevos nombres

Para el paso **Proponer nuevos nombres**, puede ingresar un nombre para mostrar para cada elemento individualmente o puede cambiar el nombre de los elementos en masa.

Cambiar el nombre de los elementos individualmente

Siga estos pasos para ingresar un nombre para mostrar para cada elemento que desee cambiar de nombre.

Pasos

1. En el campo **Nombre para mostrar**, ingrese un nombre para mostrar propuesto para cada elemento de la lista.

Ver "[Cambiar el nombre de la cuadrícula, los sitios y los nodos](#)" para conocer los requisitos de nomenclatura.

2. Para eliminar cualquier elemento que no desee renombrar, seleccione  en la columna **Eliminar de la lista**.

Si no va a proponer un nuevo nombre para un elemento, deberá eliminarlo de la tabla.

3. Cuando haya propuesto nuevos nombres para todos los elementos de la tabla, seleccione **Cambiar nombre**.

Aparece un mensaje de éxito. Los nuevos nombres para mostrar ahora se utilizan en todo Grid Manager.

Cambiar el nombre de los elementos de forma masiva

Utilice la herramienta de cambio de nombre masivo si los nombres de los elementos comparten una cadena común que desea reemplazar con una cadena diferente.

Pasos

1. Para el paso **Proponer nuevos nombres**, seleccione **Usar herramienta de cambio de nombre masivo**.

La **Vista previa de cambio de nombre** incluye todos los elementos que se mostraron para el paso **Proponer nuevos nombres**. Puede utilizar la vista previa para ver cómo se verán los nombres para mostrar después de reemplazar una cadena compartida.

2. En el campo **Cadena existente**, ingrese la cadena compartida que desea reemplazar. Por ejemplo, si la cadena que desea reemplazar es `Data-Center-1` , ingrese **Centro-de-Datos-1**.

A medida que escribe, su texto se resalta dondequiera que se encuentre en los nombres de la izquierda.

3. Seleccionar  para eliminar cualquier elemento que no desee cambiar de nombre con esta herramienta.

Por ejemplo, supongamos que desea cambiar el nombre de todos los nodos que contienen la cadena `Data-Center-1` , pero no quiere cambiar el nombre del `Data-Center-1` sitio en sí. Seleccionar  para eliminar el sitio de la vista previa de cambio de nombre.

Bulk rename tool

Rename preview ?

Data-Center-1 X

Data-Center-1-ADM1 X

Data-Center-1-ARC1 X

Data-Center-1-G1 X

Data-Center-1-S1 X

Data-Center-1-S2 X

Data-Center-1-S3 X

Data-Center-1-S4 ✓

Cancel

Add names

Enter the shared string you want to replace. Then, enter a new string to use instead. Optionally, remove any items that you do not want to rename with this tool.

Existing string

Data-Center-1

The string you want to replace. Represented by *italicized text* in the preview section.

New string

The string you want to use instead. Represented by **bolded text** in the preview section.

4. En el campo **Nueva cadena**, ingrese la cadena de reemplazo que desea utilizar en su lugar. Por ejemplo, introduzca **DC1**.

Ver "**Cambiar el nombre de la cuadrícula, los sitios y los nodos**" para conocer los requisitos de nomenclatura.

A medida que ingresa la cadena de reemplazo, los nombres de la izquierda se actualizan, por lo que puede verificar que los nuevos nombres serán correctos.

Bulk rename tool

Rename preview

DC1-ADM1

DC1-ARC1

DC1-G1

DC1-S1

DC1-S2

DC1-S3

DC1-S4

Cancel

Add names

Enter the shared string you want to replace. Then, enter a new string to use instead. Optionally, remove any items that you do not want to rename with this tool.

Existing string

Data-Center-1

The string you want to replace. Represented by *italicized text* in the preview section.

New string

DC1

The string you want to use instead. Represented by **bolded text** in the preview section.

5. Cuando esté satisfecho con los nombres que se muestran en la vista previa, seleccione **Agregar nombres** para agregar los nombres a la tabla para el paso **Proponer nuevos nombres**.
6. Realice los cambios adicionales necesarios o seleccione **X** para eliminar cualquier elemento que no desee cambiar de nombre.
7. Cuando esté listo para cambiar el nombre de todos los elementos de la tabla, seleccione **Cambiar nombre**.

Se muestra un mensaje de éxito. Los nuevos nombres para mostrar ahora se utilizan en todo Grid Manager.

Descargar el paquete de recuperación

Cuando haya terminado de cambiar el nombre de los elementos, descargue y guarde un nuevo paquete de recuperación. Los nuevos nombres para mostrar de los elementos que renombró se incluyen en el `Passwords.txt` archivo.

Pasos

1. Introduzca la contraseña de aprovisionamiento.
2. Seleccione **Descargar paquete de recuperación**.

La descarga comienza inmediatamente.
3. Cuando se complete la descarga, abra el `Passwords.txt` archivo para ver el nombre del servidor para todos los nodos y los nombres para mostrar de cualquier nodo renombrado.
4. Copiar el `sgws-recovery-package-id-revision.zip` archivo en dos ubicaciones seguras,

protegidas y separadas.



El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

5. Seleccione **Finalizar** para volver al primer paso.

Revertir los nombres para mostrar a los nombres del sistema

Puede revertir una cuadrícula, un sitio o un nodo renombrado a su nombre de sistema original. Cuando revierte un elemento a su nombre de sistema, las páginas de Grid Manager y otras ubicaciones de StorageGRID ya no muestran un **Nombre para mostrar** para ese elemento. Sólo se muestra el nombre del sistema del elemento.

Pasos

1. Seleccione **MANTENIMIENTO > Tareas > Cambiar el nombre de la cuadrícula, los sitios y los nodos**.
2. Para el paso **Seleccionar nombres**, seleccione los elementos que desea revertir a los nombres del sistema.
3. Seleccione **Continuar**.
4. Para el paso **Proponer nuevos nombres**, revierta los nombres para mostrar a los nombres del sistema de manera individual o en masa.

Revertir a los nombres del sistema individualmente

- a. Copie el nombre del sistema original de cada elemento y péguelo en el campo **Nombre para mostrar**, o seleccione  para eliminar cualquier elemento que no desee revertir.

Para revertir un nombre para mostrar, el nombre del sistema debe aparecer en el campo **Nombre para mostrar**, pero el nombre no distingue entre mayúsculas y minúsculas.

- b. Seleccione **Cambiar nombre**.

Aparece un mensaje de éxito. Los nombres para mostrar de estos elementos ya no se utilizan.

Revertir a los nombres del sistema de forma masiva

- a. Para el paso **Proponer nuevos nombres**, seleccione **Usar herramienta de cambio de nombre masivo**.
- b. En el campo **Cadena existente**, ingrese la cadena de nombre para mostrar que desea reemplazar.
- c. En el campo **Nueva cadena**, ingrese la cadena de nombre del sistema que desea utilizar en su lugar.
- d. Seleccione **Agregar nombres** para agregar los nombres a la tabla para el paso **Proponer nuevos nombres**.
- e. Confirme que cada entrada en el campo **Nombre para mostrar** coincida con el nombre en el campo **Nombre del sistema**. Realice cualquier cambio o seleccione  para eliminar cualquier elemento que no desee revertir.

Para revertir un nombre para mostrar, el nombre del sistema debe aparecer en el campo **Nombre para mostrar**, pero el nombre no distingue entre mayúsculas y minúsculas.

- f. Seleccione **Cambiar nombre**.

Se muestra un mensaje de éxito. Los nombres para mostrar de estos elementos ya no se utilizan.

5. [Descargue y guarde un nuevo paquete de recuperación](#) .

Los nombres para mostrar de los elementos que revertiste ya no se incluyen en el `Passwords.txt` archivo.

Procedimientos de nodo

Procedimientos de mantenimiento de nodos

Es posible que necesite realizar procedimientos de mantenimiento relacionados con nodos de red o servicios de nodos específicos.

Procedimientos del Administrador de servidores

El Administrador de servidor se ejecuta en cada nodo de la red para supervisar el inicio y la detención de los servicios y para garantizar que se unan y salgan correctamente del sistema StorageGRID . El Administrador de servidor también supervisa los servicios en cada nodo de la red e intentará automáticamente reiniciar cualquier servicio que informe fallas.

Para realizar procedimientos del Administrador de servidor, normalmente es necesario acceder a la línea de comandos del nodo.



Debe acceder al Administrador de servidor solo si el soporte técnico se lo indica.



Debe cerrar la sesión de shell de comando actual y cerrar sesión después de terminar con el Administrador de servidor. Ingresar: `exit`

Procedimientos de reinicio, apagado y encendido del nodo

Utilice estos procedimientos para reiniciar uno o más nodos, para apagar y reiniciar nodos, o para apagar y encender nodos nuevamente.

Procedimientos de reasignación de puertos

Puede utilizar los procedimientos de reasignación de puertos para eliminar las reasignaciones de puertos de un nodo, por ejemplo, si desea configurar un punto final del balanceador de carga utilizando un puerto que se reasignó previamente.

Procedimientos del Administrador de servidores

Ver el estado y la versión del Administrador del servidor

Para cada nodo de la red, puede ver el estado actual y la versión del Administrador de servidor que se ejecuta en ese nodo de la red. También puede obtener el estado actual de todos los servicios que se ejecutan en ese nodo de la red.

Antes de empezar

Tú tienes el `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de la red:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Ver el estado actual del Administrador de servidor ejecutándose en el nodo de la red: **`service servermanager status`**

Se informa el estado actual del Administrador de servidor que se ejecuta en el nodo de la red (en ejecución o no). Si el estado del Administrador del servidor es `running`, se muestra el tiempo que ha estado ejecutándose desde la última vez que se inició. Por ejemplo:

```
servermanager running for 1d, 13h, 0m, 30s
```

3. Ver la versión actual del Administrador de servidor ejecutándose en un nodo de la red: **`service`**

servermanager version

La versión actual está listada. Por ejemplo:

```
11.1.0-20180425.1905.39c9493
```

4. Cerrar sesión en el 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 la red en cualquier momento.

Antes de empezar

Tú tienes el `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de la red:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Ver el estado de todos los servicios que se ejecutan en el nodo de la red: `storagegrid-status`

Por ejemplo, la salida del nodo de administración principal muestra el estado actual de los servicios AMS, CMN y NMS como En ejecución. Esta salida 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
attrDownSampl	11.1.0	Running
attrDownSamp2	11.1.0	Running
node exporter	0.13.0+ds	Running

3. Regrese a la línea de comando, presione **Ctrl+C**.

4. Opcionalmente, vea un informe estático de todos los servicios que se ejecutan en el nodo de la red:
`/usr/local/servermanager/reader.rb`

Este informe incluye la misma información que el informe actualizado continuamente, pero no se actualiza si cambia el estado de un servicio.

5. Cerrar sesión en el shell de comandos: `exit`

Iniciar el Administrador del servidor y todos los servicios

Es posible que necesite iniciar el Administrador de servidor, que también inicia todos los servicios en el nodo de la red.

Antes de empezar

Tú tienes el `Passwords.txt` archivo.

Acerca de esta tarea

Al iniciar el Administrador de servidor en un nodo de la red donde ya se está ejecutando, se reinicia el Administrador de servidor y todos los servicios en el nodo de la red.

Pasos

1. Inicie sesión en el nodo de la red:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`

d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Iniciar el Administrador del servidor: `service servermanager start`

3. Cerrar sesión en el shell de comandos: `exit`

Reinicie el Administrador del servidor y todos los servicios

Es posible que sea necesario reiniciar el administrador del servidor y todos los servicios que se ejecutan en un nodo de la red.

Antes de empezar

Tú tienes el `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de la red:

a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`

b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

c. Introduzca el siguiente comando para cambiar a root: `su -`

d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Reinicie el Administrador de servidor y todos los servicios en el nodo de la red: `service servermanager restart`

El Administrador de servidor y todos los servicios en el nodo de la red se detienen y luego se reinician.



Usando el `restart` El comando es lo mismo que usar el `stop` orden seguida de la `start` dominio.

3. Cerrar sesión en el shell de comandos: `exit`

Detener el Administrador de servidor y todos los servicios

El Administrador de servidor está diseñado para ejecutarse en todo momento, pero es posible que deba detenerlo y todos los servicios que se ejecutan en un nodo de la red.

Antes de empezar

Tú tienes el `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de la red:

a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`

b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Detener el administrador del servidor y todos los servicios que se ejecutan en el nodo de la red: `service servermanager stop`

El Administrador de servidor y todos los servicios que se ejecutan en el nodo de la red se finalizan correctamente. Los servicios pueden tardar hasta 15 minutos en apagarse.

3. Cerrar sesión en el shell de comandos: `exit`

Ver el estado actual del servicio

Puede ver el estado actual de un servicio que se ejecuta en un nodo de la red en cualquier momento.

Antes de empezar

Tú tienes el `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de la red:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Ver el estado actual de un servicio que se ejecuta en un nodo de la red: `'service servicename status` Se informa el estado actual del servicio solicitado que se ejecuta en el nodo de la red (en ejecución o no). Por ejemplo:

```
cmn running for 1d, 14h, 21m, 2s
```

3. Cerrar sesión en el shell de comandos: `exit`

Detener el servicio

Algunos procedimientos de mantenimiento requieren que usted detenga un solo servicio mientras mantiene otros servicios en funcionamiento en el nodo de la red. Detenga servicios individuales únicamente cuando así lo indique un procedimiento de mantenimiento.

Antes de empezar

Tú tienes el `Passwords.txt` archivo.

Acerca de esta tarea

Cuando utiliza estos pasos para "detener administrativamente" un servicio, el Administrador de servidor no reiniciará automáticamente el servicio. Debe iniciar el servicio único manualmente o reiniciar el Administrador del servidor.

Si necesita detener el servicio LDR en un nodo de almacenamiento, tenga en cuenta que puede llevar un tiempo detener el servicio si hay conexiones activas.

Pasos

1. Inicie sesión en el nodo de la red:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Detener un servicio individual: `service servicename stop`

Por ejemplo:

```
service ldr stop
```



Los servicios pueden tardar hasta 11 minutos en detenerse.

3. Cerrar sesión en el shell de comandos: `exit`

Información relacionada

["Forzar la terminación del servicio"](#)

Forzar la terminación del servicio

Si necesita detener un servicio inmediatamente, puede utilizar el `force-stop` dominio.

Antes de empezar

Tú tienes el `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de la red:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Forzar manualmente la finalización del servicio: `service servicename force-stop`

Por ejemplo:

```
service ldr force-stop
```

El sistema espera 30 segundos antes de finalizar el servicio.

3. Cerrar sesión en el shell de comandos: `exit`

Iniciar o reiniciar el servicio

Es posible que necesite iniciar un servicio que se haya detenido o que necesite detener y reiniciar un servicio.

Antes de empezar

Tú tienes el `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de la red:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Decide qué comando emitir, en función de si el servicio está ejecutándose o detenido.
 - Si el servicio está actualmente detenido, utilice el `start` Comando para iniciar el servicio manualmente: `service servicename start`

Por ejemplo:

```
service ldr start
```

- Si el servicio se está ejecutando actualmente, utilice el `restart` Comando para detener el servicio y luego reiniciarlo: `service servicename restart`

Por ejemplo:

```
service ldr restart
```

+



Usando el `restart` El comando es lo mismo que usar el `stop` orden seguida de la `start` dominio. Puedes emitir `restart` incluso si el servicio está actualmente detenido.

3. Cerrar sesión en el shell de comandos: `exit`

Utilice un archivo DoNotStart

Si está realizando varios procedimientos de mantenimiento o configuración bajo la dirección de soporte técnico, es posible que se le solicite utilizar un archivo DoNotStart para evitar que los servicios se inicien cuando se inicia o reinicia el Administrador de servidor.



Debe agregar o eliminar un archivo DoNotStart solo si el soporte técnico se lo ha indicado.

Para evitar que un servicio se inicie, coloque un archivo DoNotStart en el directorio del servicio cuyo inicio desea evitar. Al iniciarse, el Administrador del servidor busca el archivo DoNotStart. Si el archivo está presente, no se podrá iniciar el servicio (ni ningún servicio que dependa de él). Cuando se elimina el archivo DoNotStart, el servicio detenido anteriormente se iniciará en el próximo inicio o reinicio del Administrador de servidor. Los servicios no se inician automáticamente cuando se elimina el archivo DoNotStart.

La forma más eficiente de evitar que todos los servicios se reinicien es evitar que se inicie el servicio NTP. Todos los servicios dependen del servicio NTP y no pueden ejecutarse si el servicio NTP no se está ejecutando.

Agregar archivo DoNotStart para el servicio

Puede evitar que se inicie un servicio individual agregando un archivo DoNotStart al directorio de ese servicio en un nodo de la cuadrícula.

Antes de empezar

Tú tienes el `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de la red:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Agregar un archivo DoNotStart: `touch /etc/sv/service/DoNotStart`

dónde `service` es el nombre del servicio cuyo inicio se impedirá. Por ejemplo,

```
touch /etc/sv/ldr/DoNotStart
```


Se crea un archivo `DoNotStart`. No se necesita ningún contenido de archivo.

Cuando se reinicia el Administrador de servidor o el nodo de la red, el Administrador de servidor se reinicia, pero el servicio no.

3. Cerrar sesión en el shell de comandos: `exit`

Eliminar el archivo `DoNotStart` para el servicio

Cuando elimina un archivo `DoNotStart` que impide que se inicie un servicio, debe iniciar ese servicio.

Antes de empezar

Tú tienes el `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de la red:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Eliminar el archivo `DoNotStart` del directorio de servicio: `rm /etc/sv/service/DoNotStart`

dónde `service` es el nombre del servicio. Por ejemplo,

```
rm /etc/sv/ldr/DoNotStart
```

3. Iniciar el servicio: `service servicename start`
4. Cerrar sesión en el shell de comandos: `exit`

Solucionar problemas del Administrador del servidor

Si surge un problema al utilizar el Administrador de servidor, verifique su archivo de registro.

Los mensajes de error relacionados con el Administrador del servidor se capturan en el archivo de registro del Administrador del servidor, que se encuentra en: `/var/local/log/servermanager.log`

Consulte este archivo para ver si hay mensajes de error relacionados con fallas. Escala el problema al soporte técnico si es necesario. Es posible que se le solicite que envíe archivos de registro al soporte técnico.

Servicio con un estado de error

Si detecta que un servicio ha entrado en un estado de error, intente reiniciar el servicio.

Antes de empezar

Tú tienes el `Passwords.txt` archivo.

Acerca de esta tarea

El Administrador del servidor supervisa los servicios y reinicia cualquiera que se haya detenido inesperadamente. Si un servicio falla, el Administrador de servidor intenta reiniciarlo. Si hay tres intentos fallidos de iniciar un servicio en un plazo de cinco minutos, el servicio entra en un estado de error. El Administrador del servidor no intenta otro reinicio.

Pasos

1. Inicie sesión en el nodo de la red:

- Introduzca el siguiente comando: `ssh admin@grid_node_IP`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- Introduzca el siguiente comando para cambiar a root: `su -`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Confirme el estado de error del servicio: `service servicename status`

Por ejemplo:

```
service ldr status
```

Si el servicio está en un 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 ["eliminar 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, comuníquese con el soporte técnico.

4. Cerrar sesión en el shell de comandos: `exit`

Procedimientos de reinicio, apagado y encendido

Realizar un reinicio continuo

Puede realizar un reinicio continuo para reiniciar varios nodos de la red sin causar una interrupción del servicio.

Antes de empezar

- Ha iniciado sesión en Grid Manager en el nodo de administración principal y está utilizando un [navegador](#)

web compatible" .



Debe iniciar sesión en el nodo de administración principal para realizar este procedimiento.

- Tú tienes el ["Permiso de mantenimiento o acceso root"](#) .

Acerca de esta tarea

Utilice este procedimiento si necesita reiniciar varios nodos al mismo tiempo. Por ejemplo, puede utilizar este procedimiento después de cambiar el modo FIPS de la cuadrícula. ["Política de seguridad TLS y SSH"](#) . Cuando cambia el modo FIPS, debe reiniciar todos los nodos para que el cambio surta efecto.



Si solo necesita reiniciar un nodo, puede ["reinicie el nodo desde la pestaña Tareas"](#) .

Cuando StorageGRID reinicia los nodos de la red, emite el `reboot` comando en cada nodo, lo que hace que el nodo se apague y se reinicie. Todos los servicios se reinician automáticamente.

- Reiniciar un nodo VMware reinicia la máquina virtual.
- Reiniciar un nodo Linux reinicia el contenedor.
- Al reiniciar un nodo del dispositivo StorageGRID se reinicia el controlador de cómputo.

El procedimiento de reinicio continuo puede reiniciar varios nodos al mismo tiempo, con estas excepciones:

- Dos nodos del mismo tipo no se reiniciarán al mismo tiempo.
- Los nodos de puerta de enlace y los nodos de administración no se reiniciarán al mismo tiempo.

En cambio, estos nodos se reinician secuencialmente para garantizar que los grupos de alta disponibilidad, los datos de objetos y los servicios de nodos críticos siempre permanezcan disponibles.

Cuando reinicia el nodo de administración principal, su navegador pierde temporalmente el acceso al Administrador de cuadrícula, por lo que ya no puede supervisar el procedimiento. Por este motivo, el nodo de administración principal se reinicia en último lugar.

Realizar un reinicio continuo

Selecciona los nodos que desea reiniciar, revisa sus selecciones, inicia el procedimiento de reinicio y supervisa el progreso.

Seleccionar nodos

Como primer paso, acceda a la página de reinicio continuo y seleccione los nodos que desea reiniciar.

Pasos

1. Seleccione **MANTENIMIENTO > Tareas > Reinicio progresivo**.
2. Revise el estado de la conexión y los íconos de alerta en la columna **Nombre del nodo**.



No se puede reiniciar un nodo si está desconectado de la red. Las casillas de verificación están deshabilitadas para los nodos con estos íconos:  o  .

3. Si algún nodo tiene alertas activas, revise la lista de alertas en la columna **Resumen de alertas**.



Para ver todas las alertas actuales de un nodo, también puede seleccionar el **Nodos** > **Pestaña Descripción general**.

4. Opcionalmente, realice las acciones recomendadas para resolver cualquier alerta actual.
5. Opcionalmente, si todos los nodos están conectados y desea reiniciarlos todos, seleccione la casilla de verificación en el encabezado de la tabla y seleccione **Seleccionar todo**. De lo contrario, seleccione cada nodo que desee reiniciar.

Puede utilizar las opciones de filtro de la tabla para ver subconjuntos de nodos. Por ejemplo, puede ver y seleccionar solo nodos de almacenamiento o todos los nodos en un sitio determinado.

6. Seleccione **Revisar selección**.

Selección de reseñas

En este paso, puede determinar cuánto tiempo puede tardar el procedimiento de reinicio total y confirmar que seleccionó los nodos correctos.

1. En la página de selección de revisión, revise el Resumen, que indica cuántos nodos se reiniciarán y el tiempo total estimado para que todos los nodos se reinicien.
2. Opcionalmente, para eliminar un nodo específico de la lista de reinicio, seleccione **Eliminar**.
3. Opcionalmente, para agregar más nodos, seleccione **Paso anterior**, seleccione los nodos adicionales y seleccione **Revisar selección**.
4. Cuando esté listo para iniciar el procedimiento de reinicio continuo para todos los nodos seleccionados, seleccione **Reiniciar nodos**.
5. Si seleccionó reiniciar el nodo de administración principal, lea el mensaje de información y seleccione **Sí**.



El nodo de administración principal será el último nodo en reiniciarse. Mientras este nodo se reinicia, se perderá la conexión de su navegador. Cuando el nodo de administración principal vuelva a estar disponible, deberá volver a cargar la página de reinicio continuo.

Monitorear un reinicio continuo

Mientras se ejecuta el procedimiento de reinicio continuo, puedes supervisararlo desde el nodo de administración principal.

Pasos

1. Revise el progreso general de la operación, que incluye la siguiente información:
 - Número de nodos reiniciados
 - Número de nodos en proceso de reinicio
 - Número de nodos que quedan por reiniciar
2. Revise la tabla para cada tipo de nodo.

Las tablas proporcionan una barra de progreso de la operación en cada nodo y muestran la etapa de reinicio de ese nodo, que puede ser una de estas:

- Esperando para reiniciar
- Servicios de parada

- Reiniciando el sistema
- Servicios de inicio
- Reinicio completado

Detener el procedimiento de reinicio continuo

Puede detener el procedimiento de reinicio continuo desde el nodo de administración principal. Al detener el procedimiento, cualquier nodo que tenga el estado "Deteniendo servicios", "Reiniciando sistema" o "Iniciando servicios" completará la operación de reinicio. Sin embargo, estos nodos ya no serán rastreados como parte del procedimiento.

Pasos

1. Seleccione **MANTENIMIENTO > Tareas > Reinicio progresivo**.
2. Desde el paso **Reinicio del monitor**, seleccione **Detener procedimiento de reinicio**.

Reiniciar el nodo de la red desde la pestaña Tareas

Puede reiniciar un nodo de red individual desde la pestaña Tareas en la página Nodos.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de mantenimiento o acceso root"](#).
- Tienes la contraseña de aprovisionamiento.
- Si está reiniciando el nodo de administración principal o cualquier nodo de almacenamiento, debe revisar las siguientes consideraciones:
 - Cuando reinicia el nodo de administración principal, su navegador pierde temporalmente el acceso al Administrador de cuadrícula.
 - Si reinicia dos o más nodos de almacenamiento en un sitio determinado, es posible que no pueda acceder a ciertos objetos mientras dure el reinicio. Este problema puede ocurrir si alguna regla ILM utiliza la opción de ingesta **Dual commit** (o una regla específica **Balanced** y no es posible crear inmediatamente todas las copias requeridas). En este caso, StorageGRID confirmará los objetos recién ingeridos en dos nodos de almacenamiento en el mismo sitio y evaluará ILM más tarde.
 - Para garantizar que pueda acceder a todos los objetos mientras un nodo de almacenamiento se está reiniciando, deje de ingerir objetos en un sitio durante aproximadamente una hora antes de reiniciar el nodo.

Acerca de esta tarea

Cuando StorageGRID reinicia un nodo de la red, emite el `reboot` comando en el nodo, que hace que el nodo se apague y reinicie. Todos los servicios se reinician automáticamente.

- Reiniciar un nodo VMware reinicia la máquina virtual.
- Reiniciar un nodo Linux reinicia el contenedor.
- Al reiniciar un nodo del dispositivo StorageGRID se reinicia el controlador de cómputo.



Si necesita reiniciar más de un nodo, puede utilizar el ["procedimiento de reinicio continuo"](#).

Pasos

1. Seleccione **NODOS**.
2. Seleccione el nodo de la red que desea reiniciar.
3. Seleccione la pestaña **Tareas**.
4. Seleccione **Reiniciar**.

Aparece un cuadro de diálogo de confirmación. Si está reiniciando el nodo de administración principal, el cuadro de diálogo de confirmación le recordará que la conexión de su navegador al Administrador de Grid se perderá temporalmente cuando se detengan los servicios.

5. Introduzca la contraseña de aprovisionamiento y seleccione **Aceptar**.
6. Espere a que el nodo se reinicie.

Podría tomar algún tiempo para que los servicios se cierren.

Cuando el nodo se reinicia, aparece el ícono gris (Administrativamente inactivo) para el nodo en la página Nodos. Cuando todos los servicios se hayan iniciado nuevamente y el nodo esté conectado exitosamente a la red, la página Nodos debe mostrar un estado normal (sin íconos a la izquierda del nombre del nodo), lo que indica que no hay alertas activas y que el nodo está conectado a la red.

Reiniciar el nodo de la red desde el shell de comandos

Si necesita supervisar la operación de reinicio más de cerca o si no puede acceder al Administrador de red, puede iniciar sesión en el nodo de red y ejecutar el comando de reinicio del Administrador de servidor desde el shell de comandos.

Antes de empezar

Tú tienes el `Passwords.txt` archivo.

Pasos

1. Inicie sesión en el nodo de la red:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Opcionalmente, detener 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. Reiniciar el nodo de la red: `reboot`
4. Cerrar sesión en el shell de comandos: `exit`

Apagar el nodo de la red

Puede apagar un nodo de la red desde el shell de comandos del nodo.

Antes de empezar

- Tú tienes el `Passwords.txt` archivo.

Acerca de esta tarea

Antes de realizar este procedimiento, revise estas consideraciones:

- En general, no debe apagar más de un nodo a la vez para evitar interrupciones.
- No apague un nodo durante un procedimiento de mantenimiento a menos que la documentación o el soporte técnico lo indiquen explícitamente.
- El proceso de apagado depende de dónde esté instalado el nodo, de la siguiente manera:
 - Al apagar un nodo VMware se apaga la máquina virtual.
 - Al apagar un nodo Linux se apaga el contenedor.
 - Al apagar un nodo del dispositivo StorageGRID se apaga el controlador de cómputo.
- Si planea apagar más de un nodo de almacenamiento en un sitio, deje de ingerir objetos en ese sitio durante aproximadamente una hora antes de apagar los nodos.

Si alguna regla de ILM usa la opción de ingesta de **Confirmación dual** (o si una regla usa la opción **Equilibrada** y no se pueden crear inmediatamente todas las copias requeridas), StorageGRID confirma inmediatamente cualquier objeto recién ingerido en dos nodos de almacenamiento en el mismo sitio y evalúa ILM más tarde. Si se apaga más de un nodo de almacenamiento en un sitio, es posible que no pueda acceder a los objetos recién ingeridos mientras dure el apagado. Las operaciones de escritura también pueden fallar si quedan muy pocos nodos de almacenamiento disponibles en el sitio. Ver ["Administrar objetos con ILM"](#).

Pasos

1. Inicie sesión en el nodo de la red:

- Introduzca el siguiente comando: `ssh admin@grid_node_IP`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- Introduzca el siguiente comando para cambiar a root: `su -`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Detener todos los servicios: `service servermanager stop`

Los servicios pueden tardar hasta 15 minutos en apagarse, y es posible que desees iniciar sesión en el sistema de forma remota para supervisar el proceso de apagado.

3. Si el nodo se ejecuta en una máquina virtual VMware o es un nodo de dispositivo, emita el comando de apagado: `shutdown -h now`

Realice este paso independientemente del resultado de la `service servermanager stop` dominio.



Después de emitir el `shutdown -h now` comando en un nodo del dispositivo, debe apagar y encender el dispositivo para reiniciar el nodo.

Para el dispositivo, este comando apaga el controlador, pero el dispositivo permanece encendido. Debes completar el siguiente paso.

4. Si está apagando un nodo del dispositivo, siga los pasos correspondientes a su dispositivo.

SG6160

- a. Apague el controlador de almacenamiento SG6100-CN.
- b. Espere a que el LED de encendido azul del controlador de almacenamiento SG6100-CN se apague.

SGF6112

- a. Apague el aparato.
- b. Espere a que el LED de encendido azul se apague.

SG6000

- a. Espere a que el LED verde de caché activa en la parte posterior de los controladores de almacenamiento se apague.

Este LED se enciende cuando es necesario escribir datos almacenados en caché en las unidades. Debe esperar a que este LED se apague antes de apagar el dispositivo.

- b. Apague el aparato y espere hasta que el LED de encendido azul se apague.

SG5800

- a. Espere a que el LED verde de caché activa en la parte posterior del controlador de almacenamiento se apague.

Este LED se enciende cuando es necesario escribir datos almacenados en caché en las unidades. Debe esperar a que este LED se apague antes de apagar el dispositivo.

- b. Desde la página de inicio de SANtricity System Manager, seleccione **Ver operaciones en progreso**.
- c. Confirme que todas las operaciones se hayan completado antes de continuar con el siguiente paso.
- d. Apague ambos interruptores de encendido en el estante del controlador y espere a que todos los LED en el estante del controlador se apaguen.

SG5700

- a. Espere a que el LED verde de caché activa en la parte posterior del controlador de almacenamiento se apague.

Este LED se enciende cuando es necesario escribir datos almacenados en caché en las unidades. Debe esperar a que este LED se apague antes de apagar el dispositivo.

- b. Apague el aparato y espere a que se detenga toda actividad del LED y de la pantalla de siete segmentos.

SG100 o SG1000

- a. Apague el aparato.
- b. Espere a que el LED de encendido azul se apague.

Apagar el host

Antes de apagar un host, debe detener los servicios en todos los nodos de la red en ese host.

Pasos

1. Inicie sesión en el nodo de la red:

- a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
- b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Detener 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 desees iniciar sesión en el sistema de forma remota para supervisar el proceso de apagado.

3. Repita los pasos 1 y 2 para cada nodo del host.

4. Si tienes un host Linux:

- a. Inicie sesión en el sistema operativo host.
- b. Detener el nodo: `storagegrid node stop`
- c. Apague el sistema operativo host.

5. Si el nodo se ejecuta en una máquina virtual VMware o es un nodo de dispositivo, emita el comando de apagado: `shutdown -h now`

Realice este paso independientemente del resultado de la `service servermanager stop` dominio.



Después de emitir el `shutdown -h now` comando en un nodo del dispositivo, debe apagar y encender el dispositivo para reiniciar el nodo.

Para el dispositivo, este comando apaga el controlador, pero el dispositivo permanece encendido. Debes completar el siguiente paso.

6. Si está apagando un nodo del dispositivo, siga los pasos correspondientes a su dispositivo.

SG6160

- a. Apague el controlador de almacenamiento SG6100-CN.
- b. Espere a que el LED de encendido azul del controlador de almacenamiento SG6100-CN se apague.

SGF6112

- a. Apague el aparato.
- b. Espere a que el LED de encendido azul se apague.

SG6000

- a. Espere a que el LED verde de caché activa en la parte posterior de los controladores de almacenamiento se apague.

Este LED se enciende cuando es necesario escribir datos almacenados en caché en las unidades. Debe esperar a que este LED se apague antes de apagar el dispositivo.

- b. Apague el aparato y espere hasta que el LED de encendido azul se apague.

SG5800

- a. Espere a que el LED verde de caché activa en la parte posterior del controlador de almacenamiento se apague.

Este LED se enciende cuando es necesario escribir datos almacenados en caché en las unidades. Debe esperar a que este LED se apague antes de apagar el dispositivo.

- b. Desde la página de inicio de SANtricity System Manager, seleccione **Ver operaciones en progreso**.
- c. Confirme que todas las operaciones se hayan completado antes de continuar con el siguiente paso.
- d. Apague ambos interruptores de encendido en el estante del controlador y espere a que todos los LED en el estante del controlador se apaguen.

SG5700

- a. Espere a que el LED verde de caché activa en la parte posterior del controlador de almacenamiento se apague.

Este LED se enciende cuando es necesario escribir datos almacenados en caché en las unidades. Debe esperar a que este LED se apague antes de apagar el dispositivo.

- b. Apague el aparato y espere a que se detenga toda actividad del LED y de la pantalla de siete segmentos.

SG110 o SG1100

- a. Apague el aparato.
- b. Espere a que el LED de encendido azul se apague.

SG100 o SG1000

- a. Apague el aparato.
- b. Espere a que el LED de encendido azul se apague.

7. Cerrar sesión en el shell de comandos: `exit`

Información relacionada

- ["Dispositivos de almacenamiento SGF6112 y SG6160"](#)
- ["Dispositivos de almacenamiento SG6000"](#)
- ["Dispositivos de almacenamiento SG5700"](#)
- ["Dispositivos de almacenamiento SG5800"](#)
- ["Aparatos de servicio SG110 y SG1100"](#)
- ["Aparatos de servicio SG100 y SG1000"](#)

Apagar y encender todos los nodos de la red

Es posible que necesite apagar todo el sistema StorageGRID , por ejemplo, si está trasladando un centro de datos. Estos pasos proporcionan una descripción general de alto nivel de la secuencia recomendada para realizar un apagado y un inicio controlados.

Cuando apaga todos los nodos de un sitio o red, no podrá acceder a los objetos ingeridos mientras los nodos de almacenamiento estén fuera de línea.

Detener servicios y apagar nodos de la red

Antes de poder apagar un sistema StorageGRID , debe detener todos los servicios que se ejecutan en cada nodo de la red y luego apagar todas las máquinas virtuales VMware, los motores de contenedor y los dispositivos StorageGRID .

Acerca de esta tarea

Detenga primero los servicios en los nodos de administración y los nodos de puerta de enlace y, luego, detenga los servicios en los nodos de almacenamiento.

Este enfoque le permite utilizar el nodo de administración principal para supervisar el estado de los demás nodos de la red durante el mayor tiempo posible.



Si un solo host incluye más de un nodo de red, no apague el host hasta que haya detenido todos los nodos de ese host. Si el host incluye el nodo de administración principal, apague ese host en último lugar.



Si es necesario, puede ["migrar nodos de un host Linux a otro"](#) para realizar el mantenimiento del host sin afectar la funcionalidad o disponibilidad de su red.

Pasos

1. Impedir que todas las aplicaciones cliente accedan a la red.
2. Inicie 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 el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de \$ a # .

3. Detener 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 desees 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 y en los nodos de administración no principales.

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 del dispositivo, debe apagar y encender el dispositivo para reiniciar el nodo.

5. Para el nodo de administración principal, repita los pasos para [iniciando sesión en el nodo](#) y [Detener todos los servicios en el nodo](#) .
6. Para los nodos que se ejecutan en hosts Linux:
 - a. Inicie sesión en el sistema operativo host.
 - b. Detener el nodo: `storagegrid node stop`
 - c. Apague el sistema operativo host.
7. Para los nodos que se ejecutan en máquinas virtuales VMware y para los nodos de almacenamiento del dispositivo, emita el comando de apagado: `shutdown -h now`

Realice este paso independientemente del resultado de la `service servermanager stop` dominio.

Para el dispositivo, este comando apaga el controlador de cómputo, pero el dispositivo permanece encendido. Debes completar el siguiente paso.

8. Si tiene nodos de dispositivo, siga los pasos correspondientes a su dispositivo.

SG110 o SG1100

- a. Apague el aparato.
- b. Espere a que el LED de encendido azul se apague.

SG100 o SG1000

- a. Apague el aparato.
- b. Espere a que el LED de encendido azul se apague.

SG6160

- a. Apague el controlador de almacenamiento SG6100-CN.
- b. Espere a que el LED de encendido azul del controlador de almacenamiento SG6100-CN se apague.

SGF6112

- a. Apague el aparato.
- b. Espere a que el LED de encendido azul se apague.

SG6000

- a. Espere a que el LED verde de caché activa en la parte posterior de los controladores de almacenamiento se apague.

Este LED se enciende cuando es necesario escribir datos almacenados en caché en las unidades. Debe esperar a que este LED se apague antes de apagar el dispositivo.

- b. Apague el aparato y espere hasta que el LED de encendido azul se apague.

SG5800

- a. Espere a que el LED verde de caché activa en la parte posterior del controlador de almacenamiento se apague.

Este LED se enciende cuando es necesario escribir datos almacenados en caché en las unidades. Debe esperar a que este LED se apague antes de apagar el dispositivo.

- b. Desde la página de inicio de SANtricity System Manager, seleccione **Ver operaciones en progreso**.
- c. Confirme que todas las operaciones se hayan completado antes de continuar con el siguiente paso.
- d. Apague ambos interruptores de encendido en el estante del controlador y espere a que todos los LED en el estante del controlador se apaguen.

SG5700

- a. Espere a que el LED verde de caché activa en la parte posterior del controlador de almacenamiento se apague.

Este LED se enciende cuando es necesario escribir datos almacenados en caché en las unidades. Debe esperar a que este LED se apague antes de apagar el dispositivo.

- b. Apague el aparato y espere a que se detenga toda actividad del LED y de la pantalla de siete segmentos.

9. Si es necesario, cierre la sesión del shell de comandos: `exit`

La red StorageGRID ahora se ha cerrado.

Nodos de red de puesta en marcha



Si toda la red ha estado apagada durante más de 15 días, debe comunicarse con el soporte técnico antes de iniciar cualquier nodo de la red. No intente los procedimientos de recuperación que reconstruyen los datos de Cassandra. Si lo hace podría sufrir pérdida de datos.

Si es posible, encienda los nodos de la red en este orden:

- Aplique energía a los nodos de administración primero.
- Aplique energía a los nodos de puerta de enlace por último.



Si un host incluye varios nodos de red, los nodos volverán a estar en línea automáticamente cuando encienda el host.

Pasos

1. Encienda los hosts del nodo de administración principal y cualquier nodo de administración no principal.



No podrá iniciar sesión en los nodos de administración hasta que se hayan reiniciado los nodos de almacenamiento.

2. Encienda los hosts de todos los nodos de almacenamiento.

Puede encender estos nodos en cualquier orden.

3. Encienda los hosts de todos los nodos de puerta de enlace.

4. Sign in en el Administrador de cuadrícula.

5. Seleccione **NODOS** y monitoree el estado de los nodos de la red. Verifique que no haya íconos de alerta junto a los nombres de los nodos.

Información relacionada

- ["Dispositivos de almacenamiento SGF6112 y SG6160"](#)
- ["Aparatos de servicio SG110 y SG1100"](#)
- ["Aparatos de servicio SG100 y SG1000"](#)
- ["Dispositivos de almacenamiento SG6000"](#)
- ["Dispositivos de almacenamiento SG5800"](#)
- ["Dispositivos de almacenamiento SG5700"](#)

Procedimientos de reasignación de puertos

Eliminar reasignaciones de puertos

Si desea configurar un punto final para el servicio Load Balancer y desea utilizar un puerto que ya se ha configurado como puerto asignado de una reasignación de puerto,

primero debe eliminar la reasignación de puerto existente o el punto final 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 eliminar todas las reasignaciones de puertos del nodo.

Acerca de esta tarea

Este procedimiento elimina todas las reasignaciones de puertos. Si necesita conservar algunas de las reasignaciones, comuníquese con el soporte técnico.

Para obtener información sobre cómo configurar los puntos finales del balanceador de carga, consulte ["Configuración de los puntos finales del balanceador de carga"](#).



Si la reasignación del puerto proporciona acceso al cliente, reconfigure el cliente para usar un puerto diferente como punto final del equilibrador de carga para evitar la pérdida de servicio. De lo contrario, eliminar la asignación de puertos provocará la pérdida de acceso del cliente y deberá programarse adecuadamente.



Este procedimiento no funciona para un sistema StorageGRID implementado como contenedor en hosts físicos. Vea las instrucciones para ["Eliminar reasignaciones de puertos en hosts físicos"](#).

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 de contenedor que ejecuta StorageGRID.

b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

c. Introduzca el siguiente comando para cambiar a root: `su -`

d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Ejecute el siguiente script: `remove-port-remap.sh`

3. Reiniciar el nodo: `reboot`

4. Cerrar sesión en el shell de comandos: `exit`

5. Repita estos pasos en cada nodo de administración y nodo de puerta de enlace que tengan puertos reasignados en conflicto.

Eliminar reasignaciones de puertos en hosts físicos

Si desea configurar un punto final para el servicio Load Balancer y desea utilizar un puerto que ya se ha configurado como puerto asignado de una reasignación de puerto, primero debe eliminar la reasignación de puerto existente o el punto final no será efectivo.

Acerca de esta tarea

Si está ejecutando StorageGRID en hosts físicos, siga este procedimiento en lugar del procedimiento general para eliminar reasignaciones de puertos. Debe editar el archivo de configuración del nodo para cada nodo de administración y nodo de puerta de enlace que tenga puertos reasignados en conflicto para eliminar todas las reasignaciones de puertos del nodo y reiniciar el nodo.



Este procedimiento elimina todas las reasignaciones de puertos. Si necesita conservar algunas de las reasignaciones, comuníquese con el soporte técnico.

Para obtener información sobre cómo configurar los puntos finales del equilibrador de carga, consulte las instrucciones para administrar StorageGRID.



Este procedimiento puede provocar una pérdida temporal del servicio a medida que se reinician los nodos.

Pasos

1. Inicie sesión en el host que admite el nodo. Inicie sesión como root 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. Usando un editor de texto como vim o pico, edite el archivo de configuración del nodo.

El archivo de configuración del nodo se puede encontrar en `/etc/storagegrid/nodes/node-name.conf`.

4. Localice la sección del archivo de configuración del nodo que contiene las reasignaciones de puertos.

Vea las dos últimas líneas del 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_REMAP y PORT_REMAP_INBOUND para eliminar las reasignaciones de puertos.

```

PORT_REMAP =
PORT_REMAP_INBOUND =

```

6. Ejecute el siguiente comando para validar los cambios en el archivo de configuración del nodo: `sudo storagegrid node validate node-name`

Aborde cualquier error o advertencia antes de continuar con el siguiente paso.

7. Ejecute el siguiente comando para reiniciar el nodo sin reasignaciones de puertos: `sudo storagegrid node start node-name`
8. Inicie sesión en el nodo como administrador usando la contraseña que aparece en el `Passwords.txt` archivo.
9. Verificar que los servicios se inicien correctamente.
 - a. Ver una lista de los estados de todos los servicios en el servidor: `sudo storagegrid-status`

El estado se actualiza automáticamente.

b. Espere hasta que todos los servicios tengan un estado de En ejecución o Verificado.

c. Salir de la pantalla de estado:Ctrl+C

10. Repita estos pasos en cada nodo de administración y nodo de puerta de enlace que tengan puertos reasignados en conflicto.

Procedimientos de red

Actualizar subredes para la red Grid

StorageGRID mantiene una lista de las subredes de red utilizadas para comunicarse entre los nodos de la red en la red Grid (eth0). Estas entradas incluyen las subredes utilizadas para la red Grid por cada sitio en su sistema StorageGRID , así como también cualquier subred utilizada para NTP, DNS, LDAP u otros servidores externos a los que se accede a través de la puerta de enlace de la red Grid. Cuando agrega nodos de cuadrícula o un nuevo sitio en una expansión, es posible que necesite actualizar o agregar subredes a la red de cuadrícula.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de mantenimiento o acceso root"](#) .
- Tienes la contraseña de aprovisionamiento.
- Tienes las direcciones de red, en notación CIDR, de las subredes que quieres configurar.

Acerca de esta tarea

Si está realizando una actividad de expansión que incluye agregar una nueva subred, debe agregar una nueva subred a la lista de subredes de la red Grid antes de comenzar el procedimiento de expansión. De lo contrario, tendrá que cancelar la expansión, agregar la nueva subred y comenzar la expansión nuevamente.

No utilice subredes que contengan las siguientes direcciones IPv4 para la red de cuadrícula, la red de administración o la red de cliente de ningún nodo:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4



Por ejemplo, no utilice los siguientes rangos de subred para la red de cuadrícula, la red de administración o la red de cliente de ningún nodo:

- 192.168.130.0/24 porque este rango de subred contiene las direcciones IP 192.168.130.101 y 192.168.130.102
- 192.168.131.0/24 porque este rango de subred contiene las direcciones IP 192.168.131.101 y 192.168.131.102
- 198.51.100.0/24 porque este rango de subred contiene las direcciones IP 198.51.100.2 y 198.51.100.4

Agregar una subred

Pasos

1. Seleccione **MANTENIMIENTO > Red > Red de cuadrícula**.
2. Seleccione **Agregar otra subred** para agregar una nueva subred en notación CIDR.

Por ejemplo, introduzca 10.96.104.0/22 .

3. Ingrese la contraseña de aprovisionamiento y seleccione **Guardar**.
4. Espere hasta que se apliquen los cambios y luego descargue un nuevo paquete de recuperación.
 - a. Seleccione **MANTENIMIENTO > Sistema > Paquete de recuperación**.
 - b. Introduzca la **contraseña de aprovisionamiento**.



El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID . También se utiliza para recuperar el nodo de administración principal.

Las subredes que ha especificado se configuran automáticamente para su sistema StorageGRID .

Editar una subred

Pasos

1. Seleccione **MANTENIMIENTO > Red > Red de cuadrícula**.
2. Seleccione la subred que desea editar y realice los cambios necesarios.
3. Ingrese la contraseña de aprovisionamiento y seleccione **Guardar**.
4. Seleccione **Sí** en el cuadro de diálogo de confirmación.

5. Espere hasta que se apliquen los cambios y luego descargue un nuevo paquete de recuperación.
 - a. Seleccione **MANTENIMIENTO > Sistema > Paquete de recuperación**.
 - b. Introduzca la **contraseña de aprovisionamiento**.

Eliminar una subred

Pasos

1. Seleccione **MANTENIMIENTO > Red > Red de cuadrícula**.
2. Seleccione el icono de eliminar  al lado de la subred.
3. Ingrese la contraseña de aprovisionamiento y seleccione **Guardar**.
4. Seleccione **Sí** en el cuadro de diálogo de confirmación.
5. Espere hasta que se apliquen los cambios y luego descargue un nuevo paquete de recuperación.
 - a. Seleccione **MANTENIMIENTO > Sistema > Paquete de recuperación**.
 - b. Introduzca la **contraseña de aprovisionamiento**.

Configurar direcciones IP

Pautas de dirección IP

Puede realizar la configuración de la red configurando direcciones IP para los nodos de la red utilizando la herramienta Cambiar IP.

Debe utilizar la herramienta Cambiar IP para realizar la mayoría de los cambios en la configuración de red que se estableció inicialmente durante la implementación de la red. Es posible que los cambios manuales que utilizan archivos y comandos de red estándar de Linux no se propaguen a todos los servicios de StorageGRID y que no persistan después de actualizaciones, reinicios o procedimientos de recuperación de nodos.



El procedimiento de cambio de IP puede ser un procedimiento disruptivo. Es posible que algunas partes de la red no estén disponibles hasta que se aplique la nueva configuración.



Si solo está realizando cambios en la lista de subredes de la red Grid, utilice el Administrador de Grid para agregar o cambiar la configuración de la red. De lo contrario, utilice la herramienta Cambiar IP si el Administrador de red no es accesible debido a un problema de configuración de red, o si está realizando un cambio de enrutamiento de red de red y otros cambios de red al mismo tiempo.



Si desea cambiar la dirección IP de la red de cuadrícula para todos los nodos de la cuadrícula, utilice el [procedimiento especial para cambios en toda la red](#).

Interfaces Ethernet

La dirección IP asignada a eth0 es siempre la dirección IP de la red de la red del nodo de la red. La dirección IP asignada a eth1 es siempre la dirección IP de la red de administración del nodo de la red. La dirección IP asignada a eth2 es siempre la dirección IP de la red del cliente del nodo de la red.

Tenga en cuenta que en algunas plataformas, como los dispositivos StorageGRID, eth0, eth1 y eth2 pueden ser interfaces agregadas compuestas de puentes subordinados o enlaces de interfaces físicas o VLAN. En estas plataformas, la pestaña **SSM > Recursos** puede mostrar las direcciones IP de red de cliente,

administrador y cuadrícula asignadas a otras interfaces además de eth0, eth1 o eth2.

DHCP

Sólo se puede configurar DHCP durante la fase de implementación. No se puede configurar DHCP durante la configuración. Debe utilizar los procedimientos de cambio de dirección IP si desea cambiar direcciones IP, máscaras de subred y puertos de enlace predeterminadas para un nodo de la red. El uso de la herramienta Cambiar IP hará que las direcciones DHCP se vuelvan estáticas.

Grupos de alta disponibilidad (HA)

- Si una interfaz de red de cliente está contenida en un grupo de alta disponibilidad, no puede cambiar la dirección IP de red de cliente para esa interfaz a una dirección que esté fuera de la subred configurada para el grupo de alta disponibilidad.
- No se puede cambiar la dirección IP de la red del cliente al valor de una dirección IP virtual existente asignada a un grupo de alta disponibilidad configurado en la interfaz de la red del cliente.
- Si una interfaz de red Grid está contenida en un grupo HA, no puede cambiar la dirección IP de red Grid para esa interfaz a una dirección que esté fuera de la subred configurada para el grupo HA.
- No se puede cambiar la dirección IP de la red Grid al valor de una dirección IP virtual existente asignada a un grupo HA configurado en la interfaz de la red Grid.

Cambiar la configuración de la red del nodo

Puede cambiar la configuración de red de uno o más nodos utilizando la herramienta Cambiar IP. Puede cambiar la configuración de la red Grid o agregar, cambiar o eliminar las redes de administrador o de cliente.

Antes de empezar

Tú tienes el `Passwords.txt` archivo.

Acerca de esta tarea

Linux: Si está agregando un nodo de cuadrícula a la red de administración o a la red de cliente por primera vez, y no configuró previamente `ADMIN_NETWORK_TARGET` o `CLIENT_NETWORK_TARGET` en el archivo de configuración del nodo, debe hacerlo ahora.

Consulte las instrucciones de instalación de StorageGRID para su sistema operativo Linux:

- ["Instalar StorageGRID en Red Hat Enterprise Linux"](#)
- ["Instalar StorageGRID en Ubuntu o Debian"](#)

Dispositivos: En los dispositivos StorageGRID, si la red de cliente o de administrador no se configuró en el instalador del dispositivo StorageGRID durante la instalación inicial, la red no se puede agregar usando solo la herramienta Cambiar IP. Primero, debes ["Coloque el aparato en modo de mantenimiento"](#), configure los enlaces, regrese el dispositivo al modo operativo normal y luego use la herramienta Cambiar IP para modificar la configuración de la red. Ver el ["procedimiento para configurar enlaces de red"](#).

Puede cambiar la dirección IP, la máscara de subred, la puerta de enlace o el valor de MTU de uno o más nodos en cualquier red.

También puede agregar o eliminar un nodo de una red de cliente o de una red de administración:

- Puede agregar un nodo a una red de cliente o a una red de administración agregando una dirección

IP/máscara de subred en esa red al nodo.

- Puede eliminar un nodo de una red de cliente o de una red de administración eliminando la dirección IP/máscara de subred del nodo en esa red.

Los nodos no se pueden eliminar de la red.



No se permiten intercambios de direcciones IP. Si debe intercambiar direcciones IP entre nodos de la red, debe utilizar una dirección IP intermedia temporal.



Si el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID y está cambiando la dirección IP de un nodo de administración, tenga en cuenta que cualquier relación de confianza de usuario que se haya configurado utilizando la dirección IP del nodo de administración (en lugar de su nombre de dominio completo, como se recomienda) dejará de ser válida. Ya no podrá iniciar sesión en el nodo. Inmediatamente después de cambiar la dirección IP, debe actualizar o reconfigurar la relación de confianza del usuario autenticado del nodo en los Servicios de federación de Active Directory (AD FS) con la nueva dirección IP. Vea las instrucciones para ["configuración de SSO"](#).



Cualquier cambio que realice en la red mediante la herramienta Cambiar IP se propaga al firmware del instalador de los dispositivos StorageGRID. De ese modo, si se reinstala el software StorageGRID en un dispositivo, o si un dispositivo se coloca 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 el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de \$ a #.

2. Inicie la herramienta Cambiar IP ingresando el siguiente comando: `change-ip`

3. Introduzca la contraseña de aprovisionamiento cuando se le solicite.

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. Opcionalmente, seleccione **1** para elegir qué nodos actualizar. A continuación seleccione una de las siguientes opciones:

- **1:** Nodo único - seleccionar por nombre
- **2:** Nodo único: seleccionar por sitio, luego por nombre
- **3:** Nodo único: seleccionar por IP actual
- **4:** Todos los nodos en un sitio
- **5:** Todos los nodos de la cuadrícula

Nota: Si desea actualizar todos los nodos, permita que "todos" permanezca seleccionado.

Después de realizar su selección, aparece el menú principal, con el campo **Nodos seleccionados** actualizado para reflejar su elección. Todas las acciones posteriores se realizan únicamente en los nodos mostrados.

5. En el menú principal, seleccione la opción **2** para editar la información de IP/máscara, puerta de enlace y MTU de los nodos seleccionados.

a. Seleccione la red donde desea realizar cambios:

- **1:** Red de cuadrícula
- **2:** Red de administración
- **3:** Red de clientes
- **4:** Todas las redes

Después de realizar su selección, el mensaje muestra el nombre del nodo, el nombre de la red (Grid, Admin o Cliente), el tipo de datos (IP/máscara, Puerta de enlace o MTU) y el valor actual.

Editar la dirección IP, la longitud del prefijo, la puerta de enlace o la MTU de una interfaz configurada por DHCP cambiará la interfaz a estática. Cuando selecciona cambiar una interfaz configurada por DHCP, se muestra una advertencia para informarle que la interfaz cambiará a estática.

Interfaces configuradas como *fixed* No se puede editar.

b. Para establecer un nuevo valor, ingréselo en el formato que se muestra para el valor actual.

c. Para dejar el valor actual sin cambios, presione **Enter**.

d. Si el tipo de datos es IP/mask , puede eliminar la red de administrador o cliente del nodo ingresando

d o 0.0.0.0/0.

e. Después de editar todos los nodos que desea cambiar, ingrese **q** para regresar al menú principal.

Sus cambios se conservan hasta que se borren o apliquen.

6. Revise sus cambios seleccionando una de las siguientes opciones:

- **5:** Muestra ediciones en la salida que están aisladas para mostrar solo el elemento modificado. Los cambios se resaltan en verde (adiciones) o rojo (eliminaciones), como se muestra en el ejemplo de salida:

```
=====
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 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
Press Enter to continue
```

- **6:** Muestra 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 el formato tachado. La visualización correcta depende de que su cliente terminal admita las secuencias de escape VT100 necesarias.

7. Seleccione la opción **7** para validar todos los cambios.

Esta validación garantiza que no se violen las reglas para las redes Grid, Admin y Client, como no usar 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, la validación pasó.

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

8. Una vez pasada la validación, elija una de las siguientes opciones:

- **8:** Guardar cambios no aplicados.

Esta opción le permite salir de la herramienta Cambiar IP y volver a iniciarla más tarde, sin perder ningún cambio no aplicado.

- **10:** Aplicar la nueva configuración de red.

9. Si seleccionó la opción **10**, elija una de las siguientes opciones:

- **Aplicar:** Aplicar los cambios inmediatamente y reiniciar automáticamente cada nodo si es necesario.

Si la nueva configuración de red no requiere ningún cambio en la red física, puede seleccionar **Aplicar** para aplicar los cambios inmediatamente. Los nodos se reiniciarán automáticamente, si es necesario. Se mostrarán los nodos que necesitan reiniciarse.

- **etapa:** Aplicar los cambios la próxima vez que los nodos se reinicien manualmente.

Si necesita realizar cambios en la configuración de red física o virtual para que la nueva configuración de red funcione, debe usar la opción **stage**, apagar los nodos afectados, realizar los cambios de red física necesarios y reiniciar los nodos afectados. Si selecciona **Aplicar** sin realizar primero estos cambios de red, los cambios generalmente fallarán.



Si utiliza la opción **stage**, debe reiniciar el nodo lo antes posible después de la puesta en escena para minimizar las interrupciones.

- **Cancelar:** No realice ningún cambio de red en este momento.

Si no sabía que los cambios propuestos requieren que se reinicien los nodos, puede posponer los cambios para minimizar el impacto en el usuario. Al seleccionar **cancelar** regresará al menú principal y conservará los cambios para que pueda aplicarlos más tarde.

Cuando selecciona **aplicar** o **puesta en escena**, 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 preparar cambios, se genera un nuevo paquete de recuperación como resultado del cambio de configuración de la red.

10. Si seleccionó **etapa**, siga estos pasos una vez completado el aprovisionamiento:

a. Realice los cambios de red físicos o virtuales que sean necesarios.

Cambios en la red física: Realice los cambios necesarios en la red física, apagando el nodo de forma segura si es necesario.

Linux: Si está agregando el nodo a una red de administración o red de cliente por primera vez, asegúrese de haber agregado la interfaz como se describe en "[Linux: Agregar interfaces a un nodo existente](#)".

a. Reinicie los nodos afectados.

11. Seleccione **0** para salir de la herramienta Cambiar IP una vez completados los cambios.

12. Descargue un nuevo paquete de recuperación desde el Administrador de Grid.

a. Seleccione **MANTENIMIENTO > Sistema > Paquete de recuperación**.

b. Introduzca la contraseña de aprovisionamiento.

Agregar o cambiar listas de subredes en la red de administración

Puede agregar, eliminar o cambiar las subredes en la Lista de subredes de la red de administración de uno o más nodos.

Antes de empezar

- Tú tienes el `Passwords.txt` archivo.

Puede agregar, eliminar o cambiar subredes a todos los nodos en la Lista de subredes de la red de administración.

No utilice subredes que contengan las siguientes direcciones IPv4 para la red de cuadrícula, la red de administración o la red de cliente de ningún nodo:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4



Por ejemplo, no utilice los siguientes rangos de subred para la red de cuadrícula, la red de administración o la red de cliente de ningún nodo:

- 192.168.130.0/24 porque este rango de subred contiene las direcciones IP 192.168.130.101 y 192.168.130.102
- 192.168.131.0/24 porque este rango de subred contiene las direcciones IP 192.168.131.101 y 192.168.131.102
- 198.51.100.0/24 porque este rango de subred contiene las direcciones IP 198.51.100.2 y 198.51.100.4

Pasos

1. Inicie sesión en el nodo de administración principal:

- Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- Introduzca el siguiente comando para cambiar a root: `su -`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Inicie la herramienta Cambiar IP ingresando el siguiente comando: `change-ip`

3. Introduzca la contraseña de aprovisionamiento cuando se le solicite.

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. Opcionalmente, limite las redes/nodos en los que se realizan operaciones. Elija una de las siguientes opciones:
- Seleccione los nodos que desea editar eligiendo **1**, si desea filtrar por nodos específicos en los que realizar la operación. Seleccione una de las siguientes opciones:
 - **1**: Nodo único (seleccionar por nombre)
 - **2**: Nodo único (seleccionar por sitio, luego por nombre)
 - **3**: Nodo único (seleccionar por IP actual)
 - **4**: Todos los nodos en un sitio
 - **5**: Todos los nodos de la cuadrícula
 - **0**: Regresar
 - Permitir que "todos" permanezcan seleccionados. Después de realizar la selección, aparece la pantalla del menú principal. El campo Nodos seleccionados refleja su nueva selección y ahora todas las operaciones seleccionadas solo 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:
- Agregue una subred ingresando este comando: `add CIDR`
 - Eliminar una subred ingresando este comando: `del CIDR`
 - Establezca la lista de subredes ingresando este comando: `set CIDR`



Para todos los comandos, puede ingresar varias direcciones utilizando 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 la "flecha hacia arriba" para recuperar valores escritos previamente en el mensaje de entrada actual y luego editarlos si es necesario.

El siguiente ejemplo de entrada 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, ingrese **q** para regresar a la pantalla del menú principal. Sus cambios se conservan hasta que se borren o apliquen.



Si seleccionó cualquiera de los modos de selección de nodos "todos" en el paso 2, presione **Enter** (sin **q**) para pasar al siguiente nodo de la lista.

8. Elija una de las siguientes opciones:

- Seleccione la opción **5** para mostrar las ediciones en una salida aislada para mostrar solo el elemento modificado. Los cambios se resaltan en verde (adiciones) o rojo (eliminaciones), como se muestra en el siguiente 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 muestra la configuración completa. Los cambios se resaltan en verde (adiciones) o rojo (eliminaciones). **Nota:** Algunos emuladores de terminal pueden mostrar adiciones y eliminaciones usando el formato tachado.

Cuando intenta cambiar la lista de subredes, se muestra el siguiente mensaje:

CAUTION: The Admin Network subnet list on the node might contain /32 subnets derived from automatically applied routes that aren't persistent. Host routes (/32 subnets) are applied automatically if the IP addresses provided for external services such as NTP or DNS aren't reachable using default StorageGRID routing, but are reachable using a different interface and gateway. Making and applying changes to the subnet list will make all automatically applied subnets persistent. If you don't want that to happen, delete the unwanted subnets before applying changes. If you know that all /32 subnets in the list were added intentionally, you can ignore this caution.

Si no asignó específicamente las subredes del servidor NTP y DNS a una red, StorageGRID crea automáticamente una ruta de host (/32) para la conexión. 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 cualquier cambio a la lista de subredes.



Si bien puede utilizar estas rutas de host descubiertas 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 programados.

Esta validación garantiza que se cumplan 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 realizados y regresar más tarde para continuar realizando cambios.

Esta opción le permite salir de la herramienta Cambiar IP y volver a iniciarla 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 los cambios y 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 el siguiente ejemplo de salida:

```
Generating new grid networking description file...
```

```
Running provisioning...
```

```
Updating grid network configuration on Name
```

12. Descargue un nuevo paquete de recuperación desde el Administrador de Grid.

- Seleccione **MANTENIMIENTO > Sistema > Paquete de recuperación**.
- Introduzca la contraseña de aprovisionamiento.

Agregar o cambiar listas de subredes en Grid Network

Puede utilizar la herramienta Cambiar IP para agregar o cambiar subredes en la red Grid.

Antes de empezar

- Tú tienes el `Passwords.txt` archivo.

Puede agregar, eliminar o cambiar subredes en la Lista de subredes de la red Grid. Los cambios afectarán el enrutamiento en todos los nodos de la red.



Si solo está realizando cambios en la lista de subredes de la red Grid, utilice el Administrador de Grid para agregar o cambiar la configuración de la red. De lo contrario, utilice la herramienta Cambiar IP si el Administrador de red no es accesible debido a un problema de configuración de red, o si está realizando un cambio de enrutamiento de red de red y otros cambios de red al mismo tiempo.

No utilice subredes que contengan las siguientes direcciones IPv4 para la red de cuadrícula, la red de administración o la red de cliente de ningún nodo:

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4



Por ejemplo, no utilice los siguientes rangos de subred para la red de cuadrícula, la red de administración o la red de cliente de ningún nodo:

- 192.168.130.0/24 porque este rango de subred contiene las direcciones IP 192.168.130.101 y 192.168.130.102
- 192.168.131.0/24 porque este rango de subred contiene las direcciones IP 192.168.131.101 y 192.168.131.102
- 198.51.100.0/24 porque este rango de subred contiene las direcciones IP 198.51.100.2 y 198.51.100.4

Pasos

1. Inicie sesión en el nodo de administración principal:

- Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- Introduzca el siguiente comando para cambiar a root: `su -`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Inicie la herramienta Cambiar IP ingresando el siguiente comando: `change-ip`

3. Introduzca la contraseña de aprovisionamiento cuando se le solicite.

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 Grid (opción **4**).



Los cambios en la lista de subredes de la red Grid se aplican a toda la red.

5. Elija una de las siguientes opciones:

- Agregue una subred ingresando este comando: `add CIDR`
- Eliminar una subred ingresando este comando: `del CIDR`
- Establezca la lista de subredes ingresando este comando: `set CIDR`



Para todos los comandos, puede ingresar varias direcciones utilizando 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 la "flecha hacia arriba" para recuperar valores escritos previamente en el mensaje de entrada actual y luego editarlos si es necesario.

El siguiente ejemplo de entrada muestra la configuración de subredes para la lista de subredes de la red Grid:

```
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, ingrese **q** para regresar a la pantalla del menú principal. Sus cambios se conservan hasta que se borren o apliquen.

7. Elija una de las siguientes opciones:

- Seleccione la opción **5** para mostrar las ediciones en una salida aislada para mostrar solo el elemento modificado. Los cambios se resaltan en verde (adiciones) o rojo (eliminaciones), como se muestra en el siguiente 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 muestra 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 el formato tachado.

8. Seleccione la opción **7** para validar todos los cambios programados.

Esta validación garantiza que se cumplan 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 realizados y regresar más tarde para continuar realizando cambios.

Esta opción le permite salir de la herramienta Cambiar IP y volver a iniciarla 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 los cambios y 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 el siguiente ejemplo de salida:

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

11. Si seleccionó la opción **10** al realizar cambios en la red de cuadrícula, seleccione una de las siguientes opciones:

- **Aplicar:** Aplicar los cambios inmediatamente y reiniciar automáticamente cada nodo si es necesario.

Si la nueva configuración de red funcionará simultáneamente con la configuración de red anterior sin ningún cambio externo, puede utilizar la opción **aplicar** para un cambio de configuración totalmente automatizado.

- **etapa:** Aplicar los cambios la próxima vez que se reinicien los nodos.

Si necesita realizar cambios en la configuración de red física o virtual para que la nueva configuración de red funcione, debe usar la opción **stage**, apagar los nodos afectados, realizar los cambios de red física necesarios y reiniciar los nodos afectados.



Si utiliza la opción **stage**, reinicie el nodo lo antes posible después de la puesta en escena para minimizar las interrupciones.

- **Cancelar:** No realice ningún cambio de red en este momento.

Si no sabía que los cambios propuestos requieren que se reinicien los nodos, puede posponer los cambios para minimizar el impacto en el usuario. Al seleccionar **cancelar** regresará al menú principal y conservará los cambios para que pueda aplicarlos más tarde.

Después de aplicar o preparar cambios, se genera un nuevo paquete de recuperación como resultado del cambio de configuración de la red.

12. Si la configuración se detiene debido a errores, están disponibles las siguientes opciones:

- Para finalizar el procedimiento de cambio de IP y regresar al menú principal, ingrese **a**.
- Para volver a intentar la operación que falló, ingrese **r**.
- Para continuar con la siguiente operación, ingrese **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 estará completo hasta que todas las operaciones se hayan completado con éxito.

- Si tuvo que intervenir manualmente (para reiniciar un nodo, por ejemplo) y está seguro de que la acción que la herramienta cree que falló en realidad se completó con éxito, ingrese **f** para marcarla como exitosa y pasar a la siguiente operación.

13. Descargue un nuevo paquete de recuperación desde el Administrador de Grid.

- Seleccione **MANTENIMIENTO > Sistema > Paquete de recuperación**.
- Introduzca la contraseña de aprovisionamiento.



El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

Cambiar las direcciones IP de todos los nodos de la red

Si necesita cambiar la dirección IP de la red de todos los nodos de la red, debe seguir este procedimiento especial. No es posible realizar un cambio de IP de la red de cuadrícula completa utilizando el procedimiento para cambiar nodos individuales.

Antes de empezar

- Tú tienes el `Passwords.txt` archivo.

Para garantizar que la red se inicie correctamente, debe realizar todos los cambios al mismo tiempo.



Este procedimiento se aplica únicamente a la red Grid. No puede utilizar este procedimiento para cambiar direcciones IP en las redes de administrador o cliente.

Si desea cambiar las direcciones IP y la MTU de los nodos en un solo sitio, siga las ["Cambiar la configuración de la red del nodo"](#) instrucciones.

Pasos

1. Planifique con anticipación los cambios que necesita realizar fuera de la herramienta Cambiar IP, como cambios en DNS o NTP y cambios en la configuración de inicio de sesión único (SSO), si se utiliza.



Si los servidores NTP existentes no serán accesibles a la red en las nuevas direcciones IP, agregue los nuevos servidores NTP antes de realizar el procedimiento de cambio de IP.



Si los servidores DNS existentes no serán accesibles a la red en las nuevas direcciones IP, agregue los nuevos servidores DNS antes de realizar el procedimiento de cambio de IP.



Si SSO está habilitado para su sistema StorageGRID y se configuraron confianzas de usuario confiable mediante direcciones IP del nodo de administración (en lugar de nombres de dominio completos, como se recomienda), prepárese para actualizar o reconfigurar estas confianzas de usuario confiable en los Servicios de federación de Active Directory (AD FS) inmediatamente después de cambiar las direcciones IP. Ver ["Configurar el inicio de sesión único"](#).



Si es necesario, agregue 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 el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

3. Inicie la herramienta Cambiar IP ingresando el siguiente comando: `change-ip`
4. Introduzca la contraseña de aprovisionamiento cuando se le solicite.

Aparece el menú principal. De forma predeterminada, el `Selected nodes` El campo está configurado 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 Grid.

Después de realizar su selección, el mensaje muestra los nombres de los nodos, el nombre de la red de cuadrícula, el tipo de datos (IP/máscara, puerta de enlace o MTU) y los valores actuales.

Editar la dirección IP, la longitud del prefijo, la puerta de enlace o la MTU de una interfaz configurada por DHCP cambiará la interfaz a estática. Se muestra una advertencia antes de cada interfaz configurada por DHCP.

Interfaces configuradas como *fixed* No se puede editar.

- a. Para establecer un nuevo valor, ingréselo en el formato que se muestra para el valor actual.
 - b. Después de editar todos los nodos que desea cambiar, ingrese **q** para regresar al menú principal.

Sus cambios se conservan hasta que se borren o apliquen.

6. Revise sus cambios seleccionando una de las siguientes opciones:

- **5:** Muestra ediciones en la salida que están aisladas para mostrar solo el elemento modificado. Los cambios se resaltan en verde (adiciones) o rojo (eliminaciones), como se muestra en el ejemplo de salida:

```

=====
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 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 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 el formato tachado. La visualización correcta depende de que su cliente terminal admita las secuencias de escape VT100 necesarias.

7. Seleccione la opción **7** para validar todos los cambios.

Esta validación garantiza que no se violen las reglas de la red Grid, como no utilizar subredes superpuestas.

En este ejemplo, la validación devolvió errores.

```

Validating new networking configuration... FAILED.

DK-10-224-S-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
DK-10-224-S-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-S-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, la validación pasó.

```

Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue

```

8. Una vez pasada la validación, seleccione **10** para aplicar la nueva configuración de red.

9. Seleccione **etapa** para aplicar los cambios la próxima vez que se reinicien los nodos.



Debes seleccionar **etapa**. No realice un reinicio continuo, ya sea manualmente o seleccionando **aplicar** en lugar de **etapa**; la red no se iniciará correctamente.

10. Una vez completados los cambios, seleccione **0** para salir de la herramienta Cambiar IP.

11. Apague todos los nodos simultáneamente.



Es necesario apagar toda la red para que todos los nodos queden inactivos al mismo tiempo.

12. Realice los cambios de red físicos o virtuales que sean necesarios.

13. Verifique que todos los nodos de la red estén inactivos.

14. Encienda todos los nodos.

15. Después de que la red se inicie correctamente:

- a. Si agregó nuevos servidores NTP, elimine los valores del servidor NTP antiguo.
- b. Si agregó nuevos servidores DNS, elimine los valores del servidor DNS antiguo.

16. Descargue el nuevo paquete de recuperación desde Grid Manager.

- a. Seleccione **MANTENIMIENTO > Sistema > Paquete de recuperación**.
- b. Introduzca la contraseña de aprovisionamiento.

Información relacionada

- ["Agregar o cambiar listas de subredes en Grid Network"](#)
- ["Apagar el nodo de la red"](#)

Agregar interfaces a un nodo existente

Linux: Agregar interfaces de administrador o cliente a un nodo existente

Utilice estos pasos para agregar una interfaz en la red de administración o en la red de cliente a un nodo Linux después de haberlo 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 agregar la interfaz. Para obtener más información sobre el archivo de configuración del nodo, consulte las instrucciones para su sistema operativo Linux:

- ["Instalar StorageGRID en Red Hat Enterprise Linux"](#)
- ["Instalar StorageGRID en Ubuntu o Debian"](#)

Realice este procedimiento en el servidor Linux que aloja el nodo que necesita la nueva asignación de red, no dentro del nodo. Este procedimiento solo agrega la interfaz al nodo; se produce un error de validación si intenta especificar otros parámetros de red.

Para proporcionar información de dirección, debe utilizar la herramienta Cambiar IP. Ver ["Cambiar la configuración de la red del nodo"](#).

Pasos

1. Inicie sesión en el servidor Linux que aloja el nodo.
2. Editar 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 objetivo 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 de validación de nodo:

```
sudo storagegrid node validate node-name
```

4. Resolver todos los errores de validación.

5. Ejecute el comando de recarga de nodo:

```
sudo storagegrid node reload node-name
```

Linux: Agregar interfaces troncales o de acceso a un nodo

Puede agregar troncales adicionales o interfaces de acceso a un nodo Linux después de haberlo instalado. Las interfaces que agregue se muestran en la página de interfaces VLAN y en la página de grupos HA.

Antes de empezar

- Tiene acceso a las instrucciones para instalar StorageGRID en su plataforma Linux.
 - ["Instalar StorageGRID en Red Hat Enterprise Linux"](#)
 - ["Instalar StorageGRID en Ubuntu o Debian"](#)
- Tú tienes el `Passwords.txt` archivo.
- Tienes ["permisos de acceso específicos"](#).



No intente agregar interfaces a un nodo mientras esté activo un procedimiento de actualización de software, de recuperación o de expansión.

Acerca de esta tarea

Utilice estos pasos para agregar una o más interfaces adicionales a un nodo Linux después de que el nodo se haya instalado. Por ejemplo, es posible que desee agregar una interfaz troncal a un nodo de administración o de puerta de enlace, de modo que pueda usar interfaces VLAN para segregar el tráfico que pertenece a diferentes aplicaciones o inquilinos. O bien, es posible que desee agregar una interfaz de acceso para usar en un grupo de alta disponibilidad (HA).

Si agrega 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 HA; no necesita configurar una interfaz VLAN.

El nodo no está disponible por un breve tiempo cuando se agregan interfaces. Debes realizar este procedimiento en un nodo a la vez.

Pasos

1. Inicie sesión en el servidor Linux que aloja el nodo.
2. Usando un editor de texto como vim o pico, edite el archivo de configuración del nodo:

```
/etc/storagegrid/nodes/node-name.conf
```

3. Agregue una entrada al archivo para especificar el nombre y, opcionalmente, la descripción de cada interfaz adicional que desee agregar al nodo. Utilice este formato.

```
INTERFACE_TARGET_nnnn=value
```

Para *nnnn*, especifique un número único para cada INTERFACE_TARGET entrada que estás agregando.

Para *value*, especifique el nombre de la interfaz física en el host físico. Luego, opcionalmente, agregue una coma y proporcione una descripción de la interfaz, que se muestra en la página de interfaces de VLAN y en la página de grupos de HA.

Por ejemplo:

```
INTERFACE_TARGET_0001=ens256, Trunk
```



No especifique ningún otro parámetro de red o se producirá un error de validación.

4. Ejecute el siguiente comando para validar los cambios en el archivo de configuración del nodo:

```
sudo storagegrid node validate node-name
```

Aborde cualquier error o advertencia 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 agregó una o más interfaces troncales, vaya a ["configurar interfaces VLAN"](#) configurar una o más interfaces VLAN para cada nueva interfaz principal.
- Si agregó una o más interfaces de acceso, vaya a ["configurar grupos de alta disponibilidad"](#) para agregar las nuevas interfaces directamente a los grupos de HA.

VMware: Agregar interfaces troncales o de acceso a un nodo

Puede agregar un enlace troncal o una interfaz de acceso a un nodo de VM después de que se haya instalado el nodo. Las interfaces que agregue se muestran en la página de interfaces VLAN y en la página de grupos HA.

Antes de empezar

- Tienes acceso a las instrucciones para ["Instalación de StorageGRID en su plataforma VMware"](#) .

- Tiene máquinas virtuales VMware con nodo de administración y nodo de puerta de enlace.
- Tiene una subred de red que no se utiliza como red de cuadrícula, de administrador o de cliente.
- Tú tienes el `Passwords.txt` archivo.
- Tienes "[permisos de acceso específicos](#)".



No intente agregar interfaces a un nodo mientras esté activo un procedimiento de actualización de software, de recuperación o de expansión.

Acerca de esta tarea

Utilice estos pasos para agregar una o más interfaces adicionales a un nodo VMware después de que se haya instalado el nodo. Por ejemplo, es posible que desee agregar una interfaz troncal a un nodo de administración o de puerta de enlace, de modo que pueda usar interfaces VLAN para segregar el tráfico que pertenece a diferentes aplicaciones o inquilinos. O quizás desee agregar una interfaz de acceso para usar en un grupo de alta disponibilidad (HA).

Si agrega 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 HA; no necesita configurar una interfaz VLAN.

Es posible que el nodo no esté disponible por un breve período cuando agregue interfaces.

Pasos

1. En vCenter, agregue un nuevo adaptador de red (tipo VMXNET3) a una máquina virtual de nodo de administración y de nodo de puerta de enlace. Seleccione las casillas de verificación **Conectado** y **Conectar al encender**.

Network adapter 4 *		CLIENT683_old_vlan	Connected
Status	☒ Connect At Power On		
Adapter Type	VMXNET 3		
DirectPath I/O	☒ Enable		

2. Utilice SSH para iniciar sesión en el nodo de administración o en el nodo de puerta de enlace.
3. Usar `ip link show` para confirmar que se detecta 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 agregó una o más interfaces troncales, vaya a ["configurar interfaces VLAN"](#) configurar una o más interfaces VLAN para cada nueva interfaz principal.
- Si agregó una o más interfaces de acceso, vaya a ["configurar grupos de alta disponibilidad"](#) para agregar las nuevas interfaces directamente a los grupos de HA.

Configurar servidores DNS

Puede agregar, actualizar y eliminar servidores DNS, de modo que pueda utilizar nombres de host de nombre de dominio completo (FQDN) en lugar de direcciones IP.

Para utilizar nombres de dominio completos (FQDN) en lugar de direcciones IP al especificar nombres de host para destinos externos, especifique la dirección IP de cada servidor DNS que utilizará. Estas entradas se utilizan para AutoSupport, correos electrónicos de alerta, notificaciones SNMP, puntos finales de servicios de plataforma, grupos de almacenamiento en la nube y más.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de mantenimiento o acceso root"](#) .
- Tienes las direcciones IP de los servidores DNS para configurar.

Acerca de esta tarea

Para garantizar un funcionamiento correcto, especifique dos o tres servidores DNS. Si especifica más de tres, es posible que solo se utilicen tres debido a las limitaciones conocidas del sistema operativo en algunas plataformas. Si tiene restricciones de enrutamiento en su entorno, puede ["personalizar la lista de servidores DNS"](#) para que los nodos individuales (normalmente todos los nodos de un sitio) utilicen un conjunto diferente de hasta tres servidores DNS.

Si es posible, utilice servidores DNS a los que cada sitio pueda acceder localmente para garantizar que un sitio aislado pueda resolver los FQDN para destinos externos.

Agregar un servidor DNS

Siga estos pasos para agregar un servidor DNS.

Pasos

1. Seleccione **MANTENIMIENTO > Red > Servidores DNS**.
2. Seleccione **Agregar otro servidor** para agregar un servidor DNS.
3. Seleccione **Guardar**.

Modificar un servidor DNS

Siga estos pasos para modificar un servidor DNS.

Pasos

1. Seleccione **MANTENIMIENTO > Red > Servidores DNS**.
2. Seleccione la dirección IP del nombre del servidor que desea editar y realice los cambios necesarios.
3. Seleccione **Guardar**.

Eliminar un servidor DNS

Siga estos pasos para eliminar una dirección IP de un servidor DNS.

Pasos

1. Seleccione **MANTENIMIENTO > Red > Servidores DNS**.
2. Seleccione el icono de eliminar  junto a la dirección IP.
3. Seleccione **Guardar**.

Modificar la configuración de DNS para un solo nodo de red

En lugar de configurar el DNS globalmente para toda la implementación, puede ejecutar un script para configurar el DNS de manera diferente para cada nodo de la red.

En general, debe utilizar la opción **MANTENIMIENTO > Red > Servidores DNS** en el Administrador de Grid para configurar servidores DNS. Utilice el siguiente script solo si necesita utilizar diferentes servidores DNS para diferentes nodos de la red.

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 el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

- e. Agregue la clave privada SSH al agente SSH. Ingresar: `ssh-add`
- f. Ingrese la contraseña de acceso SSH que aparece en el `Passwords.txt` archivo.

2. Inicie sesión en el nodo que desea actualizar con una configuración de 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. Agregue la dirección IPv4 de un servidor que proporciona servicio de nombre de dominio para su red: `add <nameserver IP_address>`
5. Repita el `add nameserver` Comando para agregar servidores de nombres.
6. Siga las instrucciones que se le soliciten 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 la cuadrícula, repita los pasos desde [iniciando sesión en el nodo](#) a través de [cerrando el shell de comandos](#).
10. Cuando ya no necesite acceso sin contraseña a otros servidores, elimine la clave privada del agente SSH.
Ingresar: `ssh-add -D`

Administrar servidores NTP

Puede agregar, actualizar o eliminar servidores de Protocolo de tiempo de red (NTP) para garantizar que los datos se sincronicen con precisión entre los nodos de la red en su sistema StorageGRID.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un [navegador web compatible](#).
- Tú tienes el [Permiso de mantenimiento o acceso root](#).
- Tienes la contraseña de aprovisionamiento.
- Tienes las direcciones IPv4 de los servidores NTP para configurar.

Cómo StorageGRID utiliza NTP

El sistema StorageGRID utiliza el Protocolo de tiempo de red (NTP) para sincronizar el tiempo entre todos los nodos de la red.

En cada sitio, al menos dos nodos del sistema StorageGRID tienen asignada la función NTP principal. Se sincronizan con un mínimo sugerido de cuatro y un máximo de seis fuentes de tiempo externas y entre sí. Cada nodo del sistema StorageGRID que no sea un nodo NTP principal actúa como un cliente NTP y se sincroniza con estos nodos NTP principales.

Los servidores NTP externos se conectan a los nodos a los que previamente asignó roles NTP primarios. Por este motivo, se recomienda especificar al menos dos nodos con roles NTP primarios.

Directrices del servidor NTP

Siga estas pautas para protegerse contra problemas de sincronización:

- Los servidores NTP externos se conectan a los nodos a los que previamente asignó roles NTP primarios. Por este motivo, se recomienda especificar al menos dos nodos con roles NTP primarios.
- Asegúrese de que al menos dos nodos en cada sitio puedan acceder al menos a cuatro fuentes NTP externas. Si solo un nodo en un sitio puede acceder a las fuentes NTP, se producirán problemas de sincronización si ese nodo deja de funcionar. Además, designar dos nodos por sitio como fuentes NTP primarias garantiza una sincronización precisa si un sitio está aislado del resto de la red.
- Los servidores NTP externos especificados deben utilizar el protocolo NTP. Debe especificar referencias de servidor NTP de Stratum 3 o superior para evitar problemas con la diferencia horaria.



Al especificar la fuente NTP externa para una instalación de 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 hora en versiones anteriores de Windows no es lo suficientemente preciso y Microsoft no lo admite para su uso en entornos de alta precisión, incluido StorageGRID. Para más detalles, véase ["Límite de soporte para configurar el servicio de hora de Windows para entornos de alta precisión"](#).

Configurar servidores NTP

Siga estos pasos para agregar, actualizar o eliminar servidores NTP.

Pasos

1. Seleccione **MANTENIMIENTO > Red > Servidores NTP**.
2. En la sección Servidores, agregue, actualice o elimine entradas de servidor NTP, según sea necesario.

Debe incluir al menos cuatro servidores NTP y puede especificar hasta seis servidores.

3. Ingrese la contraseña de aprovisionamiento para su sistema StorageGRID, luego seleccione **Guardar**.

La página estará deshabilitada hasta que se completen las actualizaciones de configuración.



Si todos sus servidores NTP no pasan la prueba de conexión después de guardar los nuevos servidores NTP, no continúe. Póngase en contacto con el soporte técnico.

Resolver problemas del servidor NTP

Si encuentra problemas con la estabilidad o disponibilidad de los servidores NTP especificados originalmente durante la instalación, puede actualizar la lista de fuentes NTP externas que utiliza el sistema StorageGRID agregando servidores adicionales o actualizando o eliminando servidores existentes.

Restaurar la conectividad de red para nodos aislados

En determinadas circunstancias, es posible que uno o más grupos de nodos no puedan comunicarse con el resto de la red. Por ejemplo, los cambios de dirección IP a nivel de sitio o de red pueden generar nodos aislados.

Acerca de esta tarea

El aislamiento del nodo se indica mediante:

- Alertas, como **No se puede comunicar con el nodo (Alertas > Actual)**
- Diagnósticos relacionados con la conectividad (**SOPORTE > Herramientas > Diagnóstico**)

Algunas de las consecuencias de tener nodos aislados incluyen las siguientes:

- Si hay varios nodos aislados, es posible que no pueda iniciar sesión ni acceder al Administrador de red.
- Si se aíslan varios nodos, los valores de cuota y uso de almacenamiento que se muestran en el panel del Administrador de inquilinos podrían estar desactualizados. Los totales se actualizarán cuando se restablezca la conectividad de la red.

Para resolver el problema de aislamiento, ejecute 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 esté aislado de la red. La utilidad proporciona a los nodos la dirección IP de un nodo no aislado en la red, lo que permite que el nodo o grupo de nodos aislado vuelva a contactar a toda la red.



Si el sistema de nombres de dominio de multidifusión (mDNS) está deshabilitado en las redes, es posible que deba ejecutar la utilidad de línea de comandos en cada nodo aislado.

Pasos

Este procedimiento no aplica cuando solo algunos servicios están fuera de línea o reportan errores de comunicación.

1. Acceda al nodo y verifique `/var/local/log/dynip.log` para mensajes de aislamiento.

Por ejemplo:

```
[2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
no contact with other nodes.
If this warning persists, manual action might be required.
```

Si está utilizando la consola VMware, contendrá un mensaje que indica que el nodo podría estar aislado.

En las implementaciones de Linux, los mensajes de aislamiento aparecerían en `/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>
```

dónde `<address>` es la dirección IP de un nodo remoto que está conectado a la red.

```
# /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 haya sido aislado previamente:

- Los servicios del nodo se han iniciado.
- El estado del servicio de IP dinámica es "En ejecución" después de ejecutar el `storagegrid-status dominio`.
- En la página Nodos, el nodo ya no aparece desconectado del resto de la cuadrícula.



Si se ejecuta el `add_node_ip.py` El comando no resuelve el problema, podría haber otros problemas de red que deban resolverse.

Procedimientos de host y middleware

Linux: Migrar el nodo de la red a un nuevo host

Puede migrar uno o más nodos StorageGRID de un host Linux (el *host de origen*) a otro host Linux (el *host de destino*) para realizar el mantenimiento del host sin afectar la funcionalidad ni la disponibilidad de su red.

Por ejemplo, es posible que desee migrar un nodo para realizar parches al sistema operativo y reiniciarlo.

Antes de empezar

- Planificó su implementación de StorageGRID para incluir soporte de migración.
 - ["Requisitos de migración de contenedores de nodos para Red Hat Enterprise Linux"](#)
 - ["Requisitos de migración de contenedores de nodos para Ubuntu o Debian"](#)
- El host de destino ya está preparado para el uso de StorageGRID .
- El almacenamiento compartido se utiliza para todos los volúmenes de almacenamiento por nodo
- Las interfaces de red tienen nombres consistentes en todos los hosts.



En una implementación de producción, no ejecute más de un nodo de almacenamiento en un solo host. El uso de un host dedicado para cada nodo de almacenamiento proporciona un dominio de falla aislado.

Se pueden implementar otros tipos de nodos, como nodos de administración o nodos de puerta de enlace, en el mismo host. 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.

Nodo de exportación desde el host de origen

Como primer paso, apague el nodo de la red y expórtelo desde el host Linux de origen.

Ejecute los siguientes comandos en el *host de origen*.

Pasos

1. Obtenga el estado de todos los nodos que se ejecutan actualmente en el host de origen.

```
sudo storagegrid node status all
```

Ejemplo de salida:

```
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 deténgalo si su estado de ejecución es En ejecución.

```
sudo storagegrid node stop DC1-S3
```

Ejemplo de salida:

```
Stopping node DC1-S3  
Waiting up to 630 seconds for node shutdown
```

3. Exportar el nodo desde el host de origen.

```
sudo storagegrid node export DC1-S3
```

Ejemplo de salida:

```
Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.  
Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you  
want to import it again.
```

4. Tome nota de la `import` Comando sugerido en la salida.

Ejecutará este comando en el host de destino en el siguiente paso.

Importar nodo en el host de destino

Después de exportar el nodo desde el host de origen, importe y valide el nodo en el host de destino. La validación confirma que el nodo tiene acceso a los mismos dispositivos de interfaz de red y almacenamiento en bloque que tenía en el host de origen.

Ejecute los siguientes comandos en el *host de destino*.

Pasos

1. Importar el nodo en el host de destino.

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

Ejemplo de salida:

```
Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.  
You should run 'storagegrid node validate DC1-S3'
```

2. Validar la configuración del nodo en el nuevo host.

```
sudo storagegrid node validate DC1-S3
```

Ejemplo de salida:

```
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, corríjalo antes de iniciar el nodo migrado.

Para obtener información sobre solución de problemas, consulte las instrucciones de instalación de StorageGRID para su sistema operativo Linux.

- ["Instalar StorageGRID en Red Hat Enterprise Linux"](#)
- ["Instalar StorageGRID en Ubuntu o Debian"](#)

Iniciar el nodo migrado

Después de validar el nodo migrado, inicie el nodo ejecutando un comando en el *host de destino*.

Pasos

1. Inicie el nodo en el nuevo host.

```
sudo storagegrid node start DC1-S3
```

2. Sign in en Grid Manager y verifique que el estado del nodo sea verde sin ninguna alerta.



Verificar que el estado del nodo sea verde garantiza que el nodo migrado se haya reiniciado por completo y se haya reincorporado a la red. Si el estado no es verde, no migre ningún nodo adicional para no tener más de un nodo fuera de servicio.

3. Si no puede acceder al Administrador de cuadrícula, espere 10 minutos y luego ejecute el siguiente comando:

```
sudo storagegrid node status _node-name
```

Confirme que el nodo migrado tenga un estado de ejecución en ejecución.

VMware: Configurar la máquina virtual para el reinicio automático

Si la máquina virtual no se reinicia después de reiniciar VMware vSphere Hypervisor, es posible que deba configurar la máquina virtual para que se reinicie automáticamente.

Debe realizar este procedimiento si nota que una máquina virtual no se reinicia mientras recupera un nodo de la red o realiza otro procedimiento de mantenimiento.

Pasos

1. En el árbol de VMware vSphere Client, seleccione la máquina virtual que no está iniciada.
2. Haga clic derecho en la máquina virtual y seleccione **Encender**.
3. Configure VMware vSphere Hypervisor para reiniciar la máquina virtual automáticamente en el futuro.

Recuperar o reemplazar nodos

Advertencias y consideraciones para la recuperación del nodo de la red

Si un nodo de la red falla, debes recuperarlo lo antes posible. Debe revisar todas las advertencias y consideraciones para la recuperación del nodo antes de comenzar.



StorageGRID es un sistema distribuido compuesto por múltiples nodos que trabajan entre sí. No utilice instantáneas de disco para restaurar nodos de la red. En su lugar, consulte los procedimientos de recuperación y mantenimiento para cada tipo de nodo.



Si un sitio completo de StorageGRID ha fallado, comuníquese con el soporte técnico. El soporte técnico trabajará con usted para desarrollar y ejecutar un plan de recuperación del sitio que maximice la cantidad de datos recuperados y cumpla con sus objetivos comerciales. Ver ["Cómo el soporte técnico recupera un sitio"](#).

Algunas de las razones para recuperar un nodo de red fallido lo antes posible incluyen las siguientes:

- Un nodo de red fallido puede reducir la redundancia de los datos del sistema y de los objetos, dejándolo vulnerable al riesgo de pérdida permanente de datos si otro nodo falla.
- Un nodo de red fallido puede afectar la eficiencia de las operaciones diarias.
- Un nodo de red fallido puede reducir su capacidad para monitorear las operaciones del sistema.
- Un nodo de red fallido puede provocar un error interno del servidor 500 si se aplican reglas ILM estrictas.
- Si un nodo de la red no se recupera rápidamente, los tiempos de recuperación podrían aumentar. Por ejemplo, podrían formarse colas que sea necesario eliminar antes de que se complete la recuperación.

Siga siempre el procedimiento de recuperación para el tipo específico de nodo de red que está recuperando. Los procedimientos de recuperación varían para los nodos de administración primarios o no primarios, los nodos de puerta de enlace, los nodos de dispositivo y los nodos de almacenamiento.

Condiciones previas para la recuperación de nodos de la red

Al recuperar nodos de la red se asumen todas las siguientes condiciones:

- Se ha reemplazado y configurado el hardware físico o virtual fallado.
- La versión del instalador del dispositivo StorageGRID en el dispositivo de reemplazo coincide con la versión del software de su sistema StorageGRID, como se describe en ["Verificar y actualizar la versión del instalador del dispositivo StorageGRID"](#).
- Si está recuperando un nodo de red que no sea el nodo de administración principal, existe conectividad entre el nodo de red que se está recuperando y el nodo de administración principal.
- Si está recuperando un nodo de almacenamiento del dispositivo, debe especificar el mismo tipo de almacenamiento que el dispositivo original (combinado, solo metadatos o solo datos) durante la instalación del dispositivo. Si especifica un tipo de almacenamiento diferente, la recuperación fallará y será necesario reinstalar el dispositivo con el tipo de almacenamiento correcto especificado.

Orden de recuperación de nodos si falla un servidor que aloja más de un nodo de red

Si falla un servidor que aloja más de un nodo de red, puede recuperar los nodos en cualquier orden. Sin embargo, si el servidor fallido aloja el nodo de administración principal, primero deberá recuperar ese nodo. Recuperar primero el nodo de administración principal evita que otras recuperaciones de nodos se detengan mientras esperan comunicarse con el nodo de administración principal.

Direcciones IP de los nodos recuperados

No intente recuperar un nodo utilizando una dirección IP que esté actualmente asignada a cualquier otro nodo. Al implementar el nuevo nodo, utilice la dirección IP actual del nodo fallido o una dirección IP no utilizada.

Si utiliza una nueva dirección IP para implementar el nuevo nodo y luego recupera el nodo, la nueva dirección IP seguirá utilizándose para el nodo recuperado. Si desea volver a la dirección IP original, utilice la herramienta Cambiar IP una vez completada la recuperación.

Reúna los materiales necesarios para la recuperación del nodo de la red

Antes de realizar procedimientos de mantenimiento, debe asegurarse de tener los materiales necesarios para recuperar un nodo de red fallido.

Artículo	Notas
Archivo de instalación de StorageGRID	Si necesita recuperar un nodo de la red, debe 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.
Servicio de computadora portátil	La computadora portátil de servicio debe tener lo siguiente: • Puerto de red • Cliente SSH (por ejemplo, PuTTY) • "Navegador web compatible"

Artículo	Notas
Paquete de recuperación .zip archivo	Obtenga una copia del paquete de recuperación más reciente .zip archivo: <code>sgws-recovery-package-id-revision.zip</code> El contenido de la .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 fallas de la red. 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 al Administrador de red, 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 para el paquete de recuperación: <code>/var/local/install/sgws-recovery-package-grid-id-revision.zip.gpg</code> Utilice el paquete de recuperación con el número de revisión más alto.
`Passwords.txt` archivo	Contiene las contraseñas necesarias para acceder a los nodos de la red en la línea de comando. Incluido en el paquete de recuperación.
Frase de contraseña de aprovisionamiento	La frase de contraseña se crea y se documenta cuando se instala por primera vez el sistema StorageGRID . La frase de contraseña de aprovisionamiento no está en el <code>Passwords.txt</code> archivo.
Documentación actual para su plataforma	Vaya al sitio web del proveedor de la plataforma para obtener la documentación. Para conocer las versiones compatibles actuales de su plataforma, consulte la "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 esté ["Recuperación de volúmenes de almacenamiento fallidos en un nodo de almacenamiento"](#) .

Debe utilizar la versión de StorageGRID que se esté ejecutando actualmente en la red.

Pasos

1. Determinar qué versión del software está instalada actualmente. Desde la parte superior del Administrador de cuadrícula, seleccione el ícono de ayuda y seleccione **Acerca de**.
2. Ir a la ["Página de descargas de NetApp para StorageGRID"](#) .
3. Seleccione la versión de StorageGRID que se está ejecutando actualmente en la red.

Las versiones del software StorageGRID tienen este formato: 11.x.y .

4. Sign in con el nombre de usuario y la contraseña de su cuenta de NetApp .
5. Lea el Acuerdo de licencia de usuario final, seleccione la casilla de verificación y luego seleccione **Aceptar y continuar**.
6. En la columna **Instalar StorageGRID** de la página de descarga, seleccione la opción .tgz o .zip archivo para su plataforma.

La versión que se muestra en el archivo de instalación debe coincidir con la versión del software que está instalado actualmente.

Utilice el .zip archivo si está ejecutando Windows.

Plataforma	Archivo de instalación
Red Hat Enterprise Linux	StorageGRID-Webscale-version-RPM-uniqueID.zip StorageGRID-Webscale-version-RPM-uniqueID.tgz
Ubuntu o Debian o electrodomésticos	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 comprimido.
8. Siga el paso apropiado para su plataforma para elegir los archivos que necesita, en función de su plataforma y de los nodos de la red que necesita recuperar.

Las rutas enumeradas en el paso para cada plataforma son relativas al directorio de nivel superior instalado por el archivo de almacenamiento.

9. Si se está recuperando de una "[Sistema Red Hat Enterprise Linux](#)" , seleccione los archivos apropiados.

Ruta y nombre de archivo	Descripción
	Un 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.
	Paquete RPM para instalar el servicio de host StorageGRID en sus hosts RHEL.

Ruta y nombre de archivo	Descripción
Herramienta de scripting de implementación	Descripción
	Un script de Python utilizado para automatizar la configuración de un sistema StorageGRID .
	Un script de Python utilizado para automatizar la configuración de dispositivos StorageGRID .
	Un archivo de configuración de ejemplo para usar con el <code>configure-storagegrid.py</code> guion.
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único está habilitado. También puede utilizar este script para la integración de Ping Federate.
	Un archivo de configuración en blanco para usar con el <code>configure-storagegrid.py</code> guion.
	Ejemplo de rol y manual de Ansible para configurar hosts RHEL para la implementación de contenedores StorageGRID . Puede personalizar el rol o el libro de jugadas según sea necesario.
	Un ejemplo de secuencia de comandos de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script de ayuda llamado por el compañero <code>storagegrid-ssoauth-azure.py</code> Script de Python para realizar interacciones de SSO con Azure.
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno de StorageGRID que no sea de producción para realizar pruebas de compatibilidad de actualización.

1. Si se está recuperando de una "Sistema Ubuntu o Debian" , seleccione los archivos apropiados.

Ruta y nombre de archivo	Descripción
	Un 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 puede utilizar para realizar pruebas e implementaciones de prueba de concepto.
	Paquete DEB para instalar las imágenes del nodo StorageGRID en hosts Ubuntu o Debian.
	Suma de comprobación MD5 del archivo /debs/storagegrid-webscale-images-version-SHA.deb .
	Paquete DEB para instalar el servicio de host StorageGRID en hosts Ubuntu o Debian.
Herramienta de scripting de implementación	Descripción
	Un script de Python utilizado para automatizar la configuración de un sistema StorageGRID .
	Un script de Python utilizado para automatizar la configuración de dispositivos StorageGRID .
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único está habilitado. También puede utilizar este script para la integración de Ping Federate.
	Un archivo de configuración de ejemplo para usar con el <code>configure-storagegrid.py</code> guion.
	Un archivo de configuración en blanco para usar con el <code>configure-storagegrid.py</code> guion.
	Ejemplo de rol y manual de estrategias de Ansible para configurar hosts Ubuntu o Debian para la implementación de contenedores StorageGRID . Puede personalizar el rol o el libro de jugadas según sea necesario.

Ruta y nombre de archivo	Descripción
	Un ejemplo de secuencia de comandos de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script de ayuda llamado por el compañero <code>storagegrid-ssoauth-azure.py</code> Script de Python para realizar interacciones de SSO con Azure.
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno de StorageGRID que no sea de producción para realizar pruebas de compatibilidad de actualización.

1. Si se está recuperando de una "Sistema VMware" , seleccione los archivos apropiados.

Ruta y nombre de archivo	Descripción
	Un 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 la máquina virtual que se utiliza como plantilla para crear máquinas virtuales de nodo de cuadrícula.
	El archivo de plantilla de formato de virtualización abierta(<code>.ovf</code>) y archivo de manifiesto(<code>.mf</code>) para implementar el nodo de administración principal.
	El archivo de plantilla(<code>.ovf</code>) y archivo de manifiesto(<code>.mf</code>) para implementar nodos de administración no principales.
	El archivo de plantilla(<code>.ovf</code>) y archivo de manifiesto(<code>.mf</code>) para implementar nodos de puerta de enlace.

Ruta y nombre de archivo	Descripción
	El archivo de plantilla(<code>.ovf</code>) y archivo de manifiesto(<code>.mf</code>) para implementar nodos de almacenamiento basados en máquinas virtuales.
Herramienta de scripting de implementación	Descripción
	Un script de shell Bash utilizado para automatizar la implementación de nodos de red virtuales.
	Un archivo de configuración de ejemplo para usar con el <code>deploy-vsphere-ovftool.sh</code> guion.
	Un script de Python utilizado para automatizar la configuración de un sistema StorageGRID .
	Un script de Python utilizado para automatizar la configuración de dispositivos StorageGRID .
	Un ejemplo de script de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único (SSO) está habilitado. También puede utilizar este script para la integración de Ping Federate.
	Un archivo de configuración de ejemplo para usar con el <code>configure-storagegrid.py</code> guion.
	Un archivo de configuración en blanco para usar con el <code>configure-storagegrid.py</code> guion.
	Un ejemplo de secuencia de comandos de Python que puede utilizar para iniciar sesión en la API de administración de Grid cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script de ayuda llamado por el compañero <code>storagegrid-ssoauth-azure.py</code> Script de Python para realizar interacciones de SSO con Azure.

Ruta y nombre de archivo	Descripción
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puede usar estos esquemas para confirmar que cualquier código que haya escrito para usar las API de administración de StorageGRID será compatible con la nueva versión de StorageGRID si no tiene un entorno de StorageGRID que no sea de producción para realizar pruebas de compatibilidad de actualización.

1. Si está recuperando un sistema basado en un dispositivo StorageGRID , seleccione los archivos apropiados.

Ruta y nombre de archivo	Descripción
	Paquete DEB para instalar las imágenes del nodo StorageGRID en sus dispositivos.
	Suma de comprobación MD5 del archivo <code>/debs/storagegridwebscale-images-version-SHA.deb</code> .



Para la instalación del dispositivo, estos archivos solo son necesarios si necesita evitar el tráfico de red. El dispositivo puede descargar los archivos necesarios desde el nodo de administración principal.

Seleccionar el procedimiento de recuperación del nodo

Debe seleccionar el procedimiento de recuperación correcto para el tipo de nodo que ha fallado.

Nodo de cuadrícula	Procedimiento de recuperación
Más de un nodo de almacenamiento	Póngase en contacto con el soporte técnico. Si ha fallado más de un nodo de almacenamiento, el soporte técnico debe ayudar con la recuperación para evitar inconsistencias en la base de datos que podrían provocar la pérdida de datos. Podría ser necesario un procedimiento de recuperación del sitio. "Cómo el soporte técnico recupera un sitio"
Un solo nodo de almacenamiento	El procedimiento de recuperación del nodo de almacenamiento depende del tipo y la duración de la falla. "Recuperarse de fallos del nodo de almacenamiento"

Nodo de cuadrícula	Procedimiento de recuperación
Nodo de administración	El procedimiento del nodo de administración depende de si necesita recuperar el nodo de administración principal o un nodo de administración no principal. "Recuperarse de fallos del nodo de administración"
Nodo de puerta de enlace	"Recuperarse de fallos del nodo de enlace"
Nodo de archivo	"Recuperación de errores del nodo de archivo (sitio de documentación de StorageGRID 11.8)"



Si falla un servidor que aloja más de un nodo de red, puede recuperar los nodos en cualquier orden. Sin embargo, si el servidor fallido aloja el nodo de administración principal, primero deberá recuperar ese nodo. Recuperar primero el nodo de administración principal evita que otras recuperaciones de nodos se detengan mientras esperan comunicarse con el nodo de administración principal.

Recuperarse de fallos del nodo de almacenamiento

Recuperarse de fallos del nodo de almacenamiento

El procedimiento para recuperar un nodo de almacenamiento fallido depende del tipo de falla y del tipo de nodo de almacenamiento que ha fallado.

Utilice esta tabla para seleccionar el procedimiento de recuperación para un nodo de almacenamiento fallido.

Asunto	Acción	Notas
- Más de un nodo de almacenamiento ha fallado. - Un segundo nodo de almacenamiento falló menos de 15 días después de una falla o recuperación del nodo de almacenamiento. Esto incluye el caso en el que un nodo de almacenamiento falla mientras la recuperación de otro nodo de almacenamiento aún está en proceso.	Póngase en contacto con el soporte técnico.	La recuperación de más de un nodo de almacenamiento (o más de un nodo de almacenamiento en un plazo de 15 días) podría afectar la integridad de la base de datos de Cassandra, lo que puede provocar la pérdida de datos. El soporte técnico puede determinar cuándo es seguro comenzar 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 todas las solicitudes de servicio de plataforma pendientes para ese sitio.

Asunto	Acción	Notas
Ha fallado más de un nodo de almacenamiento en un sitio o ha fallado un sitio entero.	Póngase en contacto con el soporte técnico. Podría ser necesario realizar un procedimiento de recuperación del sitio.	El soporte técnico evaluará su situación y desarrollará un plan de recuperación. Ver "Cómo el soporte técnico recupera un sitio" .
Se ha producido un error en un nodo de almacenamiento del dispositivo.	"Recuperar el nodo de almacenamiento del dispositivo"	El procedimiento de recuperación de los nodos de almacenamiento del dispositivo es el mismo para todas las fallas.
Uno o más volúmenes de almacenamiento han fallado, pero la unidad del sistema está intacta	"Recuperarse de una falla del volumen de almacenamiento donde la unidad del sistema está intacta"	Este procedimiento se utiliza para nodos de almacenamiento basados en software.
La unidad del sistema ha fallado.	"Recuperarse de una falla de la unidad del sistema"	El procedimiento de reemplazo de nodo depende de la plataforma de implementación y de si algún volumen de almacenamiento también ha fallado.



Algunos procedimientos de recuperación de StorageGRID utilizan Reaper para manejar las reparaciones de Cassandra. Las reparaciones se producen automáticamente tan pronto como se hayan iniciado los servicios relacionados o requeridos. Es posible que notes que la salida del script menciona "reaper" o "reparación de Cassandra". Si ve un mensaje de error que indica que la reparación ha fallado, ejecute el comando indicado en el mensaje de error.

Recuperar el nodo de almacenamiento del dispositivo

Advertencias para recuperar nodos de almacenamiento del dispositivo

El procedimiento para recuperar un nodo de almacenamiento de un dispositivo StorageGRID fallido es el mismo independientemente de si se está recuperando de la pérdida de la unidad del sistema o de la pérdida de volúmenes de almacenamiento únicamente.



Si más de un nodo de almacenamiento ha fallado (o está fuera de línea), comuníquese con el soporte técnico. No realice el siguiente procedimiento de recuperación. Podría ocurrir pérdida de datos.



Si esta es la segunda falla del nodo de almacenamiento en menos de 15 días después de una falla o recuperación del nodo de almacenamiento, comuníquese con el soporte técnico. Reconstruir Cassandra en dos o más nodos de almacenamiento dentro de 15 días puede provocar la pérdida de datos.



Si ha fallado más de un nodo de almacenamiento en un sitio, es posible que se requiera un procedimiento de recuperación del sitio. Ver "[Cómo el soporte técnico recupera un sitio](#)".



Si las reglas de ILM están configuradas para almacenar solo una copia replicada y la copia existe en un volumen de almacenamiento que ha fallado, no podrá recuperar el objeto.



Para conocer los procedimientos de mantenimiento de hardware, como las instrucciones para reemplazar un controlador o reinstalar SANtricity OS, consulte la "[Instrucciones de mantenimiento para su dispositivo de almacenamiento](#)".

Preparar el nodo de almacenamiento del dispositivo para la reinstalación

Al recuperar un nodo de almacenamiento de un dispositivo, primero debe preparar el dispositivo para la reinstalación del software StorageGRID .

Pasos

1. Inicie sesión en el nodo de almacenamiento fallido:

- Introduzca el siguiente comando: `ssh admin@grid_node_IP`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- Introduzca el siguiente comando para cambiar a root: `su -`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de \$ a # .

2. Prepare el nodo de almacenamiento del dispositivo para la instalación del software StorageGRID .

```
sgareinstall
```

3. Cuando se le solicite continuar, ingrese: `y`

El dispositivo se reinicia y su sesión SSH finaliza. Por lo general, el instalador del dispositivo StorageGRID tarda unos 5 minutos en estar disponible, aunque en algunos casos es posible que tengas que esperar hasta 30 minutos.



No intente acelerar el reinicio apagando y encendiendo el dispositivo ni reiniciándolo de ninguna otra manera. Podría interrumpir las actualizaciones automáticas del BIOS, BMC u otro firmware.

El nodo de almacenamiento del dispositivo StorageGRID se restablece y los datos en el nodo de almacenamiento ya no son accesibles. Las direcciones IP configuradas durante el proceso de instalación original deben permanecer intactas; sin embargo, se recomienda que lo confirme una vez completado el procedimiento.

Después de ejecutar el `sgareinstall` comando, se eliminan todas las cuentas, contraseñas y claves SSH proporcionadas por StorageGRID y se generan nuevas claves de host.

Iniciar la instalación del dispositivo StorageGRID

Para instalar StorageGRID en un nodo de almacenamiento del dispositivo, utilice el

instalador del dispositivo StorageGRID , que está incluido en el dispositivo.

Antes de empezar

- El dispositivo se ha instalado en un rack, se ha conectado a sus redes y se ha encendido.
- Los enlaces de red y las direcciones IP se han configurado para el dispositivo mediante el instalador de dispositivos StorageGRID .
- Conoce la dirección IP del nodo de administración principal de la red StorageGRID .
- Todas las subredes de la red Grid que aparecen en la página de configuración de IP del instalador del dispositivo StorageGRID se han definido en la lista de subredes de la red Grid en el nodo de administración principal.
- Ha completado estas tareas previas siguiendo las instrucciones de instalación para su dispositivo de almacenamiento. Ver "[Inicio rápido para la instalación de hardware](#)" .
- Estás usando un "[navegador web compatible](#)" .
- Conoce una de las direcciones IP asignadas al controlador de cómputo en el dispositivo. Puede utilizar la dirección IP para la red de administración (puerto de administración 1 en el controlador), la red de cuadrícula o la red de cliente.

Acerca de esta tarea

Para instalar StorageGRID en un nodo de almacenamiento del dispositivo:

- Usted especifica o confirma la dirección IP del nodo de administración principal y el nombre de host (nombre del sistema) del nodo.
- Inicia la instalación y espera mientras se configuran los volúmenes y se instala el software.



Al recuperar un nodo de almacenamiento del dispositivo, vuelva a instalarlo con el mismo tipo de almacenamiento que el dispositivo original (combinado, solo metadatos o solo datos). Si especifica un tipo de almacenamiento diferente, la recuperación fallará y será necesario reinstalar el dispositivo con el tipo de almacenamiento correcto especificado.

- A mitad 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 fallido.
- Una vez configurado el nodo, se completa el proceso de instalación del dispositivo y éste se reinicia.

Pasos

1. Abra un navegador e ingrese una de las direcciones IP del controlador de cómputo en el dispositivo.

```
https://Controller_IP:8443
```

Aparece la página de inicio del instalador del dispositivo StorageGRID .

2. En la sección de conexión del nodo de administración principal, determine si necesita especificar la dirección IP para el nodo de administración principal.

El instalador del dispositivo StorageGRID puede descubrir esta dirección IP automáticamente, suponiendo que el nodo de administración principal, o al menos otro nodo de la red con ADMIN_IP configurado, esté presente en la misma subred.

3. Si esta dirección IP no se muestra o necesita cambiarla, especifique la dirección:

Opción	Pasos
Entrada manual de IP	a. Desmarque la casilla de verificación Habilitar descubrimiento de nodo de administración. b. Introduzca la dirección IP manualmente. c. Haga clic en Guardar. d. Espere mientras el estado de conexión de la nueva dirección IP pasa a ser "listo".
Descubrimiento automático de todos los nodos de administración principales conectados	a. Seleccione la casilla de verificación Habilitar descubrimiento de nodo de administración. b. De la lista de direcciones IP descubiertas, seleccione el nodo de administración principal para la red donde se implementará este nodo de almacenamiento del dispositivo. c. Haga clic en Guardar. d. Espere mientras el estado de conexión de la nueva dirección IP pasa a ser "listo".

4. En el campo **Nombre del nodo**, ingrese el mismo nombre de host (nombre del sistema) que se utilizó para el nodo que está recuperando y haga clic en **Guardar**.
5. En la sección Instalación, confirme que el estado actual sea "Listo para iniciar la instalación de *node name* en la red con el nodo de administración principal ``admin_ip``" y que el botón **Iniciar instalación** esté habilitado.

Si el botón **Iniciar instalación** no está habilitado, es posible que necesite cambiar la configuración de red o la configuración del puerto. Para obtener instrucciones, consulte las instrucciones de mantenimiento de su aparato.

6. Desde la página de inicio del instalador del dispositivo StorageGRID , haga clic en **Iniciar instalación**.

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.

Primary Admin Node connection

Enable Admin Node discovery

☐

Primary Admin Node IP

172.16.4.210

Connection state

Connection to 172.16.4.210 ready

Cancel

Save

Node name

Node name

NetApp-SGA

Cancel

Save

Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

Start Installation

El estado actual cambia a "La instalación está en curso" y se muestra la página de instalación del monitor.



Si necesita acceder manualmente a la página de instalación del monitor, haga clic en **Instalación del monitor** en la barra de menú. Ver "[Supervisar la instalación del dispositivo](#)"

Supervisar la instalación del dispositivo StorageGRID

El instalador del dispositivo StorageGRID proporciona el estado hasta que se completa la instalación. Una vez finalizada la instalación del software, el dispositivo se reinicia.

Pasos

1. Para supervisar el progreso de la instalación, haga clic en **Supervisar instalación** en la barra de menú.

La página de instalación del monitor muestra el progreso de la instalación.

Monitor Installation

1. Configure storage			Running
Step	Progress	Status	
Connect to storage controller		Complete	
Clear existing configuration		Complete	
Configure volumes		Creating volume StorageGRID-obj-00	
Configure host settings		Pending	

2. Install OS	Pending
3. Install StorageGRID	Pending
4. Finalize installation	Pending

La barra de estado azul indica qué tarea está actualmente en progreso. Las barras de estado verdes indican tareas que se han completado correctamente.



El instalador garantiza que las tareas completadas en una instalación anterior no se vuelvan a ejecutar. Si está volviendo a ejecutar una instalación, cualquier tarea que no necesite volver a ejecutarse se mostrará con una barra de estado verde y un estado de "Omitido".

2. Revise el progreso de las dos primeras etapas de instalación.

- **1. Configurar almacenamiento**

Durante esta etapa, el instalador se conecta al controlador de almacenamiento, borra cualquier configuración existente, se comunica con SANtricity OS para configurar volúmenes y configura los ajustes del host.

- **2. Instalar sistema operativo**

Durante esta etapa, el instalador copia la imagen del sistema operativo base de StorageGRID al dispositivo.

3. Continúe monitoreando el progreso de la instalación hasta que la etapa **Instalar StorageGRID** se pause y aparezca un mensaje en la consola integrada que le solicite que apruebe este nodo en el Nodo de administración mediante el Administrador de Grid.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

4. Vaya a ["Seleccione Iniciar recuperación para configurar el nodo de almacenamiento del dispositivo"](#).

Seleccione Iniciar recuperación para configurar el nodo de almacenamiento del dispositivo

Debe seleccionar Iniciar recuperación en el Administrador de red para configurar un nodo de almacenamiento del dispositivo como reemplazo del nodo fallido.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de mantenimiento o acceso root"](#).
- Tienes la contraseña de aprovisionamiento.

- Ha implementado un nodo de almacenamiento de dispositivo de recuperación.
- Tienes la fecha de inicio de cualquier trabajo de reparación de datos codificados por borrado.
- Ha verificado que el nodo de almacenamiento no se ha reconstruido en los últimos 15 días.

Pasos

1. Desde el Administrador de red, seleccione **MANTENIMIENTO > Tareas > Recuperación**.
2. Seleccione el nodo de la cuadrícula que desea recuperar en la lista de Nodos pendientes.

Los nodos aparecen en la lista después de fallar, pero no puedes seleccionar un nodo hasta que se haya reinstalado y esté listo para la recuperación.

3. Introduzca la **contraseña de aprovisionamiento**.
4. Haga clic en **Iniciar recuperación**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search Q				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	

Passphrase

Provisioning Passphrase

Start Recovery

5. Supervise el progreso de la recuperación en la tabla Nodo de cuadrícula en recuperación.

Cuando el nodo de la red llega a la etapa "Esperando pasos manuales", vaya al siguiente tema y realice los pasos manuales para volver a montar y reformatar los volúmenes de almacenamiento del dispositivo.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Recovering Grid Node

Name	Start Time	Progress	Stage
dc2-s3	2016-09-12 16:12:40 PDT		Waiting For Manual Steps

Reset



En cualquier momento durante la recuperación, puede hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparece un cuadro de diálogo que indica que el nodo quedará en un estado indeterminado si restablece el procedimiento.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Si desea volver a intentar la recuperación después de restablecer el procedimiento, debe restaurar el nodo del dispositivo a un estado preinstalado ejecutando `sgareinstall` en el nodo.

Volver a montar y reformatear los volúmenes de almacenamiento del dispositivo (pasos manuales)

Debe ejecutar manualmente dos scripts para volver a montar los volúmenes de almacenamiento preservados y reformatear cualquier volumen de almacenamiento fallido. El primer script vuelve a montar los volúmenes que están formateados correctamente como volúmenes de almacenamiento StorageGRID . El segundo script reformatea cualquier volumen no montado, reconstruye la base de datos de Cassandra, si es necesario, e inicia los servicios.

Antes de empezar

- Ya ha reemplazado el hardware de todos los volúmenes de almacenamiento fallidos que sabe que requieren reemplazo.

Ejecutando el `sn-remount-volumes` El script podría ayudarle a identificar volúmenes de almacenamiento fallidos adicionales.

- Ha verificado que no se está realizando un desmantelamiento de un nodo de almacenamiento o ha pausado el procedimiento de desmantelamiento del nodo. (En el Administrador de red, seleccione **MANTENIMIENTO > Tareas > Desmantelamiento.**)
- Has comprobado que no hay ninguna expansión en curso. (En el Administrador de cuadrícula, seleccione **MANTENIMIENTO > Tareas > Expansión.**)



Comuníquese con el soporte técnico si más de un nodo de almacenamiento está fuera de línea o si un nodo de almacenamiento en esta red se ha reconstruido en los últimos 15 días. No corras el `sn-recovery-postinstall.sh` guion. La reconstrucción de Cassandra en dos o más nodos de almacenamiento con una diferencia de 15 días entre sí podría provocar la 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.
- Ejecutar el `sn-remount-volumes` script para volver a montar volúmenes de almacenamiento formateados correctamente. Cuando se ejecuta este script, hace 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 consistente, determina si el volumen de almacenamiento es un volumen de almacenamiento StorageGRID con el formato correcto.
 - Si el volumen de almacenamiento está formateado correctamente, vuelve a montar el volumen de almacenamiento. Todos los datos existentes en el volumen permanecen intactos.
- Revise la salida del script y resuelva cualquier problema.
- Ejecutar el `sn-recovery-postinstall.sh` guion. Cuando este script se ejecuta, hace lo siguiente.



No reinicie un nodo de almacenamiento durante la recuperación antes de ejecutarlo `sn-recovery-postinstall.sh` (paso 4) para reformatear los volúmenes de almacenamiento fallidos y restaurar los metadatos de los objetos. Reiniciar el nodo de almacenamiento antes `sn-recovery-postinstall.sh` Completa las causas de errores en los servicios que intentan iniciarse y provoca que los nodos del dispositivo StorageGRID salgan del modo de mantenimiento.

- Reformatea cualquier volumen de almacenamiento que `sn-remount-volumes` No se pudo montar el script o se encontró que estaba formateado incorrectamente.



Si se reformatea un volumen de almacenamiento, se perderán todos los datos de ese volumen. Debe realizar un procedimiento adicional para restaurar datos de objetos desde otras ubicaciones en la cuadrícula, asumiendo que las reglas ILM se configuraron para almacenar más de una copia de objeto.

- Reconstruye la base de datos de 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 el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Ejecute el primer script para volver a montar cualquier volumen de almacenamiento formateado correctamente.



Si todos los volúmenes de almacenamiento son nuevos y necesitan formatearse, o si todos los volúmenes de almacenamiento han fallado, puede omitir este paso y ejecutar el segundo script para reformatear todos los volúmenes de almacenamiento sin montar.

a. Ejecute el script: `sn-remount-volumes`

Este script puede tardar horas en ejecutarse en volúmenes de almacenamiento que contienen datos.

b. Mientras se ejecuta el script, revise el resultado y responda las indicaciones.



Según sea necesario, puede utilizar el `tail -f` Comando para monitorear el contenido del archivo de registro del script(`/var/local/log/sn-remount-volumes.log`). El archivo de registro contiene información más detallada que la salida 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 will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

===== Device /dev/sdd =====
```



```

Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

===== Device /dev/sde =====
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.

```

En el ejemplo de salida, un volumen de almacenamiento se volvió a montar correctamente y tres volúmenes de almacenamiento tuvieron errores.

- `/dev/sdb` Pasó la verificación de consistencia del sistema de archivos XFS y tenía una estructura de volumen válida, por lo que se volvió a montar correctamente. Se conservan los datos de los dispositivos que se vuelven a montar mediante el script.
- `/dev/sdc` No se pudo pasar 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 se inicializó o el superbloque del disco estaba dañado. Cuando el script no puede montar un volumen de almacenamiento, le pregunta si desea

ejecutar la verificación de consistencia del sistema de archivos.

- Si el volumen de almacenamiento está conectado a un nuevo disco, responda **N** a la pregunta. No es necesario comprobar el sistema de archivos en un disco nuevo.
- Si el volumen de almacenamiento está conectado a un disco existente, responda **Y** a la pregunta. Puede utilizar los resultados de la comprobación del sistema de archivos para determinar el origen de la corrupción. Los resultados se guardan en el `/var/local/log/sn-remount-volumes.log` archivo de registro.
- `/dev/sde`Pasó la verificación de consistencia del sistema de archivos XFS y tenía una estructura de volumen válida; sin embargo, el ID del nodo LDR en el `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 la salida del script y resuelva cualquier problema.



Si un volumen de almacenamiento no pasó la verificación de consistencia del sistema de archivos XFS o no se pudo montar, revise cuidadosamente los mensajes de error en la salida. Debes comprender las implicaciones de ejecutar el `sn-recovery-postinstall.sh` guión en estos volúmenes.

- a. Verifique que los resultados incluyan una entrada para todos los volúmenes esperados. Si no aparece algún volumen, 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, la salida 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 se informa que un volumen de almacenamiento pertenece a otro nodo de almacenamiento, comuníquese con el soporte técnico. Si ejecuta el `sn-recovery-postinstall.sh` script, el volumen de almacenamiento se formateará, lo que podría provocar pérdida de datos.

- c. Si no se pudo montar algún dispositivo de almacenamiento, anote el nombre del dispositivo y repárelo o reemplácelo.



Debe reparar o reemplazar cualquier dispositivo de almacenamiento que no se haya podido montar.

Utilizará el nombre del dispositivo para buscar el ID del volumen, que es una entrada obligatoria cuando ejecuta el `repair-data` script para restaurar datos de objetos al volumen (el siguiente procedimiento).

- d. Después de reparar o reemplazar todos los dispositivos que no se pueden montar, ejecute el `sn-remount-volumes` Ejecute el script nuevamente para confirmar que se hayan vuelto a montar todos los volúmenes de almacenamiento que se pueden volver a montar.



Si un volumen de almacenamiento no se puede montar o está formateado incorrectamente y continúa con el siguiente paso, se eliminarán el volumen y todos los datos que contenga. Si tenía dos copias de datos de objetos, solo tendrá una copia hasta que complete el siguiente procedimiento (restauración de datos de objetos).



No corras el `sn-recovery-postinstall.sh` script si cree que los datos restantes en un volumen de almacenamiento fallido no se pueden reconstruir desde otro lugar en la red (por ejemplo, si su política ILM usa una regla que solo hace una copia o si los volúmenes han fallado en varios nodos). En su lugar, comuníquese con el soporte técnico para determinar cómo recuperar sus datos.

4. Ejecutar el `sn-recovery-postinstall.sh` guion: `sn-recovery-postinstall.sh`

Este script reformatea cualquier volumen de almacenamiento que no se pudo montar o que se encontró que estaba formateado incorrectamente; reconstruye la base de datos Cassandra en el nodo, si es necesario; e inicia los servicios en el nodo de almacenamiento.

Tenga en cuenta lo siguiente:

- El script podría tardar horas en ejecutarse.
- En general, debes dejar la sesión SSH en paz mientras se ejecuta el script.
- No presione **Ctrl+C** mientras la sesión SSH esté activa.
- El script se ejecutará en segundo plano si ocurre una interrupción en la red y finaliza la sesión SSH, pero puede ver el progreso desde la página de Recuperación.
- Si el nodo de almacenamiento utiliza el servicio RSM, es posible que el script parezca detenerse durante 5 minutos mientras se reinician los servicios del nodo. Se espera este retraso de 5 minutos cada vez que el servicio RSM se inicia por primera vez.



El servicio RSM está presente en los nodos de almacenamiento que incluyen el servicio ADC.



Algunos procedimientos de recuperación de StorageGRID utilizan Reaper para manejar las reparaciones de Cassandra. Las reparaciones se producen automáticamente tan pronto como se hayan iniciado los servicios relacionados o requeridos. Es posible que notes que la salida del script menciona "reaper" o "reparación de Cassandra". Si ve un mensaje de error que indica que la reparación ha fallado, ejecute el comando indicado en el mensaje de error.

5. Como el `sn-recovery-postinstall.sh` El script se ejecuta y supervisa la página de Recuperación en el Administrador de Grid.

La barra de progreso y la columna Etapa en la página Recuperación proporcionan un estado de alto nivel del `sn-recovery-postinstall.sh` guion.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search 				
Name	IPv4 Address	State	Recoverable	
No results found.				

Recovering Grid Node

Name	Start Time	Progress	Stage
DC1-S3	2016-06-02 14:03:35 PDT		Recovering Cassandra

6. Después de la `sn-recovery-postinstall.sh`. Una vez que el script haya iniciado servicios en el nodo, puede restaurar los datos del objeto en cualquier volumen de almacenamiento que haya sido formateado por el script.

El script le pregunta si desea utilizar el proceso de restauración de volumen de Grid Manager.

- En la mayoría de los casos, deberías "[restaurar datos de objetos usando Grid Manager](#)". Respuesta `y` para utilizar el Administrador de cuadrícula.
- En casos excepcionales, como cuando se lo solicita el soporte técnico o cuando sabe que el nodo de reemplazo tiene menos volúmenes disponibles para el almacenamiento de objetos que el nodo original, debe "[restaurar datos de objetos manualmente](#)" utilizando el `repair-data` guion. Si se aplica uno de estos casos, responda `n`.



Si respondes `n` para utilizar el proceso de restauración de volumen de Grid Manager (restaurar datos de objetos manualmente):

- No es posible restaurar datos de objetos mediante Grid Manager.
- Puede supervisar el progreso de los trabajos de restauración manual utilizando Grid Manager.

Después de realizar la selección, el script se completa y se muestran los siguientes pasos para recuperar los datos del objeto. Después de revisar estos pasos, presione cualquier tecla para regresar a la línea de comando.

Restaurar datos de objetos en el volumen de almacenamiento del dispositivo

Después de recuperar los volúmenes de almacenamiento para el nodo de almacenamiento del dispositivo, puede restaurar los datos de objetos replicados o codificados por borrado que se perdieron cuando falló el nodo de almacenamiento.

¿Qué procedimiento debo utilizar?

Siempre que sea posible, restaure los datos de los objetos utilizando la página **Restauración de volumen** en el Administrador de cuadrícula.

- Si los volúmenes se enumeran en **MANTENIMIENTO > Restauración de volumen > Nodos a restaurar**, restaure los datos del objeto utilizando el ["Página de restauración de volumen en el Administrador de cuadrícula"](#).
- Si los volúmenes no aparecen en **MANTENIMIENTO > Restauración de volúmenes > Nodos a restaurar**, siga los pasos a continuación para usar el `repair-data` script para restaurar datos de objetos.

Si el nodo de almacenamiento recuperado contiene menos volúmenes que el nodo que está reemplazando, debe usar el `repair-data` guion.



El script de reparación de datos está obsoleto y se eliminará en una versión futura. Cuando sea posible, utilice el ["Procedimiento de restauración de volumen en el Administrador de cuadrícula"](#).

Utilice el `repair-data` script para restaurar datos de objetos

Antes de empezar

- Ha confirmado que el nodo de almacenamiento recuperado tiene un estado de conexión de **Conectado***  en la pestaña ***NODOS > Descripción general** en el Administrador de cuadrícula.

Acerca de esta tarea

Los datos de objetos se pueden restaurar desde otros nodos de almacenamiento o desde un grupo de almacenamiento en la nube, suponiendo que las reglas ILM de la red se configuraron de tal manera que las copias de objetos estén disponibles.

Tenga en cuenta lo siguiente:

- Si se configuró una regla ILM para almacenar solo una copia replicada y esa copia existía en un volumen de almacenamiento que falló, no podrá recuperar el objeto.
- Si la única copia restante de un objeto está en un grupo de almacenamiento en la nube, StorageGRID debe emitir varias solicitudes al punto final del grupo de almacenamiento en la nube para restaurar los datos del objeto. Antes de realizar este procedimiento, comuníquese con el soporte técnico para obtener ayuda para estimar el tiempo de recuperación y los costos asociados.

Acerca de `repair-data` guion

Para restaurar los datos del objeto, ejecute el `repair-data` guion. Este script inicia el proceso de restauración de datos de objetos y trabaja con el escaneo ILM para garantizar que se cumplan las reglas ILM.

Seleccione **Datos replicados** o **Datos codificados por borrado (EC)** a continuación para conocer las diferentes opciones para `repair-data` script, en función de si está restaurando datos replicados o datos codificados por borrado. Si necesita restaurar ambos tipos de datos, debe ejecutar ambos conjuntos de comandos.



Para obtener más información sobre el `repair-data` guión, entrar `repair-data --help` desde la línea de comandos del nodo de administración principal.



El script de reparación de datos está obsoleto y se eliminará en una versión futura. Cuando sea posible, utilice el ["Procedimiento de restauración de volumen en el Administrador de cuadrícula"](#).

Datos replicados

Hay dos comandos disponibles para restaurar datos replicados, según si necesita reparar todo el nodo 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 datos replicados con este comando:

```
repair-data show-replicated-repair-status
```

Datos codificados por borrado (EC)

Hay dos comandos disponibles para restaurar datos codificados por borrado, según si necesita reparar todo el nodo o solo ciertos volúmenes del nodo:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Puede realizar un seguimiento de las reparaciones de datos codificados por borrado con este comando:

```
repair-data show-ec-repair-status
```



Las reparaciones de datos codificados por borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. Sin embargo, si no se pueden contabilizar todos los datos codificados por borrado, no se podrá completar la reparación. La reparación se completará después de que todos los nodos estén disponibles.



El trabajo de reparación de EC reserva temporalmente una gran cantidad de almacenamiento. Es posible que se activen alertas de almacenamiento, pero se resolverán cuando se complete la reparación. Si no hay suficiente almacenamiento para la reserva, el trabajo de reparación de EC fallará. Las reservas de almacenamiento se liberan cuando se completa el trabajo de reparación de EC, independientemente de si el trabajo falló o tuvo éxito.

Buscar el nombre de host para el 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 el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Utilice el `/etc/hosts` archivo para encontrar el nombre de host del nodo de almacenamiento para los volúmenes de almacenamiento restaurados. Para ver una lista de todos los nodos en la cuadrícula,

ingrese lo siguiente: `cat /etc/hosts`.

Reparar datos si todos los volúmenes han fallado

Si todos los volúmenes de almacenamiento han fallado, repare todo el nodo. Siga las instrucciones para **datos replicados**, **datos codificados por borrado (EC)** o ambos, según utilice datos replicados, datos codificados por borrado (EC) o ambos.

Si sólo han fallado algunos volúmenes, vaya a [Reparar datos si solo han fallado algunos volúmenes](#).



No puedes correr `repair-data` operaciones para más de un nodo al mismo tiempo. Para recuperar varios nodos, comuníquese con el soporte técnico.

Datos replicados

Si su cuadrícula incluye datos replicados, utilice el `repair-data start-replicated-node-repair` comando con el `--nodes` opción, donde `--nodes` es el nombre de host (nombre del sistema), para reparar todo el nodo de almacenamiento.

Este comando repara los datos replicados en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



A medida que se restauran los datos de los objetos, se activa la alerta **Objetos perdidos** si el sistema StorageGRID no puede localizar los datos de los objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Debe determinar la causa de la pérdida y si es posible recuperarla. Ver "[Investigar objetos perdidos](#)".

Datos codificados por borrado (EC)

Si su cuadrícula contiene datos codificados por borrado, utilice el `repair-data start-ec-node-repair` comando con el `--nodes` opción, donde `--nodes` es el nombre de host (nombre del sistema), para reparar todo el nodo de almacenamiento.

Este comando repara los datos codificados por borrado en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

La operación devuelve un valor único `repair ID` que identifica esta `repair_data` operación. Utilice este `repair ID` Para seguir el progreso y el resultado de la `repair_data` operación. No se devuelve ningún otro comentario mientras se completa el proceso de recuperación.

Las reparaciones de datos codificados por borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. La reparación se completará después de que todos los nodos estén disponibles.

Reparar datos si solo han fallado algunos volúmenes

Si sólo han fallado algunos de los volúmenes, repare los volúmenes afectados. Siga las instrucciones para **datos replicados**, **datos codificados por borrado (EC)** o ambos, según utilice datos replicados, datos codificados por borrado (EC) o ambos.

Si todos los volúmenes han fallado, vaya a [Reparar datos si todos los volúmenes han fallado](#) .

Introduzca los ID de volumen en hexadecimal. Por ejemplo, 0000 es el primer volumen y 000F Es el decimosexto volumen. Puede especificar un volumen, un rango de volúmenes o varios volúmenes que no estén en una secuencia.

Todos los volúmenes deben estar en el mismo nodo de almacenamiento. Si necesita restaurar volúmenes para más de un nodo de almacenamiento, comuníquese con el soporte técnico.

Datos replicados

Si su cuadrícula contiene datos replicados, utilice el `start-replicated-volume-repair` comando con el `--nodes` opción para identificar el nodo (donde `--nodes` es el nombre de host del nodo). Luego agregue el `--volumes` o `--volume-range` opción, como se muestra en los siguientes ejemplos.

Volumen único: este comando restaura los datos replicados al volumen 0002 en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Rango de volúmenes: este comando restaura los datos replicados en todos los volúmenes del rango 0003 a 0009 en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Varios volúmenes no en una secuencia: este comando restaura datos replicados a los volúmenes 0001 , 0005 , y 0008 en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



A medida que se restauran los datos de los objetos, se activa la alerta **Objetos perdidos** si el sistema StorageGRID no puede localizar los datos de los objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Tenga en cuenta la descripción de la alerta y las acciones recomendadas para determinar la causa de la pérdida y si es posible la recuperación.

Datos codificados por borrado (EC)

Si su cuadrícula contiene datos codificados por borrado, utilice el `start-ec-volume-repair` comando con el `--nodes` opción para identificar el nodo (donde `--nodes` es el nombre de host del nodo). Luego agregue el `--volumes` o `--volume-range` opción, 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 llamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Rango de volúmenes: este comando restaura datos codificados por borrado en todos los volúmenes del rango 0004 a 0006 en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Varios volúmenes no en una secuencia: este comando restaura datos codificados por borrado en los volúmenes 000A , 000C , y 000E en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

El `repair-data` La operación devuelve un valor único. `repair ID` que identifica esto `repair_data` operación. Utilice esto `repair ID` Para seguir el progreso y el resultado de la `repair_data` operación. No se devuelve ningún otro comentario mientras se completa el proceso de recuperación.



Las reparaciones de datos codificados por borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. La reparación se completará después de que todos los nodos estén disponibles.

Reparación de monitores

Supervise el estado de los trabajos de reparación, dependiendo de si utiliza **datos replicados**, **datos codificados por borrado (EC)** o ambos.

También puede supervisar el estado de los trabajos de restauración de volumen en proceso y ver un historial de trabajos de restauración completados en "[Administrador de red](#)".

Datos replicados

- Para obtener un porcentaje estimado de finalización de la reparación replicada, agregue el `show-replicated-repair-status` Opción para el comando `reparar-datos`.

```
repair-data show-replicated-repair-status
```

- Para determinar si las reparaciones están completas:
 - a. Seleccione **NODOS > Nodo de almacenamiento en reparación > ILM**.
 - b. Revise los atributos en la sección Evaluación. Cuando se completan las reparaciones, el atributo **En espera - Todo** indica 0 objetos.
- Para supervisar la reparación con más detalle:
 - a. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
 - b. Seleccione **grid > Nodo de almacenamiento en reparación > LDR > Almacén de datos**.
 - c. Utilice una combinación de los siguientes atributos para determinar, lo mejor posible, si las reparaciones replicadas están completas.



Pueden existir inconsistencias en Cassandra y no se realiza un seguimiento de las reparaciones fallidas.

- **Reparaciones intentadas (XRPA)**: utilice este atributo para rastrear el 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 escaneo actual (proporcionado por el atributo **Período de escaneo – Estimado**), significa que el escaneo ILM no encontró objetos de alto riesgo que necesiten reparación en ningún nodo.



Los objetos de alto riesgo son objetos que corren el riesgo de perderse por completo. Esto no incluye objetos que no satisfacen su configuración ILM.

- **Período de escaneo estimado (XSCM)**: utilice este atributo para estimar cuándo se aplicará un cambio de política a los objetos ingeridos previamente. Si el atributo **Reparaciones intentadas** no aumenta durante un período más largo que el período de escaneo actual, es probable que se realicen reparaciones replicadas. Tenga en cuenta que el período de escaneo puede cambiar. El atributo **Período de escaneo estimado (XSCM)** se aplica a toda la cuadrícula y es el máximo de todos los períodos de escaneo de nodos. Puede consultar el historial de atributos **Período de escaneo – Estimado** de la cuadrícula para determinar un período de tiempo apropiado.

Datos codificados por borrado (EC)

Para supervisar la reparación de datos codificados por borrado y volver a intentar cualquier solicitud que pueda haber fallado:

1. Determinar el estado de las reparaciones de datos codificados por borrado:
 - Seleccione **SOPORTE > Herramientas > Métricas** para ver el tiempo estimado de finalización y el porcentaje de finalización del trabajo actual. Luego, seleccione **Descripción general de EC** en la sección Grafana. Consulte los paneles **Tiempo estimado de finalización del trabajo de Grid EC** 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
```

La salida enumera información, incluyendo `repair ID`, para todas las reparaciones realizadas anteriormente y actualmente en curso.

2. Si la salida muestra que la operación de reparación falló, utilice el `--repair-id` Opción para reintentar la reparación.

Este comando vuelve a intentar una reparación de nodo fallida, utilizando el ID de reparación 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando vuelve a intentar una reparación de volumen fallida, utilizando el ID de reparación 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Comprobar el estado del almacenamiento después de recuperar el nodo de almacenamiento del dispositivo

Después de recuperar un nodo de almacenamiento del dispositivo, debe verificar que el estado deseado del nodo de almacenamiento del dispositivo esté configurado en línea y asegurarse de que el estado sea en línea de manera predeterminada cada vez que se reinicie el servidor del nodo de almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Se ha recuperado el nodo de almacenamiento y se ha completado la recuperación de datos.

Pasos

1. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
2. Verifique los valores de **Nodo de almacenamiento recuperado > LDR > Almacenamiento > Estado de almacenamiento - deseado** y **Estado de almacenamiento - actual**.

El valor de ambos atributos debe ser En línea.

3. Si el Estado de almacenamiento - Deseado está configurado en Solo lectura, complete los siguientes pasos:
 - a. Haga clic en la pestaña **Configuración**.
 - b. En la lista desplegable **Estado de almacenamiento – Deseado**, seleccione **En línea**.
 - c. Haga clic en **Aplicar cambios**.

- d. Haga clic en la pestaña **Descripción general** y confirme que los valores de **Estado de almacenamiento - Deseado** y **Estado de almacenamiento - Actual** estén actualizados a En línea.

Recuperarse de una falla del volumen de almacenamiento donde la unidad del sistema está intacta

Recuperarse de una falla del 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 donde uno o más volúmenes de almacenamiento en el nodo de almacenamiento han fallado, pero la unidad del sistema está intacta. Si solo fallaron los volúmenes de almacenamiento, el nodo de almacenamiento aún estará disponible para el sistema StorageGRID .



Este procedimiento de recuperación se aplica únicamente a los nodos de almacenamiento basados en software. Si los volúmenes de almacenamiento han fallado en un nodo de almacenamiento del dispositivo, utilice el procedimiento del dispositivo en su lugar: "[Recuperar el nodo de almacenamiento del dispositivo](#)".

Este procedimiento de recuperación incluye las siguientes tareas:

- "[Revisar las advertencias para la recuperación del volumen de almacenamiento](#)"
- "[Identificar y desmontar volúmenes de almacenamiento fallidos](#)"
- "[Recuperar los volúmenes y reconstruir la base de datos de Cassandra](#)"
- "[Restaurar datos de objetos](#)"
- "[Comprobar el estado de almacenamiento](#)"

Advertencias para la recuperación del volumen de almacenamiento

Antes de recuperar volúmenes de almacenamiento fallidos para un nodo de almacenamiento, revise las siguientes advertencias.

Los volúmenes de almacenamiento (o rangedbs) en un nodo de almacenamiento se identifican mediante un número hexadecimal, conocido como ID de 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 utiliza hasta 4 TB de espacio para metadatos de objetos y operaciones de base de datos de Cassandra; cualquier espacio restante en ese volumen se utiliza para datos de objetos. Todos los demás volúmenes de almacenamiento se utilizan exclusivamente para datos de objetos.

Si el volumen 0 falla y necesita recuperarse, la base de datos de Cassandra podría reconstruirse como parte del procedimiento de recuperación del volumen. Cassandra también podría reconstruirse en las siguientes circunstancias:

- Un nodo de almacenamiento vuelve a estar en línea después de haber estado fuera de línea durante 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 fuera de línea, es posible que algunos datos de Cassandra no estén disponibles. Si Cassandra se ha reconstruido recientemente, es posible que sus datos aún no sean

consistentes en toda la red. Puede ocurrir pérdida de datos si se reconstruye Cassandra cuando demasiados nodos de almacenamiento están fuera de línea o si dos o más nodos de almacenamiento se reconstruyen con una diferencia de 15 días entre sí.



Si más de un nodo de almacenamiento ha fallado (o está fuera de línea), comuníquese con el soporte técnico. No realice el siguiente procedimiento de recuperación. Podría ocurrir pérdida de datos.



Si esta es la segunda falla del nodo de almacenamiento en menos de 15 días después de una falla o recuperación del nodo de almacenamiento, comuníquese con el soporte técnico. Reconstruir Cassandra en dos o más nodos de almacenamiento dentro de 15 días puede provocar la pérdida de datos.



Si ha fallado más de un nodo de almacenamiento en un sitio, es posible que se requiera un procedimiento de recuperación del sitio. Ver "[Cómo el soporte técnico recupera un sitio](#)".



Si las reglas de ILM están configuradas para almacenar solo una copia replicada y la copia existe en un volumen de almacenamiento que ha fallado, no podrá recuperar el objeto.

Información relacionada

["Advertencias y consideraciones para la recuperación del nodo de la red"](#)

Identificar y desmontar volúmenes de almacenamiento fallidos

Al recuperar un nodo de almacenamiento con volúmenes de almacenamiento fallidos, debe identificar y desmontar los volúmenes fallidos. Debe verificar que solo se reformateen los volúmenes de almacenamiento fallidos como parte del procedimiento de recuperación.

Antes de empezar

Ha iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".

Acerca de esta tarea

Debe recuperar los volúmenes de almacenamiento fallidos lo antes posible.

El primer paso del proceso de recuperación es detectar volúmenes que se han desconectado, necesitan desmontarse o tienen errores de E/S. Si los volúmenes fallidos aún están conectados pero tienen un sistema de archivos dañado aleatoriamente, es posible que el sistema no detecte ninguna corrupción en partes no utilizadas o no asignadas del disco.



Debe finalizar este procedimiento antes de realizar pasos manuales para recuperar los volúmenes, como agregar o volver a conectar los discos, detener el nodo, iniciar el nodo o reiniciar. De lo contrario, cuando se ejecuta el `reformat_storage_block_devices.rb` script, es posible que se produzca un error en el sistema de archivos que provoque que el script se bloquee o falle.



Repare el hardware y coloque correctamente los discos antes de ejecutar el `reboot dominio`.



Identifique cuidadosamente los volúmenes de almacenamiento fallidos. Utilizará esta información para verificar qué volúmenes deben reformatearse. Una vez reformateado un volumen, no se pueden recuperar los datos del volumen.

Para recuperar correctamente los volúmenes de almacenamiento fallidos, debe conocer los nombres de los dispositivos de los volúmenes de almacenamiento fallidos y sus identificadores de volumen.

Durante la instalación, a cada dispositivo de almacenamiento se le asigna un identificador único universal (UUID) de sistema de archivos y se monta en un directorio rangedb en el nodo de almacenamiento utilizando ese UUID de sistema de archivos asignado. El UUID del sistema de archivos y el directorio rangedb se enumeran en el `/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, el dispositivo `/dev/sdc` tiene un tamaño de volumen de 4 TB, está montado en `/var/local/rangedb/0`, utilizando el nombre del dispositivo `/dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-elcf1809faba` en el `/etc/fstab` archivo:

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	croot	Online	10.4 GB	4.53 GB	655,360	559,513	Unknown
/var/local	svlsc	Online	96.6 GB	92.8 GB	94,369,792	94,369,445	Unknown
/var/local/rangedb/0	sdc	Online	4,396 GB	4,379 GB	858,993,408	858,983,455	Unavailable
/var/local/rangedb/1	sdd	Online	4,396 GB	4,362 GB	858,993,408	858,973,530	Unavailable
/var/local/rangedb/2	sde	Online	4,396 GB	4,370 GB	858,993,408	858,982,305	Unavailable

Pasos

- Complete los siguientes pasos para registrar los volúmenes de almacenamiento fallidos y los nombres de sus dispositivos:
 - Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
 - 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

- Seleccione **sitio > Nodo de almacenamiento fallido > SSM > Recursos > Descripción general > Principal**. Determine el punto de montaje y el tamaño del volumen de cada volumen de almacenamiento fallido 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 `sd` 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	sd	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 fallido:

- Introduzca el siguiente comando: `ssh admin@grid_node_IP`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- Introduzca el siguiente comando para cambiar a root: `su -`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

3. Ejecute el siguiente script para desmontar un volumen de almacenamiento fallido:

```
sn-unmount-volume object_store_ID
```

El `object_store_ID` es el ID del volumen de almacenamiento fallido. Por ejemplo, especifique 0 en el comando para un almacén de objetos con ID 0000.

4. Si se le solicita, presione **y** para detener el servicio Cassandra dependiendo del volumen de almacenamiento 0.



Si el servicio Cassandra ya está detenido, no se le preguntará nada. El servicio Cassandra se detiene solo para el volumen 0.

```
root@Storage-180:~/var/local/tmp/storage~ # sn-unmount-volume 0
Services depending on storage volume 0 (cassandra) aren't down.
Services depending on storage volume 0 must be stopped before running
this script.
Stop services that require storage volume 0 [y/N]? y
Shutting down services that require storage volume 0.
Services requiring storage volume 0 stopped.
Unmounting /var/local/rangedb/0
/var/local/rangedb/0 is unmounted.
```

En unos segundos, el volumen se desmontará. Aparecen mensajes indicando cada paso del proceso. El mensaje final indica que el volumen está desmontado.

5. Si el desmontaje falla porque el volumen está ocupado, puede forzar un desmontaje usando el `--use`

-umountof opción:



Forzar un desmontaje utilizando el `--use-umountof` Esta opción podría provocar que los procesos o servicios que utilizan el volumen se comporten de manera inesperada o se bloqueen.

```
root@Storage-180:~ # sn-unmount-volume --use-umountof
/var/local/rangedb/2
Unmounting /var/local/rangedb/2 using umountof
/var/local/rangedb/2 is unmounted.
Informing LDR service of changes to storage volumes
```

Recuperar volúmenes de almacenamiento fallidos y reconstruir la base de datos de Cassandra

Debe ejecutar un script que reformatee y vuelva a montar el almacenamiento en volúmenes de almacenamiento fallidos, y reconstruya la base de datos de Cassandra en el nodo de almacenamiento si el sistema determina que es necesario.

Antes de empezar

- Tú tienes el `Passwords.txt` archivo.
- Las unidades del sistema en el servidor están intactas.
- Se ha identificado la causa de la falla y, de ser necesario, ya se ha adquirido hardware de almacenamiento de reemplazo.
- El tamaño total del almacenamiento de reemplazo es el mismo que el original.
- Ha verificado que no se está realizando un desmantelamiento de un nodo de almacenamiento o ha pausado el procedimiento de desmantelamiento del nodo. (En el Administrador de red, seleccione **MANTENIMIENTO > Tareas > Desmantelamiento**.)
- Has comprobado que no hay ninguna expansión en curso. (En el Administrador de cuadrícula, seleccione **MANTENIMIENTO > Tareas > Expansión**.)
- Tienes ["revisó las advertencias sobre la recuperación del volumen de almacenamiento"](#).

Pasos

1. Según sea necesario, reemplace el almacenamiento físico o virtual fallido asociado con los volúmenes de almacenamiento fallidos que identificó y desmontó anteriormente.

No vuelva a montar los volúmenes en este paso. El almacenamiento se vuelve a montar y se agrega a `/etc/fstab` en un paso posterior.

2. En el Administrador de cuadrícula, vaya a **NODOS > appliance Storage Node > Hardware**. En la sección Dispositivo StorageGRID de la página, verifique que el modo RAID de almacenamiento esté en buen estado.
3. Inicie sesión en el nodo de almacenamiento fallido:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de \$ a # .

- 4. Utilice un editor de texto (vi o vim) para eliminar los volúmenes fallidos del `/etc/fstab` archivo y luego guarde el archivo.



Cómo comentar un volumen fallido en el `/etc/fstab` El archivo es insuficiente. El volumen debe eliminarse de `fstab` A medida que el proceso de recuperación verifica que todas las líneas en el `fstab` El archivo coincide con los sistemas de archivos montados.

- 5. Reformatee cualquier volumen de almacenamiento fallido y reconstruya la base de datos de Cassandra si es necesario. Ingresar: `reformat_storage_block_devices.rb`

- Cuando se desmonta el volumen de almacenamiento 0, aparecerán avisos y mensajes que indican que se está deteniendo el servicio Cassandra.
- Se le pedirá que reconstruya la base de datos de Cassandra si es necesario.
 - Revise las advertencias. Si ninguno de ellos aplica, reconstruya la base de datos de Cassandra. Ingresar: **y**
 - Si más de un nodo de almacenamiento está fuera de línea o si se ha reconstruido otro nodo de almacenamiento en los últimos 15 días. Ingresar: **n**

El script saldrá sin reconstruir Cassandra. Póngase en contacto con el soporte técnico.

- Para cada unidad `rangedb` en el nodo de almacenamiento, cuando se le pregunte: `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`, ingrese una de las siguientes respuestas:
 - **y** para reformatear una unidad que tenía errores. Esto reformatea el volumen de almacenamiento y agrega el volumen de almacenamiento reformateado al `/etc/fstab` archivo.
 - **n** si la unidad no contiene errores y no desea formatearla.



Al seleccionar **n** se sale del script. Monte la unidad (si cree que los datos de la unidad deben conservarse y la unidad se desmontó por error) o retire la unidad. Luego, ejecute el `reformat_storage_block_devices.rb` Comando de nuevo.



Algunos procedimientos de recuperación de StorageGRID utilizan Reaper para manejar las reparaciones de Cassandra. Las reparaciones se producen automáticamente tan pronto como se hayan iniciado los servicios relacionados o requeridos. Es posible que notes que la salida del script menciona "reaper" o "reparación de Cassandra". Si ve un mensaje de error que indica que la reparación ha fallado, ejecute el comando indicado en el mensaje de error.

En el siguiente ejemplo de salida, la unidad `/dev/sdf` debe reformatearse y no fue necesario reconstruir Cassandra:

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? y
Successfully formatted /dev/sdf with UUID b951bfcb-4804-41ad-b490-
805dfd8df16c
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12368435
Cassandra does not need rebuilding.
Starting services.
Informing storage services of new volume

Reformatting done. Now do manual steps to
restore copies of data.
```

Una vez que los volúmenes de almacenamiento se hayan reformateado y vuelto a montar y se hayan completado las operaciones necesarias de Cassandra, puede ["restaurar datos de objetos usando Grid Manager"](#) .

Restaurar datos de objetos en un volumen de almacenamiento donde la unidad del sistema está intacta

Después de recuperar un volumen de almacenamiento en un nodo de almacenamiento donde la unidad del sistema está intacta, puede restaurar los datos del objeto replicado o codificado por borrado que se perdieron cuando falló el volumen de almacenamiento.

¿Qué procedimiento debo utilizar?

Siempre que sea posible, restaure los datos de los objetos utilizando la página **Restauración de volumen** en el Administrador de cuadrícula.

- Si los volúmenes se enumeran en **MANTENIMIENTO > Restauración de volumen > Nodos a restaurar**, restaure los datos del objeto utilizando el ["Página de restauración de volumen en el Administrador de cuadrícula"](#) .
- Si los volúmenes no aparecen en **MANTENIMIENTO > Restauración de volúmenes > Nodos a restaurar**, siga los pasos a continuación para usar el `repair-data` script para restaurar datos de objetos.

Si el nodo de almacenamiento recuperado contiene menos volúmenes que el nodo que está reemplazando, debe usar el `repair-data` guion.



El script de reparación de datos está obsoleto y se eliminará en una versión futura. Cuando sea posible, utilice el ["Procedimiento de restauración de volumen en el Administrador de cuadrícula"](#) .

Utilice el `repair-data` script para restaurar datos de objetos

Antes de empezar

- Ha confirmado que el nodo de almacenamiento recuperado tiene un estado de conexión de **Conectado***  en la pestaña ***NODOS > Descripción general** en el Administrador de cuadrícula.

Acerca de esta tarea

Los datos de objetos se pueden restaurar desde otros nodos de almacenamiento o desde un grupo de almacenamiento en la nube, suponiendo que las reglas ILM de la red se configuraron de tal manera que las copias de objetos estén disponibles.

Tenga en cuenta lo siguiente:

- Si se configuró una regla ILM para almacenar solo una copia replicada y esa copia existía en un volumen de almacenamiento que falló, no podrá recuperar el objeto.
- Si la única copia restante de un objeto está en un grupo de almacenamiento en la nube, StorageGRID debe emitir varias solicitudes al punto final del grupo de almacenamiento en la nube para restaurar los datos del objeto. Antes de realizar este procedimiento, comuníquese con el soporte técnico para obtener ayuda para estimar el tiempo de recuperación y los costos asociados.

Acerca de `repair-data` guion

Para restaurar los datos del objeto, ejecute el `repair-data` guion. Este script inicia el proceso de restauración de datos de objetos y trabaja con el escaneo ILM para garantizar que se cumplan las reglas ILM.

Seleccione **Datos replicados** o **Datos codificados por borrado (EC)** a continuación para conocer las diferentes opciones para `repair-data` script, en función de si está restaurando datos replicados o datos codificados por borrado. Si necesita restaurar ambos tipos de datos, debe ejecutar ambos conjuntos de comandos.



Para obtener más información sobre el `repair-data` guión, entrar `repair-data --help` desde la línea de comandos del nodo de administración principal.



El script de reparación de datos está obsoleto y se eliminará en una versión futura. Cuando sea posible, utilice el ["Procedimiento de restauración de volumen en el Administrador de cuadrícula"](#).

Datos replicados

Hay dos comandos disponibles para restaurar datos replicados, según si necesita reparar todo el nodo 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 datos replicados con este comando:

```
repair-data show-replicated-repair-status
```

Datos codificados por borrado (EC)

Hay dos comandos disponibles para restaurar datos codificados por borrado, según si necesita reparar todo el nodo o solo ciertos volúmenes del nodo:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Puede realizar un seguimiento de las reparaciones de datos codificados por borrado con este comando:

```
repair-data show-ec-repair-status
```



Las reparaciones de datos codificados por borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. Sin embargo, si no se pueden contabilizar todos los datos codificados por borrado, no se podrá completar la reparación. La reparación se completará después de que todos los nodos estén disponibles.



El trabajo de reparación de EC reserva temporalmente una gran cantidad de almacenamiento. Es posible que se activen alertas de almacenamiento, pero se resolverán cuando se complete la reparación. Si no hay suficiente almacenamiento para la reserva, el trabajo de reparación de EC fallará. Las reservas de almacenamiento se liberan cuando se completa el trabajo de reparación de EC, independientemente de si el trabajo falló o tuvo éxito.

Buscar el nombre de host para el 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 el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Utilice el `/etc/hosts` archivo para encontrar el nombre de host del nodo de almacenamiento para los volúmenes de almacenamiento restaurados. Para ver una lista de todos los nodos en la cuadrícula,

ingrese lo siguiente: `cat /etc/hosts`.

Reparar datos si todos los volúmenes han fallado

Si todos los volúmenes de almacenamiento han fallado, repare todo el nodo. Siga las instrucciones para **datos replicados**, **datos codificados por borrado (EC)** o ambos, según utilice datos replicados, datos codificados por borrado (EC) o ambos.

Si sólo han fallado algunos volúmenes, vaya a [Reparar datos si solo han fallado algunos volúmenes](#).



No puedes correr `repair-data` operaciones para más de un nodo al mismo tiempo. Para recuperar varios nodos, comuníquese con el soporte técnico.

Datos replicados

Si su cuadrícula incluye datos replicados, utilice el `repair-data start-replicated-node-repair` comando con el `--nodes` opción, donde `--nodes` es el nombre de host (nombre del sistema), para reparar todo el nodo de almacenamiento.

Este comando repara los datos replicados en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



A medida que se restauran los datos de los objetos, se activa la alerta **Objetos perdidos** si el sistema StorageGRID no puede localizar los datos de los objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Debe determinar la causa de la pérdida y si es posible recuperarla. Ver "[Investigar objetos perdidos](#)".

Datos codificados por borrado (EC)

Si su cuadrícula contiene datos codificados por borrado, utilice el `repair-data start-ec-node-repair` comando con el `--nodes` opción, donde `--nodes` es el nombre de host (nombre del sistema), para reparar todo el nodo de almacenamiento.

Este comando repara los datos codificados por borrado en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

La operación devuelve un valor único `repair ID` que identifica esta `repair_data` operación. Utilice este `repair ID` Para seguir el progreso y el resultado de la `repair_data` operación. No se devuelve ningún otro comentario mientras se completa el proceso de recuperación.

Las reparaciones de datos codificados por borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. La reparación se completará después de que todos los nodos estén disponibles.

Reparar datos si solo han fallado algunos volúmenes

Si sólo han fallado algunos de los volúmenes, repare los volúmenes afectados. Siga las instrucciones para **datos replicados**, **datos codificados por borrado (EC)** o ambos, según utilice datos replicados, datos codificados por borrado (EC) o ambos.

Si todos los volúmenes han fallado, vaya a [Reparar datos si todos los volúmenes han fallado](#) .

Introduzca los ID de volumen en hexadecimal. Por ejemplo, 0000 es el primer volumen y 000F Es el decimosexto volumen. Puede especificar un volumen, un rango de volúmenes o varios volúmenes que no estén en una secuencia.

Todos los volúmenes deben estar en el mismo nodo de almacenamiento. Si necesita restaurar volúmenes para más de un nodo de almacenamiento, comuníquese con el soporte técnico.

Datos replicados

Si su cuadrícula contiene datos replicados, utilice el `start-replicated-volume-repair` comando con el `--nodes` opción para identificar el nodo (donde `--nodes` es el nombre de host del nodo). Luego agregue el `--volumes` o `--volume-range` opción, como se muestra en los siguientes ejemplos.

Volumen único: este comando restaura los datos replicados al volumen 0002 en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Rango de volúmenes: este comando restaura los datos replicados en todos los volúmenes del rango 0003 a 0009 en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Varios volúmenes no en una secuencia: este comando restaura datos replicados a los volúmenes 0001 , 0005 , y 0008 en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



A medida que se restauran los datos de los objetos, se activa la alerta **Objetos perdidos** si el sistema StorageGRID no puede localizar los datos de los objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Tenga en cuenta la descripción de la alerta y las acciones recomendadas para determinar la causa de la pérdida y si es posible la recuperación.

Datos codificados por borrado (EC)

Si su cuadrícula contiene datos codificados por borrado, utilice el `start-ec-volume-repair` comando con el `--nodes` opción para identificar el nodo (donde `--nodes` es el nombre de host del nodo). Luego agregue el `--volumes` o `--volume-range` opción, 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 llamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Rango de volúmenes: este comando restaura datos codificados por borrado en todos los volúmenes del rango 0004 a 0006 en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Varios volúmenes no en una secuencia: este comando restaura datos codificados por borrado en los volúmenes 000A , 000C , y 000E en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

El `repair-data` La operación devuelve un valor único. `repair ID` que identifica esto `repair_data` operación. Utilice esto `repair ID` Para seguir el progreso y el resultado de la `repair_data` operación. No se devuelve ningún otro comentario mientras se completa el proceso de recuperación.



Las reparaciones de datos codificados por borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. La reparación se completará después de que todos los nodos estén disponibles.

Reparación de monitores

Supervise el estado de los trabajos de reparación, dependiendo de si utiliza **datos replicados**, **datos codificados por borrado (EC)** o ambos.

También puede supervisar el estado de los trabajos de restauración de volumen en proceso y ver un historial de trabajos de restauración completados en "[Administrador de red](#)".

Datos replicados

- Para obtener un porcentaje estimado de finalización de la reparación replicada, agregue el `show-replicated-repair-status` Opción para el comando `reparar-datos`.

```
repair-data show-replicated-repair-status
```

- Para determinar si las reparaciones están completas:
 - a. Seleccione **NODOS > Nodo de almacenamiento en reparación > ILM**.
 - b. Revise los atributos en la sección Evaluación. Cuando se completan las reparaciones, el atributo **En espera - Todo** indica 0 objetos.
- Para supervisar la reparación con más detalle:
 - a. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
 - b. Seleccione **grid > Nodo de almacenamiento en reparación > LDR > Almacén de datos**.
 - c. Utilice una combinación de los siguientes atributos para determinar, lo mejor posible, si las reparaciones replicadas están completas.



Pueden existir inconsistencias en Cassandra y no se realiza un seguimiento de las reparaciones fallidas.

- **Reparaciones intentadas (XRPA)**: utilice este atributo para rastrear el 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 escaneo actual (proporcionado por el atributo **Período de escaneo – Estimado**), significa que el escaneo ILM no encontró objetos de alto riesgo que necesiten reparación en ningún nodo.



Los objetos de alto riesgo son objetos que corren el riesgo de perderse por completo. Esto no incluye objetos que no satisfacen su configuración ILM.

- **Período de escaneo estimado (XSCM)**: utilice este atributo para estimar cuándo se aplicará un cambio de política a los objetos ingeridos previamente. Si el atributo **Reparaciones intentadas** no aumenta durante un período más largo que el período de escaneo actual, es probable que se realicen reparaciones replicadas. Tenga en cuenta que el período de escaneo puede cambiar. El atributo **Período de escaneo estimado (XSCM)** se aplica a toda la cuadrícula y es el máximo de todos los períodos de escaneo de nodos. Puede consultar el historial de atributos **Período de escaneo – Estimado** de la cuadrícula para determinar un período de tiempo apropiado.

Datos codificados por borrado (EC)

Para supervisar la reparación de datos codificados por borrado y volver a intentar cualquier solicitud que pueda haber fallado:

1. Determinar el estado de las reparaciones de datos codificados por borrado:
 - Seleccione **SOPORTE > Herramientas > Métricas** para ver el tiempo estimado de finalización y el porcentaje de finalización del trabajo actual. Luego, seleccione **Descripción general de EC** en la sección Grafana. Consulte los paneles **Tiempo estimado de finalización del trabajo de Grid EC** 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
```

La salida enumera información, incluyendo `repair ID`, para todas las reparaciones realizadas anteriormente y actualmente en curso.

2. Si la salida muestra que la operación de reparación falló, utilice el `--repair-id` Opción para reintentar la reparación.

Este comando vuelve a intentar una reparación de nodo fallida, utilizando el ID de reparación 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando vuelve a intentar una reparación de volumen fallida, utilizando el ID de reparación 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Comprobar el estado del almacenamiento después de recuperar volúmenes de almacenamiento

Después de recuperar los volúmenes de almacenamiento, debe verificar que el estado deseado del nodo de almacenamiento esté configurado en línea y asegurarse de que el estado estará en línea de manera predeterminada cada vez que se reinicie el servidor del nodo de almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Se ha recuperado el nodo de almacenamiento y se ha completado la recuperación de datos.

Pasos

1. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
2. Verifique los valores de **Nodo de almacenamiento recuperado > LDR > Almacenamiento > Estado de almacenamiento - deseado** y **Estado de almacenamiento - actual**.

El valor de ambos atributos debe ser En línea.

3. Si el Estado de almacenamiento - Deseado está configurado en Solo lectura, complete los siguientes pasos:
 - a. Haga clic en la pestaña **Configuración**.
 - b. En la lista desplegable **Estado de almacenamiento – Deseado**, seleccione **En línea**.
 - c. Haga clic en **Aplicar cambios**.
 - d. Haga clic en la pestaña **Descripción general** y confirme que los valores de **Estado de almacenamiento - Deseado** y **Estado de almacenamiento - Actual** estén actualizados a En línea.

Recuperarse de una falla de la unidad del sistema

Advertencias para la recuperación de la unidad del sistema del nodo de almacenamiento

Antes de recuperar una unidad de sistema defectuosa de un nodo de almacenamiento, revise las instrucciones generales. ["Advertencias y consideraciones para la recuperación del nodo de la red"](#) y las siguientes advertencias específicas.

Los nodos de almacenamiento tienen una base de datos Cassandra que incluye metadatos de objetos. La base de datos de Cassandra podría reconstruirse en las siguientes circunstancias:

- Un nodo de almacenamiento vuelve a estar en línea después de haber estado fuera de línea durante más de 15 días.
- Se ha producido un error en un volumen de almacenamiento y se ha recuperado.
- 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 fuera de línea, es posible que algunos datos de Cassandra no estén disponibles. Si Cassandra se ha reconstruido recientemente, es posible que sus datos aún no sean consistentes en toda la red. Puede ocurrir pérdida de datos si se reconstruye Cassandra cuando demasiados nodos de almacenamiento están fuera de línea o si dos o más nodos de almacenamiento se reconstruyen con una diferencia de 15 días entre sí.



Si más de un nodo de almacenamiento ha fallado (o está fuera de línea), comuníquese con el soporte técnico. No realice el siguiente procedimiento de recuperación. Podría ocurrir pérdida de datos.



Si esta es la segunda falla del nodo de almacenamiento en menos de 15 días después de una falla o recuperación del nodo de almacenamiento, comuníquese con el soporte técnico. Reconstruir Cassandra en dos o más nodos de almacenamiento dentro de 15 días puede provocar la pérdida de datos.



Si ha fallado más de un nodo de almacenamiento en un sitio, es posible que se requiera un procedimiento de recuperación del sitio. Ver ["Cómo el soporte técnico recupera un sitio"](#).



Si este nodo de almacenamiento está en modo de mantenimiento de solo lectura para permitir la recuperación de objetos por parte de otro nodo de almacenamiento con volúmenes de almacenamiento fallidos, recupere los volúmenes en el nodo de almacenamiento con volúmenes de almacenamiento fallidos antes de recuperar este nodo de almacenamiento fallido. Vea las instrucciones para ["Recuperarse de una falla del volumen de almacenamiento donde la unidad del sistema está intacta"](#).



Si las reglas de ILM están configuradas para almacenar solo una copia replicada y la copia existe en un volumen de almacenamiento que ha fallado, no podrá recuperar el objeto.

Reemplazar el nodo de almacenamiento

Si la unidad del sistema ha fallado, primero debe reemplazar el nodo de almacenamiento.

Debe seleccionar el procedimiento de reemplazo de nodo para su plataforma. Los pasos para reemplazar un nodo son los mismos para todos los tipos de nodos de la red.



Este procedimiento se aplica únicamente a los nodos de almacenamiento basados en software. Debes seguir un procedimiento diferente para ["recuperar un nodo de almacenamiento del dispositivo"](#).

Linux: Si no está seguro de si la unidad de su sistema ha fallado, siga las instrucciones para reemplazar el nodo para determinar qué pasos de recuperación son necesarios.

Plataforma	Procedimiento
VMware	"Reemplazar un nodo de VMware"
Linux	"Reemplazar un nodo Linux"
OpenStack	Los archivos de disco de máquina virtual y los scripts proporcionados por NetApp para OpenStack ya no son compatibles con las operaciones de recuperación. Si necesita recuperar un nodo que se ejecuta en una implementación de OpenStack, descargue los archivos para su sistema operativo Linux. A continuación, siga el procedimiento para "Reemplazar un nodo Linux" .

Seleccione Iniciar recuperación para configurar el nodo de almacenamiento

Después de reemplazar un nodo de almacenamiento, debe seleccionar Iniciar recuperación en el Administrador de red para configurar el nuevo nodo como reemplazo del nodo fallido.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de mantenimiento o acceso root"](#).
- Tienes la contraseña de aprovisionamiento.
- Ha implementado y configurado el nodo de reemplazo.
- Tienes la fecha de inicio de cualquier trabajo de reparación de datos codificados por borrado.
- Ha verificado que el nodo de almacenamiento no se ha reconstruido en los últimos 15 días.

Acerca de esta tarea

Si el nodo de almacenamiento está instalado como un contenedor en un host Linux, debe realizar este paso solo si se cumple una de estas condiciones:

- Tuviste que usar el `--force` bandera para importar el nodo, o usted emitió `storagegrid node force-recovery node-name`
- Tenías que hacer una reinstalación completa del nodo o restaurar `/var/local`.

Pasos

1. Desde el Administrador de red, seleccione **MANTENIMIENTO > Tareas > Recuperación**.

2. Seleccione el nodo de la cuadrícula que desea recuperar en la lista de Nodos pendientes.

Los nodos aparecen en la lista después de fallar, pero no puedes seleccionar un nodo hasta que se haya reinstalado y esté listo para la recuperación.

3. Introduzca la **contraseña de aprovisionamiento**.
4. Haga clic en **Iniciar recuperación**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	✓

Passphrase

Provisioning Passphrase

.....

Start Recovery

5. Supervise el progreso de la recuperación en la tabla Nodo de cuadrícula en recuperación.



Mientras se ejecuta el procedimiento de recuperación, puede hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparece un cuadro de diálogo que indica que el nodo quedará en un estado indeterminado si restablece el procedimiento.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Si desea volver a intentar la recuperación después de restablecer el procedimiento, debe restaurar el nodo a un estado preinstalado, de la siguiente manera:

- **VMware:** eliminar el nodo de red virtual implementado. Luego, cuando esté listo para reiniciar la recuperación, vuelva a implementar el nodo.
- **Linux:** reinicie el nodo ejecutando este comando en el host Linux: `storagegrid node force-recovery node-name`

6. Cuando el nodo de almacenamiento llega a la etapa "Esperando pasos manuales", vaya a ["Volver a montar y reformatear volúmenes de almacenamiento \(pasos manuales\)"](#) .

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Recovering Grid Node

Name	Start Time	Progress	Stage
dc2-s3	2016-09-12 16:12:40 PDT		Waiting For Manual Steps

Reset

Volver a montar y reformatear volúmenes de almacenamiento (pasos manuales)

Debe ejecutar manualmente dos scripts para volver a montar los volúmenes de almacenamiento preservados y reformatear cualquier volumen de almacenamiento fallido. El primer script vuelve a montar los volúmenes que están formateados correctamente como volúmenes de almacenamiento StorageGRID . El segundo script reformatea cualquier volumen no montado, reconstruye Cassandra, si es necesario, e inicia los servicios.

Antes de empezar

- Ya ha reemplazado el hardware de todos los volúmenes de almacenamiento fallidos que sabe que requieren reemplazo.

Ejecutando el `sn-remount-volumes` El script podría ayudarle a identificar volúmenes de almacenamiento fallidos adicionales.

- Ha verificado que no se está realizando un desmantelamiento de un nodo de almacenamiento o ha pausado el procedimiento de desmantelamiento del nodo. (En el Administrador de red, seleccione **MANTENIMIENTO > Tareas > Desmantelamiento.**)
- Has comprobado que no hay ninguna expansión en curso. (En el Administrador de cuadrícula, seleccione **MANTENIMIENTO > Tareas > Expansión.**)
- Tienes ["Revisó las advertencias para la recuperación de la unidad del sistema del nodo de almacenamiento"](#) .



Comuníquese con el soporte técnico si más de un nodo de almacenamiento está fuera de línea o si un nodo de almacenamiento en esta red se ha reconstruido en los últimos 15 días. No corras el `sn-recovery-postinstall.sh` guion. La reconstrucción de Cassandra en dos o más nodos de almacenamiento con una diferencia de 15 días entre sí podría provocar la 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.
- Ejecutar el `sn-remount-volumes` script para volver a montar volúmenes de almacenamiento formateados correctamente. Cuando se ejecuta este script, hace 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 consistente, determina si el volumen de almacenamiento es un volumen de almacenamiento StorageGRID con el formato correcto.
 - Si el volumen de almacenamiento está formateado correctamente, vuelve a montar el volumen de almacenamiento. Todos los datos existentes en el volumen permanecen intactos.
- Revise la salida del script y resuelva cualquier problema.
- Ejecutar el `sn-recovery-postinstall.sh` guion. Cuando este script se ejecuta, hace lo siguiente.



No reinicie un nodo de almacenamiento durante la recuperación antes de ejecutarlo `sn-recovery-postinstall.sh` para reformatear los volúmenes de almacenamiento fallidos y restaurar los metadatos de los objetos. Reiniciar el nodo de almacenamiento antes `sn-recovery-postinstall.sh` Completa las causas de errores en los servicios que intentan iniciarse y provoca que los nodos del dispositivo StorageGRID salgan del modo de mantenimiento. Vea el paso para [script posterior a la instalación](#).

- Reformatea cualquier volumen de almacenamiento que `sn-remount-volumes` No se pudo montar el script o se encontró que estaba formateado incorrectamente.



Si se reformatea un volumen de almacenamiento, se perderán todos los datos de ese volumen. Debe realizar un procedimiento adicional para restaurar datos de objetos desde otras ubicaciones en la cuadrícula, asumiendo que las reglas ILM se configuraron para almacenar más de una copia de objeto.

- Reconstruye la base de datos de 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 el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Ejecute el primer script para volver a montar cualquier volumen de almacenamiento formateado correctamente.



Si todos los volúmenes de almacenamiento son nuevos y necesitan formatearse, o si todos los volúmenes de almacenamiento han fallado, puede omitir este paso y ejecutar el segundo script para reformatear todos los volúmenes de almacenamiento sin montar.

a. Ejecute el script: `sn-remount-volumes`

Este script puede tardar horas en ejecutarse en volúmenes de almacenamiento que contienen datos.

b. Mientras se ejecuta el script, revise el resultado y responda las indicaciones.



Según sea necesario, puede utilizar el `tail -f` Comando para monitorear el contenido del archivo de registro del script(`/var/local/log/sn-remount-volumes.log`). El archivo de registro contiene información más detallada que la salida 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 will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
```

```

have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

===== Device /dev/sdd =====
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

===== Device /dev/sde =====
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file

```

Error: This volume does not belong to this node. Fix the attached volume and re-run this script.

En el ejemplo de salida, un volumen de almacenamiento se volvió a montar correctamente y tres volúmenes de almacenamiento tuvieron errores.

- `/dev/sdb` Pasó la verificación de consistencia del sistema de archivos XFS y tenía una estructura de volumen válida, por lo que se volvió a montar correctamente. Se conservan los datos de los dispositivos que se vuelven a montar mediante el script.
- `/dev/sdc` No se pudo pasar 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 se inicializó o el superbloque del disco estaba dañado. Cuando el script no puede montar un volumen de almacenamiento, le pregunta si desea ejecutar la verificación de consistencia del sistema de archivos.
 - Si el volumen de almacenamiento está conectado a un nuevo disco, responda **N** a la pregunta. No es necesario comprobar el sistema de archivos en un disco nuevo.
 - Si el volumen de almacenamiento está conectado a un disco existente, responda **Y** a la pregunta. Puede utilizar los resultados de la comprobación del sistema de archivos para determinar el origen de la corrupción. Los resultados se guardan en el `/var/local/log/sn-remount-volumes.log` archivo de registro.
- `/dev/sde` pasó la verificación de consistencia del sistema de archivos XFS y tenía una estructura de volumen válida; sin embargo, el ID del nodo LDR en el archivo `volID` no coincidía 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 la salida del script y resuelva cualquier problema.



Si un volumen de almacenamiento no pasó la verificación de consistencia del sistema de archivos XFS o no se pudo montar, revise cuidadosamente los mensajes de error en la salida. Debes comprender las implicaciones de ejecutar el `sn-recovery-postinstall.sh` guión en estos volúmenes.

- a. Verifique que los resultados incluyan una entrada para todos los volúmenes esperados. Si no aparece algún volumen, 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, la salida 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 se informa que un volumen de almacenamiento pertenece a otro nodo de almacenamiento, comuníquese con el soporte técnico. Si ejecuta el `sn-recovery-postinstall.sh` script, el volumen de almacenamiento se formateará, lo que podría provocar pérdida de datos.

- c. Si no se pudo montar algún dispositivo de almacenamiento, anote el nombre del dispositivo y repárelo o reemplácelo.



Debe reparar o reemplazar cualquier dispositivo de almacenamiento que no se haya podido montar.

Utilizará el nombre del dispositivo para buscar el ID del volumen, que es una entrada obligatoria cuando ejecuta el `repair-data` script para restaurar datos de objetos al volumen (el siguiente procedimiento).

- d. Después de reparar o reemplazar todos los dispositivos que no se pueden montar, ejecute el `sn-remount-volumes` Ejecute el script nuevamente para confirmar que se hayan vuelto a montar todos los volúmenes de almacenamiento que se pueden volver a montar.



Si un volumen de almacenamiento no se puede montar o está formateado incorrectamente y continúa con el siguiente paso, se eliminarán el volumen y todos los datos que contenga. Si tenía dos copias de datos de objetos, solo tendrá una copia hasta que complete el siguiente procedimiento (restauración de datos de objetos).



No corras el `sn-recovery-postinstall.sh` script si cree que los datos restantes en un volumen de almacenamiento fallido no se pueden reconstruir desde otro lugar en la red (por ejemplo, si su política ILM usa una regla que solo hace una copia o si los volúmenes han fallado en varios nodos). En su lugar, comuníquese con el soporte técnico para determinar cómo recuperar sus datos.

4. Ejecutar el `sn-recovery-postinstall.sh` guion: `sn-recovery-postinstall.sh`

Este script reformatea cualquier volumen de almacenamiento que no se pudo montar o que se encontró que estaba formateado incorrectamente; reconstruye la base de datos Cassandra en el nodo, si es necesario; e inicia los servicios en el nodo de almacenamiento.

Tenga en cuenta lo siguiente:

- El script podría tardar horas en ejecutarse.
- En general, debes dejar la sesión SSH en paz mientras se ejecuta el script.
- No presione **Ctrl+C** mientras la sesión SSH esté activa.
- El script se ejecutará en segundo plano si ocurre una interrupción en la red y finaliza la sesión SSH, pero puede ver el progreso desde la página de Recuperación.
- Si el nodo de almacenamiento utiliza el servicio RSM, es posible que el script parezca detenerse durante 5 minutos mientras se reinician los servicios del nodo. Se espera este retraso de 5 minutos cada vez que el servicio RSM se inicia por primera vez.



El servicio RSM está presente en los nodos de almacenamiento que incluyen el servicio ADC.



Algunos procedimientos de recuperación de StorageGRID utilizan Reaper para manejar las reparaciones de Cassandra. Las reparaciones se producen automáticamente tan pronto como se hayan iniciado los servicios relacionados o requeridos. Es posible que notes que la salida del script menciona "reaper" o "reparación de Cassandra". Si ve un mensaje de error que indica que la reparación ha fallado, ejecute el comando indicado en el mensaje de error.

5. [\[\[paso del script posterior a la instalación\]\]](#) Como el `sn-recovery-postinstall.sh` El script se ejecuta y supervisa la página de Recuperación en el Administrador de Grid.

La barra de progreso y la columna Etapa en la página Recuperación proporcionan un estado de alto nivel del `sn-recovery-postinstall.sh` guion.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
Name	IPv4 Address	State	Recoverable	
No results found.				

Recovering Grid Node

Name	Start Time	Progress	Stage
DC1-S3	2016-06-02 14:03:35 PDT		Recovering Cassandra

6. Después de la `sn-recovery-postinstall.sh` Una vez que el script haya iniciado servicios en el nodo, puede restaurar los datos del objeto en cualquier volumen de almacenamiento que haya sido formateado por el script.

El script le pregunta si desea utilizar el proceso de restauración de volumen de Grid Manager.

- En la mayoría de los casos, deberías ["restaurar datos de objetos usando Grid Manager"](#) . Respuesta `y` para utilizar el Administrador de cuadrícula.
- En casos excepcionales, como cuando se lo solicita el soporte técnico o cuando sabe que el nodo de reemplazo tiene menos volúmenes disponibles para el almacenamiento de objetos que el nodo original, debe ["restaurar datos de objetos manualmente"](#) utilizando el `repair-data` guion. Si se aplica uno de estos casos, responda `n` .



Si respondes `n` para utilizar el proceso de restauración de volumen de Grid Manager (restaurar datos de objetos manualmente):

- No es posible restaurar datos de objetos mediante Grid Manager.
- Puede supervisar el progreso de los trabajos de restauración manual utilizando Grid Manager.

Después de realizar la selección, el script se completa y se muestran los siguientes pasos para recuperar los datos del objeto. Después de revisar estos pasos, presione cualquier tecla para regresar a la línea de comando.

Restaurar datos de objetos al volumen de almacenamiento (fallo de la unidad del sistema)

Después de recuperar volúmenes de almacenamiento para un nodo de almacenamiento que no es un dispositivo, puede restaurar los datos de objetos replicados o codificados por borrado que se perdieron cuando falló el nodo de almacenamiento.

¿Qué procedimiento debo utilizar?

Siempre que sea posible, restaure los datos de los objetos utilizando la página **Restauración de volumen** en el Administrador de cuadrícula.

- Si los volúmenes se enumeran en **MANTENIMIENTO > Restauración de volumen > Nodos a restaurar**, restaure los datos del objeto utilizando el "[Página de restauración de volumen en el Administrador de cuadrícula](#)".
- Si los volúmenes no aparecen en **MANTENIMIENTO > Restauración de volúmenes > Nodos a restaurar**, siga los pasos a continuación para usar el `repair-data` script para restaurar datos de objetos.

Si el nodo de almacenamiento recuperado contiene menos volúmenes que el nodo que está reemplazando, debe usar el `repair-data` guion.



El script de reparación de datos está obsoleto y se eliminará en una versión futura. Cuando sea posible, utilice el "[Procedimiento de restauración de volumen en el Administrador de cuadrícula](#)".

Utilice el `repair-data` script para restaurar datos de objetos

Antes de empezar

- Ha confirmado que el nodo de almacenamiento recuperado tiene un estado de conexión de **Conectado***  en la pestaña ***NODOS > Descripción general** en el Administrador de cuadrícula.

Acerca de esta tarea

Los datos de objetos se pueden restaurar desde otros nodos de almacenamiento o desde un grupo de almacenamiento en la nube, suponiendo que las reglas ILM de la red se configuraron de tal manera que las copias de objetos estén disponibles.

Tenga en cuenta lo siguiente:

- Si se configuró una regla ILM para almacenar solo una copia replicada y esa copia existía en un volumen de almacenamiento que falló, no podrá recuperar el objeto.
- Si la única copia restante de un objeto está en un grupo de almacenamiento en la nube, StorageGRID debe emitir varias solicitudes al punto final del grupo de almacenamiento en la nube para restaurar los datos del objeto. Antes de realizar este procedimiento, comuníquese con el soporte técnico para obtener ayuda para estimar el tiempo de recuperación y los costos asociados.

Acerca de `repair-data` guion

Para restaurar los datos del objeto, ejecute el `repair-data` guion. Este script inicia el proceso de restauración de datos de objetos y trabaja con el escaneo ILM para garantizar que se cumplan las reglas ILM.

Seleccione **Datos replicados** o **Datos codificados por borrado (EC)** a continuación para conocer las diferentes opciones para `repair-data` script, en función de si está restaurando datos replicados o datos codificados por borrado. Si necesita restaurar ambos tipos de datos, debe ejecutar ambos conjuntos de comandos.



Para obtener más información sobre el `repair-data` guión, entrar `repair-data --help` desde la línea de comandos del nodo de administración principal.



El script de reparación de datos está obsoleto y se eliminará en una versión futura. Cuando sea posible, utilice el ["Procedimiento de restauración de volumen en el Administrador de cuadrícula"](#).

Datos replicados

Hay dos comandos disponibles para restaurar datos replicados, según si necesita reparar todo el nodo 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 datos replicados con este comando:

```
repair-data show-replicated-repair-status
```

Datos codificados por borrado (EC)

Hay dos comandos disponibles para restaurar datos codificados por borrado, según si necesita reparar todo el nodo o solo ciertos volúmenes del nodo:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Puede realizar un seguimiento de las reparaciones de datos codificados por borrado con este comando:

```
repair-data show-ec-repair-status
```



Las reparaciones de datos codificados por borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. Sin embargo, si no se pueden contabilizar todos los datos codificados por borrado, no se podrá completar la reparación. La reparación se completará después de que todos los nodos estén disponibles.



El trabajo de reparación de EC reserva temporalmente una gran cantidad de almacenamiento. Es posible que se activen alertas de almacenamiento, pero se resolverán cuando se complete la reparación. Si no hay suficiente almacenamiento para la reserva, el trabajo de reparación de EC fallará. Las reservas de almacenamiento se liberan cuando se completa el trabajo de reparación de EC, independientemente de si el trabajo falló o tuvo éxito.

Buscar el nombre de host para el nodo de almacenamiento

1. Inicie sesión en el nodo de administración principal:

- Introduzca el siguiente comando: `ssh admin@primary_Admin_Node_IP`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- Introduzca el siguiente comando para cambiar a root: `su -`
- Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de \$ a # .

2. Utilice el `/etc/hosts` archivo para encontrar el nombre de host del nodo de almacenamiento para los volúmenes de almacenamiento restaurados. Para ver una lista de todos los nodos en la cuadrícula, ingrese lo siguiente: `cat /etc/hosts` .

Reparar datos si todos los volúmenes han fallado

Si todos los volúmenes de almacenamiento han fallado, repare todo el nodo. Siga las instrucciones para **datos replicados**, **datos codificados por borrado (EC)** o ambos, según utilice datos replicados, datos codificados por borrado (EC) o ambos.

Si sólo han fallado algunos volúmenes, vaya a [Reparar datos si solo han fallado algunos volúmenes](#) .



No puedes correr `repair-data` operaciones para más de un nodo al mismo tiempo. Para recuperar varios nodos, comuníquese con el soporte técnico.

Datos replicados

Si su cuadrícula incluye datos replicados, utilice el `repair-data start-replicated-node-repair` comando con el `--nodes` opción, donde `--nodes` es el nombre de host (nombre del sistema), para reparar todo el nodo de almacenamiento.

Este comando repara los datos replicados en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



A medida que se restauran los datos de los objetos, se activa la alerta **Objetos perdidos** si el sistema StorageGRID no puede localizar los datos de los objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Debe determinar la causa de la pérdida y si es posible recuperarla. Ver "[Investigar objetos perdidos](#)".

Datos codificados por borrado (EC)

Si su cuadrícula contiene datos codificados por borrado, utilice el `repair-data start-ec-node-repair` comando con el `--nodes` opción, donde `--nodes` es el nombre de host (nombre del sistema), para reparar todo el nodo de almacenamiento.

Este comando repara los datos codificados por borrado en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

La operación devuelve un valor único `repair ID` que identifica esta `repair_data` operación. Utilice este `repair ID` Para seguir el progreso y el resultado de la `repair_data` operación. No se devuelve ningún otro comentario mientras se completa el proceso de recuperación.

Las reparaciones de datos codificados por borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. La reparación se completará después de que todos los nodos estén disponibles.

Reparar datos si solo han fallado algunos volúmenes

Si sólo han fallado algunos de los volúmenes, repare los volúmenes afectados. Siga las instrucciones para **datos replicados**, **datos codificados por borrado (EC)** o ambos, según utilice datos replicados, datos codificados por borrado (EC) o ambos.

Si todos los volúmenes han fallado, vaya a [Reparar datos si todos los volúmenes han fallado](#) .

Introduzca los ID de volumen en hexadecimal. Por ejemplo, 0000 es el primer volumen y 000F Es el decimosexto volumen. Puede especificar un volumen, un rango de volúmenes o varios volúmenes que no estén en una secuencia.

Todos los volúmenes deben estar en el mismo nodo de almacenamiento. Si necesita restaurar volúmenes para más de un nodo de almacenamiento, comuníquese con el soporte técnico.

Datos replicados

Si su cuadrícula contiene datos replicados, utilice el `start-replicated-volume-repair` comando con el `--nodes` opción para identificar el nodo (donde `--nodes` es el nombre de host del nodo). Luego agregue el `--volumes` o `--volume-range` opción, como se muestra en los siguientes ejemplos.

Volumen único: este comando restaura los datos replicados al volumen 0002 en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Rango de volúmenes: este comando restaura los datos replicados en todos los volúmenes del rango 0003 a 0009 en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Varios volúmenes no en una secuencia: este comando restaura datos replicados a los volúmenes 0001 , 0005 , y 0008 en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0001,0005,0008
```



A medida que se restauran los datos de los objetos, se activa la alerta **Objetos perdidos** si el sistema StorageGRID no puede localizar los datos de los objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Tenga en cuenta la descripción de la alerta y las acciones recomendadas para determinar la causa de la pérdida y si es posible la recuperación.

Datos codificados por borrado (EC)

Si su cuadrícula contiene datos codificados por borrado, utilice el `start-ec-volume-repair` comando con el `--nodes` opción para identificar el nodo (donde `--nodes` es el nombre de host del nodo). Luego agregue el `--volumes` o `--volume-range` opción, 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 llamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Rango de volúmenes: este comando restaura datos codificados por borrado en todos los volúmenes del rango 0004 a 0006 en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Varios volúmenes no en una secuencia: este comando restaura datos codificados por borrado en los volúmenes 000A , 000C , y 000E en un nodo de almacenamiento llamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

El `repair-data` La operación devuelve un valor único. `repair ID` que identifica esto `repair_data` operación. Utilice esto `repair ID` Para seguir el progreso y el resultado de la `repair_data` operación. No se devuelve ningún otro comentario mientras se completa el proceso de recuperación.



Las reparaciones de datos codificados por borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. La reparación se completará después de que todos los nodos estén disponibles.

Reparación de monitores

Supervise el estado de los trabajos de reparación, dependiendo de si utiliza **datos replicados**, **datos codificados por borrado (EC)** o ambos.

También puede supervisar el estado de los trabajos de restauración de volumen en proceso y ver un historial de trabajos de restauración completados en "[Administrador de red](#)".

Datos replicados

- Para obtener un porcentaje estimado de finalización de la reparación replicada, agregue el `show-replicated-repair-status` Opción para el comando `reparar-datos`.

```
repair-data show-replicated-repair-status
```

- Para determinar si las reparaciones están completas:
 - a. Seleccione **NODOS > Nodo de almacenamiento en reparación > ILM**.
 - b. Revise los atributos en la sección Evaluación. Cuando se completan las reparaciones, el atributo **En espera - Todo** indica 0 objetos.
- Para supervisar la reparación con más detalle:
 - a. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
 - b. Seleccione **grid > Nodo de almacenamiento en reparación > LDR > Almacén de datos**.
 - c. Utilice una combinación de los siguientes atributos para determinar, lo mejor posible, si las reparaciones replicadas están completas.



Pueden existir inconsistencias en Cassandra y no se realiza un seguimiento de las reparaciones fallidas.

- **Reparaciones intentadas (XRPA)**: utilice este atributo para rastrear el 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 escaneo actual (proporcionado por el atributo **Período de escaneo – Estimado**), significa que el escaneo ILM no encontró objetos de alto riesgo que necesiten reparación en ningún nodo.



Los objetos de alto riesgo son objetos que corren el riesgo de perderse por completo. Esto no incluye objetos que no satisfacen su configuración ILM.

- **Período de escaneo estimado (XSCM)**: utilice este atributo para estimar cuándo se aplicará un cambio de política a los objetos ingeridos previamente. Si el atributo **Reparaciones intentadas** no aumenta durante un período más largo que el período de escaneo actual, es probable que se realicen reparaciones replicadas. Tenga en cuenta que el período de escaneo puede cambiar. El atributo **Período de escaneo estimado (XSCM)** se aplica a toda la cuadrícula y es el máximo de todos los períodos de escaneo de nodos. Puede consultar el historial de atributos **Período de escaneo – Estimado** de la cuadrícula para determinar un período de tiempo apropiado.

Datos codificados por borrado (EC)

Para supervisar la reparación de datos codificados por borrado y volver a intentar cualquier solicitud que pueda haber fallado:

1. Determinar el estado de las reparaciones de datos codificados por borrado:
 - Seleccione **SOPORTE > Herramientas > Métricas** para ver el tiempo estimado de finalización y el porcentaje de finalización del trabajo actual. Luego, seleccione **Descripción general de EC** en la sección Grafana. Consulte los paneles **Tiempo estimado de finalización del trabajo de Grid EC** 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
```

La salida enumera información, incluyendo `repair ID`, para todas las reparaciones realizadas anteriormente y actualmente en curso.

2. Si la salida muestra que la operación de reparación falló, utilice el `--repair-id` Opción para reintentar la reparación.

Este comando vuelve a intentar una reparación de nodo fallida, utilizando el ID de reparación 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando vuelve a intentar una reparación de volumen fallida, utilizando el ID de reparación 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Comprobar el estado del 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 verificar que el estado deseado del nodo de almacenamiento esté configurado en línea y asegurarse de que el estado estará en línea de manera predeterminada siempre que se reinicie el servidor del nodo de almacenamiento.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Se ha recuperado el nodo de almacenamiento y se ha completado la recuperación de datos.

Pasos

1. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
2. Verifique los valores de **Nodo de almacenamiento recuperado > LDR > Almacenamiento > Estado de almacenamiento - deseado** y **Estado de almacenamiento - actual**.

El valor de ambos atributos debe ser En línea.

3. Si el Estado de almacenamiento - Deseado está configurado en Solo lectura, complete los siguientes pasos:
 - a. Haga clic en la pestaña **Configuración**.
 - b. En la lista desplegable **Estado de almacenamiento – Deseado**, seleccione **En línea**.
 - c. Haga clic en **Aplicar cambios**.

- d. Haga clic en la pestaña **Descripción general** y confirme que los valores de **Estado de almacenamiento - Deseado** y **Estado de almacenamiento - Actual** estén actualizados a En línea.

Restaurar datos de objetos mediante Grid Manager

Puede restaurar datos de objetos para un volumen de almacenamiento o un nodo de almacenamiento fallido mediante Grid Manager. También puede utilizar Grid Manager para supervisar los procesos de restauración en curso y mostrar un historial de restauración.

Antes de empezar

- Ha completado alguno de estos procedimientos para formatear volúmenes fallidos:
 - ["Volver a montar y reformatear los volúmenes de almacenamiento del dispositivo \(pasos manuales\)"](#)
 - ["Volver a montar y reformatear volúmenes de almacenamiento \(pasos manuales\)"](#)
- Ha confirmado que el nodo de almacenamiento donde está restaurando objetos tiene un estado de conexión de **Conectado***  en la pestaña ***NODOS > Descripción general** en el Administrador de cuadrícula.
- Usted ha confirmado lo siguiente:
 - No está en proceso una expansión de la red para agregar un nodo de almacenamiento.
 - La desactivación de un nodo de almacenamiento no está en proceso o ha fallado.
 - No está en proceso la recuperación de un volumen de almacenamiento fallido.
 - No está en proceso la recuperación de un nodo de almacenamiento con una unidad de sistema defectuosa.
 - No hay ningún trabajo de reequilibrio de CE en proceso.
 - La clonación del nodo del dispositivo no está en proceso.

Acerca de esta tarea

Después de haber reemplazado las unidades y realizado los pasos manuales para formatear los volúmenes, Grid Manager muestra los volúmenes como candidatos para restauración en la pestaña **MANTENIMIENTO > Restauración de volumen > Nodos a restaurar**.

Siempre que sea posible, restaure los datos de los objetos utilizando la página Restauración de volumen en el Administrador de cuadrícula. Puedes hacerlo o bien [habilitar el modo de restauración automática](#) para iniciar automáticamente la restauración del volumen cuando los volúmenes estén listos para ser restaurados o [Realizar manualmente la restauración del volumen](#) . Siga estas pautas:

- Si los volúmenes aparecen en **MANTENIMIENTO > Restauración de volumen > Nodos a restaurar**, restaure los datos del objeto como se describe en los pasos a continuación. Los volúmenes se enumerarán si:
 - Algunos, pero no todos, los volúmenes de almacenamiento en un nodo han fallado
 - Todos los volúmenes de almacenamiento en un nodo han fallado y se están reemplazando con la misma cantidad de volúmenes o más volúmenes

La página de restauración de volumen en el Administrador de cuadrícula también le permite [supervisar el proceso de restauración del volumen](#) y [ver el historial de restauración](#) .

- Si los volúmenes no aparecen en el Administrador de cuadrícula como candidatos para restauración, siga

los pasos apropiados para usar el `repair-data` script para restaurar datos de objetos:

- "Restauración de datos de objetos al volumen de almacenamiento (fallo de la unidad del sistema)"
- "Restaurar datos de objetos en un volumen de almacenamiento donde la unidad del sistema está intacta"
- "Restaurar datos de objetos en el volumen de almacenamiento del dispositivo"



El script de reparación de datos está obsoleto y se eliminará en una versión futura.

Si el nodo de almacenamiento recuperado contiene menos volúmenes que el nodo que está reemplazando, debe usar el `repair-data` guion.

Puede restaurar dos tipos de datos de objetos:

- Los objetos de datos replicados se restauran desde otras ubicaciones, asumiendo que las reglas ILM de la red se configuraron para que las copias de objetos estuvieran disponibles.
 - Si se configuró una regla ILM para almacenar solo una copia replicada y esa copia existía en un volumen de almacenamiento que falló, no podrá recuperar el objeto.
 - Si la única copia restante de un objeto está en un grupo de almacenamiento en la nube, StorageGRID debe emitir varias solicitudes al punto final del grupo de almacenamiento en la nube para restaurar los datos del objeto.
- Los objetos de datos codificados por borrado (EC) se restauran reensamblando los fragmentos almacenados. Los fragmentos corruptos o perdidos se recrean mediante el algoritmo de codificación de borrado a partir de los fragmentos de paridad y datos restantes.

Las reparaciones de datos codificados por borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. Sin embargo, si no se pueden contabilizar todos los datos codificados por borrado, no se podrá completar la reparación. La reparación se completará después de que todos los nodos estén disponibles.



La restauración del volumen depende de la disponibilidad de recursos donde se almacenan las copias de los objetos. El progreso de la restauración del volumen no es lineal y puede llevar días o semanas para completarse.

Habilitar el modo de restauración automática

Cuando habilita el modo de restauración automática, la restauración del volumen comienza automáticamente cuando los volúmenes están listos para ser restaurados.

Pasos

1. En Grid Manager, vaya a **MANTENIMIENTO > Restauración de volumen**.
2. Seleccione la pestaña **Nodos para restaurar**, luego deslice el interruptor para **Modo de restauración automática** a la posición habilitada.
3. Cuando aparezca el cuadro de diálogo de confirmación, revise los detalles.



- No podrá iniciar trabajos de restauración de volumen manualmente en ningún nodo.
- Las restauraciones de volumen comenzarán automáticamente solo cuando no haya otros procedimientos de mantenimiento en curso.
- Puede supervisar el estado del trabajo desde la página de seguimiento del progreso.
- StorageGRID vuelve a intentar automáticamente las restauraciones de volúmenes que no logran iniciarse.

4. Cuando comprenda los resultados de habilitar el modo de restauración automática, seleccione **Sí** en el cuadro de diálogo de confirmación.

Puede desactivar el modo de restauración automática en cualquier momento.

Restaurar manualmente el volumen o nodo fallido

Siga estos pasos para restaurar un volumen o nodo fallido.

Pasos

1. En Grid Manager, vaya a **MANTENIMIENTO > Restauración de volumen**.
2. Seleccione la pestaña **Nodos para restaurar**, luego deslice el interruptor para **Modo de restauración automática** a la posición deshabilitada.

El número en la pestaña indica la cantidad de nodos con volúmenes que requieren restauración.

3. Expanda cada nodo para ver los volúmenes que necesitan restauración y su estado.
4. Corrija cualquier problema que impida la restauración de cada volumen. Los problemas se indicarán cuando seleccione **Esperando pasos manuales**, si se muestra como el estado del volumen.
5. Seleccione un nodo para restaurar donde todos los volúmenes indiquen un estado Listo para restaurar.

Solo puedes restaurar los volúmenes de un nodo a la vez.

Cada volumen del nodo debe indicar que está listo para restaurar.

6. Seleccione **Iniciar restauración**.
7. Aborde cualquier advertencia que pueda aparecer o seleccione **Iniciar de todos modos** para ignorar las advertencias y comenzar la restauración.

Los nodos se mueven de la pestaña **Nodos a restaurar** a la pestaña **Progreso de restauración** cuando comienza la restauración.

Si no se puede iniciar una restauración de volumen, el nodo regresa a la pestaña **Nodos para restaurar**.

Ver el progreso de la restauración

La pestaña **Progreso de restauración** muestra el estado del proceso de restauración del volumen e información sobre los volúmenes de un nodo que se está restaurando.

Las tasas de reparación de datos para objetos replicados y codificados por borrado en todos los volúmenes son promedios que resumen todas las restauraciones en proceso, incluidas aquellas restauraciones iniciadas utilizando el `repair-data` guion. También se indica el porcentaje de objetos de dichos volúmenes que están intactos y no requieren restauración.



La restauración de datos replicados depende de la disponibilidad de recursos donde se almacenan las copias replicadas. El progreso de la restauración de datos replicados no es lineal y puede tardar días o semanas en completarse.

La sección Trabajos de restauración muestra información sobre las restauraciones de volumen iniciadas desde Grid Manager.

- El número en el encabezado de la sección Trabajos de restauración indica la cantidad de volúmenes que se están restaurando o que están en cola para su restauración.
- La tabla muestra información sobre cada volumen de un nodo que se está restaurando y su progreso.
 - El progreso de cada nodo muestra el porcentaje de cada trabajo.
 - Expanda la columna Detalles para mostrar la hora de inicio de la restauración y el ID del trabajo.
- Si falla la restauración de un volumen:
 - La columna Estado indica `failed (attempting retry)`, y se volverá a intentar automáticamente.
 - Si fallan varios trabajos de restauración, se volverá a intentar automáticamente primero el trabajo más reciente.
 - La alerta **Error de reparación de EC** se activa si los reintentos continúan fallando. Siga los pasos de la alerta para resolver el problema.

Ver historial de restauración

La pestaña **Historial de restauraciones** muestra información sobre todas las restauraciones de volumen que se han completado exitosamente.



Los tamaños no son aplicables a los objetos replicados y aparecen únicamente para las restauraciones que contienen objetos de datos con código de borrado (EC).

Supervisar trabajos de reparación de datos

Puede supervisar el estado de los trabajos de reparación mediante el `repair-data` script desde la línea de comandos.

Estos incluyen trabajos que inició manualmente o trabajos que StorageGRID inició automáticamente como parte de un procedimiento de desmantelamiento.



Si está ejecutando trabajos de restauración de volumen, "[Monitorear el progreso y ver un historial de esos trabajos en el Administrador de cuadrícula](#)" en cambio.

Monitorear el estado de `repair-data` trabajos en función de si utiliza **datos replicados**, **datos codificados por borrado (EC)** o ambos.

Datos replicados

- Para obtener un porcentaje estimado de finalización de la reparación replicada, agregue el `show-replicated-repair-status` Opción para el comando `reparar-datos`.

```
repair-data show-replicated-repair-status
```

- Para determinar si las reparaciones están completas:
 - a. Seleccione **NODOS > Nodo de almacenamiento en reparación > ILM**.
 - b. Revise los atributos en la sección Evaluación. Cuando se completan las reparaciones, el atributo **En espera - Todo** indica 0 objetos.
- Para supervisar la reparación con más detalle:
 - a. Seleccione **SOPORTE > Herramientas > Topología de cuadrícula**.
 - b. Seleccione **grid > Nodo de almacenamiento en reparación > LDR > Almacén de datos**.
 - c. Utilice una combinación de los siguientes atributos para determinar, lo mejor posible, si las reparaciones replicadas están completas.



Pueden existir inconsistencias en Cassandra y no se realiza un seguimiento de las reparaciones fallidas.

- **Reparaciones intentadas (XRPA)**: utilice este atributo para rastrear el 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 escaneo actual (proporcionado por el atributo **Período de escaneo – Estimado**), significa que el escaneo ILM no encontró objetos de alto riesgo que necesiten reparación en ningún nodo.



Los objetos de alto riesgo son objetos que corren el riesgo de perderse por completo. Esto no incluye objetos que no satisfacen su configuración ILM.

- **Período de escaneo estimado (XSCM)**: utilice este atributo para estimar cuándo se aplicará un cambio de política a los objetos ingeridos previamente. Si el atributo **Reparaciones intentadas** no aumenta durante un período más largo que el período de escaneo actual, es probable que se realicen reparaciones replicadas. Tenga en cuenta que el período de escaneo puede cambiar. El atributo **Período de escaneo estimado (XSCM)** se aplica a toda la cuadrícula y es el máximo de todos los períodos de escaneo de nodos. Puede consultar el historial de atributos **Período de escaneo – Estimado** de la cuadrícula para determinar un período de tiempo apropiado.

Datos codificados por borrado (EC)

Para supervisar la reparación de datos codificados por borrado y volver a intentar cualquier solicitud que pueda haber fallado:

1. Determinar el estado de las reparaciones de datos codificados por borrado:
 - Seleccione **SOPORTE > Herramientas > Métricas** para ver el tiempo estimado de finalización y el porcentaje de finalización del trabajo actual. Luego, seleccione **Descripción general de EC** en la sección Grafana. Consulte los paneles **Tiempo estimado de finalización del trabajo de Grid EC** 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
```

La salida enumera información, incluyendo `repair ID`, para todas las reparaciones realizadas anteriormente y actualmente en curso.

2. Si la salida muestra que la operación de reparación falló, utilice el `--repair-id` Opción para reintentar la reparación.

Este comando vuelve a intentar una reparación de nodo fallida, utilizando el ID de reparación 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando vuelve a intentar una reparación de volumen fallida, utilizando el ID de reparación 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Recuperarse de fallos del nodo de administración

Recuperación del nodo de administración primario o no primario

El proceso de recuperación de un nodo de administración depende de si es el nodo de administración principal o un nodo de administración no principal.

Los pasos de alto nivel para recuperar un nodo de administración primario o no primario son los mismos, aunque los detalles de los pasos difieren.

Siga siempre el procedimiento de recuperación correcto para el nodo de administración que está recuperando. Los procedimientos parecen iguales a alto nivel, pero difieren en los detalles.

Opciones

- ["Recuperarse de fallas del nodo de administración principal"](#)
- ["Recuperarse de fallas del nodo de administración no principal"](#)

Recuperarse de fallas del nodo de administración principal

Recuperarse de fallas del nodo de administración principal

Debe completar un conjunto específico de tareas para recuperarse de una falla del nodo de administración principal. El nodo de administración principal aloja el servicio del nodo de gestión de configuración (CMN) para la red.



Debe reparar o reemplazar rápidamente un nodo de administración principal que haya fallado o la red podría perder su capacidad de ingerir nuevos objetos. El período de tiempo exacto depende de su tasa de ingesta de objetos: si necesita una evaluación más precisa del período de tiempo para su red, comuníquese con el soporte técnico.

El servicio Nodo de gestión de configuración (CMN) en el nodo de administración principal es responsable de emitir bloques de identificadores de objetos para la red. Estos identificadores se asignan a los objetos a medida que se ingieren. No se pueden ingerir nuevos objetos a menos que haya identificadores disponibles. La ingesta de objetos puede continuar mientras el CMN no está disponible porque aproximadamente un mes de suministro de identificadores se almacena en caché en la red. Sin embargo, una vez agotados los identificadores almacenados en caché, no se pueden agregar objetos nuevos.

Siga estos pasos de alto nivel para recuperar un nodo de administración principal:

1. ["Copiar registros de auditoría del nodo de administración principal fallido"](#)
2. ["Reemplazar el nodo de administración principal"](#)
3. ["Configurar el nodo de administración principal de reemplazo"](#)
4. ["Determinar si existe un requisito de revisión urgente para el nodo de administración principal recuperado"](#)
5. ["Restaurar el registro de auditoría en el nodo de administración principal recuperado"](#)
6. ["Restaurar la base de datos del nodo de administración al recuperar un nodo de administración principal"](#)
7. ["Restaurar las métricas de Prometheus al recuperar un nodo de administración principal"](#)

Copiar registros de auditoría del nodo de administración principal fallido

Si puede copiar los registros de auditoría del nodo de administración principal fallido, debe conservarlos para mantener el registro de la actividad y el uso del sistema de la red. Puede restaurar los registros de auditoría conservados en el nodo de administración principal recuperado después de que esté en funcionamiento.

Acerca de esta tarea

Este procedimiento copia los archivos de registro de auditoría del nodo de administración fallido a una ubicación temporal en un nodo de red separado. Estos registros de auditoría conservados se pueden luego copiar al nodo de administración de reemplazo. Los registros de auditoría no se copian automáticamente al nuevo nodo de administración.

Dependiendo del tipo de falla, es posible que no pueda copiar los registros de auditoría de un nodo de administración fallido. Si la implementación solo tiene un nodo de administración, el nodo de administración recuperado comienza a registrar eventos en el registro de auditoría en un nuevo archivo vacío y se pierden los datos registrados previamente. Si la implementación incluye más de un nodo de administración, puede recuperar los registros de auditoría de otro nodo de administración.



Si no se puede acceder a los registros de auditoría en el nodo de administración fallido ahora, es posible que pueda acceder a ellos más tarde, por ejemplo, después de la recuperación del host.

Pasos

1. Si es posible, inicie sesión en el nodo de administración que falló. De lo contrario, inicie sesión en el nodo de administración principal o en otro nodo de administración, si está disponible.
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`

- b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de \$ a # .

2. Detenga el servicio AMS para evitar que cree un nuevo archivo de registro:`service ams stop`
3. Navegue hasta el directorio de exportación de auditoría:

```
cd /var/local/log
```

4. Cambiar el nombre de la fuente `audit.log` archivo a un nombre de archivo numerado único. Por ejemplo, cambie el nombre del archivo `audit.log` a `2023-10-25.txt.1` .

```
ls -l
mv audit.log 2023-10-25.txt.1
```

5. Reiniciar el servicio AMS: `service ams start`
6. Cree el directorio para copiar todos los archivos de registro de auditoría a una ubicación temporal en un nodo de cuadrícula separado: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Cuando se le solicite, ingrese la contraseña de administrador.

7. Copie todos los archivos de registro de auditoría a la ubicación temporal: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Cuando se le solicite, ingrese la contraseña de administrador.

8. Cerrar sesión como root: `exit`

Reemplazar el nodo de administración principal

Para recuperar un nodo de administración principal, primero debe reemplazar el hardware físico o virtual.

Puede reemplazar un nodo de administración principal fallido con un nodo de administración principal que se ejecute en la misma plataforma, o puede reemplazar un nodo de administración principal que se ejecute en VMware o un host Linux con un nodo de administración principal alojado en un dispositivo de servicios.

Utilice el procedimiento que coincida con la plataforma de reemplazo que seleccione para el nodo. Después de completar el procedimiento de reemplazo de nodo (que es adecuado para todos los tipos de nodo), ese procedimiento lo dirigirá al siguiente paso para la recuperación del nodo de administración principal.

Plataforma de reemplazo	Procedimiento
VMware	"Reemplazar un nodo de VMware"

Plataforma de reemplazo	Procedimiento
Linux	"Reemplazar un nodo Linux"
Servicios de electrodomésticos	"Reemplazar un dispositivo de servicios"
OpenStack	Los archivos de disco de máquina virtual y los scripts proporcionados por NetApp para OpenStack ya no son compatibles con las operaciones de recuperación. Si necesita recuperar un nodo que se ejecuta en una implementación de OpenStack, descargue los archivos para su sistema operativo Linux. A continuación, siga el procedimiento para "Reemplazar un nodo Linux" .

Configurar el nodo de administración principal de reemplazo

El nodo de reemplazo debe configurarse como el nodo de administración principal para su sistema StorageGRID .

Antes de empezar

- Para los nodos de administración principales alojados en máquinas virtuales, la máquina virtual se ha implementado, encendido e inicializado.
- Para los nodos de administración principales alojados en un dispositivo de servicios, ha reemplazado el dispositivo y ha instalado el software. Ver el ["Instrucciones de instalación para su electrodoméstico"](#) .
- Tiene la última copia de seguridad del archivo del paquete de recuperación(`sgws-recovery-package-id-revision.zip`).
- Tienes la contraseña de aprovisionamiento.

Pasos

1. Abra su navegador web y navegue hasta `https://primary_admin_node_ip` .
2. Administre una contraseña de instalador temporal según sea necesario:
 - Si ya se ha establecido una contraseña utilizando uno de estos métodos, introdúzcala para continuar.
 - Un usuario estableció la contraseña al acceder al instalador previamente
 - Para los sistemas físicos, la contraseña se importó automáticamente desde el archivo de configuración del nodo en `/etc/storagegrid/nodes/<node_name>.conf`
 - Para las máquinas virtuales, la contraseña de SSH/consola se importó automáticamente desde las propiedades de OVF
 - Si no se ha establecido una contraseña, opcionalmente establezca una contraseña para proteger el instalador de StorageGRID .
3. Haga clic en **Recuperar un nodo de administración principal fallido**.

Welcome

Use this page to install a new StorageGRID system, or recover a failed primary Admin Node for an existing system.

Note: You must have access to a StorageGRID license, network configuration and grid topology information, and NTP settings to complete the installation. You must have the latest version of the Recovery Package file to complete a primary Admin Node recovery.



Install a StorageGRID system



Recover a failed primary Admin
Node

4. Cargue la copia de seguridad más reciente del paquete de recuperación:
 - a. Haga clic en **Explorar**.
 - b. Localice el archivo de paquete de recuperación más reciente para su sistema StorageGRID y haga clic en **Abrir**.
5. Introduzca la contraseña de aprovisionamiento.
6. Haga clic en **Iniciar recuperación**.

Comienza el proceso de recuperación. Es posible que el Administrador de red no esté disponible durante unos minutos mientras se inician los servicios necesarios. Cuando se complete la recuperación, se mostrará la página de inicio de sesión.

7. Si el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID y la confianza de usuario autenticado para el nodo de administración que recuperó estaba configurada para usar el certificado de interfaz de administración predeterminado, actualice (o elimine y vuelva a crear) la confianza de usuario autenticado del nodo en los Servicios de federación de Active Directory (AD FS). Utilice el nuevo certificado de servidor predeterminado que se generó durante el proceso de recuperación del nodo de administración.



Para configurar una relación de confianza entre usuarios, consulte ["Configurar el inicio de sesión único"](#). Para acceder al certificado de servidor predeterminado, inicie sesión en el shell de comandos del nodo de administración. Ir a la `/var/local/mgmt-api` directorio y seleccione el `server.crt` archivo.



Después de recuperar un nodo de administración principal, ["determinar si es necesario aplicar una revisión"](#).

Determinar el requisito de revisión para el nodo de administración principal

Después de recuperar un nodo de administración principal, determine si necesita aplicar una revisión.

Antes de empezar

La recuperación del nodo de administración principal está completa.

Pasos

1. Sign in en Grid Manager usando un ["navegador web compatible"](#).
2. Seleccione **NODOS**.
3. De la lista de la izquierda, seleccione el nodo de administración principal.
4. En la pestaña Descripción general, observe la versión que se muestra en el campo **Versión del software**.
5. Seleccione cualquier otro nodo de la cuadrícula.
6. En la pestaña Descripción general, observe la versión que se muestra en el campo **Versión del software**.
 - Si las versiones que se muestran en los campos **Versión de software** son las mismas, no es necesario aplicar una revisión.
 - Si las versiones que se muestran en los campos **Versión del software** son diferentes, debe ["aplicar una revisión"](#) para actualizar el nodo de administración principal recuperado a la misma versión.

Restaurar el registro de auditoría en el nodo de administración principal recuperado

Si pudo conservar el registro de auditoría del nodo de administración principal fallido, puede copiarlo al nodo de administración principal que está recuperando.

Antes de empezar

- El nodo de administración recuperado está instalado y funcionando.
- Ha copiado los registros de auditoría a otra ubicación después de que el nodo de administración original fallara.

Acerca de esta tarea

Si un nodo de administración falla, es posible que se pierdan los registros de auditoría guardados en ese nodo de administración. Es posible que sea posible preservar los datos de la pérdida copiando los registros de auditoría del nodo de administración fallido y luego restaurándolos en el nodo de administración recuperado. Dependiendo de la falla, es posible que no sea posible copiar los registros de auditoría del nodo de administración fallido. En ese caso, si la implementación tiene más de un nodo de administración, puede recuperar registros de auditoría de otro nodo de administración, ya que los registros de auditoría se replican en todos los nodos de administración.

Si solo hay un nodo de administración y no se puede copiar el registro de auditoría del nodo fallido, el nodo de administración recuperado comienza a registrar eventos en el registro de auditoría como si la instalación fuera nueva.

Debe recuperar un nodo de administración lo antes posible para restaurar la funcionalidad de registro.

De forma predeterminada, la información de auditoría se envía al registro de auditoría en los nodos de administración. Puede omitir estos pasos si se aplica alguna de las siguientes situaciones:



- Configuró un servidor syslog externo y los registros de auditoría ahora se envían al servidor syslog en lugar de a los nodos de administración.
- Usted especificó explícitamente que los mensajes de auditoría deben guardarse solo en los nodos locales que los generaron.

Ver ["Configurar mensajes de auditoría y destinos de registro"](#) Para 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 el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Después de iniciar sesión como root, el mensaje cambia de \$ a # .

2. Compruebe qué archivos de auditoría se han conservado: `cd /var/local/log`

3. Copie los archivos de registro de auditoría conservados al nodo de administración recuperado: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

Cuando se le solicite, ingrese la contraseña de administrador.

4. Por seguridad, elimine los registros de auditoría del nodo de red fallido después de verificar que se hayan copiado correctamente al nodo de administración 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 root: `exit`

Restaurar la base de datos del nodo de administración al recuperar el nodo de administración principal

Si desea conservar la información histórica sobre los atributos y las alertas de un nodo de administración principal que ha fallado, puede restaurar la base de datos del nodo de administración. Solo puede restaurar esta base de datos si su sistema StorageGRID incluye otro nodo de administración.

Antes de empezar

- El nodo de administración recuperado está instalado y funcionando.
- El sistema StorageGRID incluye al menos dos nodos de administración.
- Tú tienes el `Passwords.txt` archivo.
- Tienes la contraseña de aprovisionamiento.

Acerca de esta tarea

Si un nodo de administración falla, se pierde la información histórica almacenada en su base de datos. Esta base de datos incluye la siguiente información:

- Historial de alertas
- Datos de atributos históricos, que se utilizan en gráficos de estilo heredado en la página Nodos

Cuando recupera un nodo de administración, el proceso de instalación del software crea una base de datos de nodo de administración vacía en el nodo recuperado. Sin embargo, la nueva base de datos sólo incluye información de los servidores y servicios que actualmente forman parte del sistema o que se agregarán posteriormente.

Si restauró un nodo de administración principal y su 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 principal (el *nodo de administración de origen*) al nodo de administración principal recuperado. Si su sistema solo tiene un nodo de administración principal, no podrá restaurar la base de datos del nodo de administración.



Copiar la base de datos del nodo de administración puede tardar varias horas. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios estén detenidos en el nodo de administración de origen.

Pasos

1. Inicie sesión en el nodo de administración de origen:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
2. Desde el nodo de administración de origen, detenga el servicio MI: `service mi stop`
3. Desde el nodo de administración de origen, detenga el servicio de interfaz de programación de aplicaciones de administración (mgmt-api): `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 el `Passwords.txt` archivo.
 - iii. Introduzca el siguiente comando para cambiar a root: `su -`
 - iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - b. Detener el servicio MI: `service mi stop`
 - c. Detener el servicio mgmt-api: `service mgmt-api stop`
 - d. Agregue la clave privada SSH al agente SSH. Ingresar: `ssh-add`
 - e. Ingrese la contraseña de acceso SSH que aparece en el `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 al nodo de administración recuperado. Una vez finalizada la operación de copia, el script inicia el nodo de administración recuperado.

- h. Cuando ya no necesite acceso sin contraseña a otros servidores, elimine la clave privada del agente SSH. Ingresar: `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

Opcionalmente, puede conservar las métricas históricas mantenidas por Prometheus en un nodo de administración principal que haya fallado. Las métricas de Prometheus solo se pueden restaurar si su sistema StorageGRID incluye otro nodo de administración.

Antes de empezar

- El nodo de administración recuperado está instalado y funcionando.
- El sistema StorageGRID incluye al menos dos nodos de administración.
- Tú tienes el `Passwords.txt` archivo.
- Tienes la contraseña de aprovisionamiento.

Acerca de esta tarea

Si un nodo de administración falla, se pierden las métricas mantenidas en la base de datos de Prometheus en el nodo de administración. Cuando recupera el nodo de administración, el proceso de instalación del software crea una nueva base de datos de Prometheus. Una vez iniciado el nodo de administración recuperado, registra las métricas como si hubiera realizado una nueva instalación del sistema StorageGRID .

Si restauró un nodo de administración principal y su sistema StorageGRID tiene otro nodo de administración, puede restaurar las métricas históricas copiando la base de datos de Prometheus desde un nodo de administración no principal (el *nodo de administración de origen*) al nodo de administración principal recuperado. Si su sistema solo tiene un nodo de administración principal, no podrá restaurar la base de datos de Prometheus.



Copiar la base de datos de Prometheus podría tardar una hora o más. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios estén detenidos en el nodo de administración de origen.

Pasos

1. Inicie sesión en el nodo de administración de origen:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
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 el `Passwords.txt` archivo.
 - iii. Introduzca el siguiente comando para cambiar a root: `su -`
 - iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- b. Detener el servicio Prometheus: `service prometheus stop`
- c. Agregue la clave privada SSH al agente SSH. Ingresar: `ssh-add`
- d. Ingrese la contraseña de acceso SSH que aparece en el `Passwords.txt` archivo.
- e. Copie la base de datos de 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, presione **Enter** para confirmar que desea destruir la nueva base de datos de Prometheus en el nodo de administración recuperado.

La base de datos original de Prometheus y sus datos históricos se copian al nodo de administración recuperado. Una vez finalizada la operación de copia, el script inicia el nodo de administración recuperado. Aparece el siguiente estado:

Base de datos clonada, iniciando servicios

- a. Cuando ya no necesite acceso sin contraseña a otros servidores, elimine la clave privada del agente SSH. Ingresar: `ssh-add -D`
4. Reinicie el servicio Prometheus en el nodo de administración de origen. `service prometheus start`

Recuperarse de fallas del nodo de administración no principal

Recuperarse de fallas del nodo de administración no principal

Debe completar las siguientes tareas para recuperarse de una falla del nodo de administración no principal. Un nodo de administración aloja el servicio del nodo de administración de configuración (CMN) y se conoce como el nodo de administración principal. Aunque puede tener varios nodos de administración, cada sistema StorageGRID incluye solo un nodo de administración principal. Todos los demás nodos de administración son nodos de administración no principales.

Siga estos pasos de alto nivel para recuperar un nodo de administración no principal:

1. "Copiar registros de auditoría del nodo de administración no principal que falló"
2. "Reemplazar el nodo de administración no principal"
3. "Seleccione Iniciar recuperación para configurar el nodo de administración no principal"
4. "Restaurar el registro de auditoría en un nodo de administración no principal recuperado"
5. "Restaurar la base de datos del nodo de administración al recuperar un nodo de administración no principal"
6. "Restaurar las métricas de Prometheus al recuperar un nodo de administración no principal"

Copiar registros de auditoría de un nodo de administración no principal fallido

Si puede copiar los registros de auditoría del nodo de administración fallido, debe conservarlos para mantener el registro de la red sobre la actividad y el uso del sistema. Puede restaurar los registros de auditoría conservados en el nodo de administración no principal recuperado después de que esté en funcionamiento.

Este procedimiento copia los archivos de registro de auditoría del nodo de administración fallido a una ubicación temporal en un nodo de red separado. Estos registros de auditoría conservados se pueden luego copiar al nodo de administración de reemplazo. Los registros de auditoría no se copian automáticamente al nuevo nodo de administración.

Dependiendo del tipo de falla, es posible que no pueda copiar los registros de auditoría de un nodo de administración fallido. Si la implementación solo tiene un nodo de administración, el nodo de administración recuperado comienza a registrar eventos en el registro de auditoría en un nuevo archivo vacío y se pierden los datos registrados previamente. Si la implementación incluye más de un nodo de administración, puede recuperar los registros de auditoría de otro nodo de administración.



Si no se puede acceder a los registros de auditoría en el nodo de administración fallido ahora, es posible que pueda acceder a ellos más tarde, por ejemplo, después de la recuperación del host.

1. Si es posible, inicie sesión en el nodo de administración que falló. De lo contrario, inicie sesión en el nodo de administración principal o en otro nodo de administración, si está disponible.

- a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
- b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- c. Introduzca el siguiente comando para cambiar a root: `su -`
- d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#`.

2. Detenga el servicio AMS para evitar que cree un nuevo archivo de registro: `service ams stop`
3. Navegue hasta el directorio de exportación de auditoría:

```
cd /var/local/log
```

4. Cambie el nombre del archivo `audit.log` de origen a un nombre de archivo numerado único. Por ejemplo, cambie el nombre del archivo `audit.log` a `2023-10-25.txt.1`.

```
ls -l
mv audit.log 2023-10-25.txt.1
```

5. Reiniciar el servicio AMS: `service ams start`
6. Cree el directorio para copiar todos los archivos de registro de auditoría a una ubicación temporal en un nodo de cuadrícula separado: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Cuando se le solicite, ingrese la contraseña de administrador.

7. Copie todos los archivos de registro de auditoría a la ubicación temporal: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Cuando se le solicite, ingrese la contraseña de administrador.

8. Cerrar sesión como root: `exit`

Reemplazar el nodo de administración no principal

Para recuperar un nodo de administración no principal, primero debe reemplazar el hardware físico o virtual.

Puede reemplazar un nodo de administración no principal fallido con un nodo de administración no principal que se ejecute en la misma plataforma, o puede reemplazar un nodo de administración no principal que se ejecute en VMware o un host Linux con un nodo de administración no principal alojado en un dispositivo de servicios.

Utilice el procedimiento que coincida con la plataforma de reemplazo que seleccione para el nodo. Después de completar el procedimiento de reemplazo de nodo (que es adecuado para todos los tipos de nodos), ese procedimiento lo dirigirá al siguiente paso para la recuperación del nodo de administración no principal.

Plataforma de reemplazo	Procedimiento
VMware	"Reemplazar un nodo de VMware"
Linux	"Reemplazar un nodo Linux"
Servicios de electrodomésticos	"Reemplazar un dispositivo de servicios"
OpenStack	Los archivos de disco de máquina virtual y los scripts proporcionados por NetApp para OpenStack ya no son compatibles con las operaciones de recuperación. Si necesita recuperar un nodo que se ejecuta en una implementación de OpenStack, descargue los archivos para su sistema operativo Linux. A continuación, siga el procedimiento para "Reemplazar un nodo Linux" .

Seleccione Iniciar recuperación para configurar el nodo de administración no principal

Después de reemplazar un nodo de administración no principal, debe seleccionar Iniciar recuperación en el Administrador de red para configurar el nuevo nodo como reemplazo del nodo fallido.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tú tienes el ["Permiso de mantenimiento o acceso root"](#).
- Tienes la contraseña de aprovisionamiento.
- Ha implementado y configurado el nodo de reemplazo.

Pasos

1. Desde el Administrador de red, seleccione **MANTENIMIENTO > Tareas > Recuperación**.
2. Seleccione el nodo de la cuadrícula que desea recuperar en la lista de Nodos pendientes.

Los nodos aparecen en la lista después de fallar, pero no puedes seleccionar un nodo hasta que se haya reinstalado y esté listo para la recuperación.
3. Introduzca la **contraseña de aprovisionamiento**.
4. Haga clic en **Iniciar recuperación**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search 				
	Name	IPv4 Address	State	Recoverable
	104-217-S1	10.96.104.217	Unknown	

Passphrase

Provisioning Passphrase

Start Recovery

5. Supervise el progreso de la recuperación en la tabla Nodo de cuadrícula en recuperación.



Mientras se ejecuta el procedimiento de recuperación, puede hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparece un cuadro de diálogo que indica que el nodo quedará en un estado indeterminado si restablece el procedimiento.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Si desea volver a intentar la recuperación después de restablecer el procedimiento, debe restaurar el nodo

a un estado preinstalado, de la siguiente manera:

- **VMware:** eliminar el nodo de red virtual implementado. Luego, cuando esté listo para reiniciar la recuperación, vuelva a implementar el nodo.
- **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 restablecer el procedimiento, debe restaurar el nodo del dispositivo a un estado preinstalado ejecutando `sgareinstall` en el nodo. Ver ["Preparar el dispositivo para la reinstalación \(solo reemplazo de plataforma\)"](#) .

6. Si el inicio de sesión único (SSO) está habilitado para su sistema StorageGRID y la confianza de usuario autenticado para el nodo de administración que recuperó estaba configurada para usar el certificado de interfaz de administración predeterminado, actualice (o elimine y vuelva a crear) la confianza de usuario autenticado del nodo en los Servicios de federación de Active Directory (AD FS). Utilice el nuevo certificado de servidor predeterminado que se generó durante el proceso de recuperación del nodo de administración.



Para configurar una relación de confianza entre usuarios, consulte ["Configurar el inicio de sesión único"](#) . Para acceder al certificado de servidor predeterminado, inicie sesión en el shell de comandos del nodo de administración. Ir a la `/var/local/mgmt-api` directorio y seleccione el `server.crt` archivo.

Restaurar el registro de auditoría en el nodo de administración no principal recuperado

Si pudo conservar el registro de auditoría del nodo de administración no principal que falló, de modo que se conserve la información histórica del registro de auditoría, puede copiarlo al nodo de administración no principal que está recuperando.

Antes de empezar

- El nodo de administración recuperado está instalado y funcionando.
- Ha copiado los registros de auditoría a otra ubicación después de que el nodo de administración original fallara.

Acerca de esta tarea

Si un nodo de administración falla, es posible que se pierdan los registros de auditoría guardados en ese nodo de administración. Es posible que sea posible preservar los datos de la pérdida copiando los registros de auditoría del nodo de administración fallido y luego restaurándolos en el nodo de administración recuperado. Dependiendo de la falla, es posible que no sea posible copiar los registros de auditoría del nodo de administración fallido. En ese caso, si la implementación tiene más de un nodo de administración, puede recuperar registros de auditoría de otro nodo de administración, ya que los registros de auditoría se replican en todos los nodos de administración.

Si solo hay un nodo de administración y no se puede copiar el registro de auditoría del nodo fallido, el nodo de administración recuperado comienza a registrar eventos en el registro de auditoría como si la instalación fuera nueva.

Debe recuperar un nodo de administración lo antes posible para restaurar la funcionalidad de registro.

De forma predeterminada, la información de auditoría se envía al registro de auditoría en los nodos de administración. Puede omitir estos pasos si se aplica alguna de las siguientes situaciones:



- Configuró un servidor syslog externo y los registros de auditoría ahora se envían al servidor syslog en lugar de a los nodos de administración.
- Usted especificó explícitamente que los mensajes de auditoría deben guardarse solo en los nodos locales que los generaron.

Ver ["Configurar mensajes de auditoría y destinos de registro"](#) Para 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 el `Passwords.txt` archivo.

c. Introduzca el siguiente comando para cambiar a root: `su -`

d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Después de iniciar sesión como root, el mensaje cambia de `$` a `#`.

2. Compruebe qué archivos de auditoría se han conservado:

```
cd /var/local/log
```

3. Copie los archivos de registro de auditoría conservados al nodo de administración recuperado:

```
scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
```

Cuando se le solicite, ingrese la contraseña de administrador.

4. Por seguridad, elimine los registros de auditoría del nodo de red fallido después de verificar que se hayan copiado correctamente al nodo de administración 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 root: `exit`

Restaurar la base de datos del nodo de administración al recuperar un nodo de administración no principal

Si desea conservar la información histórica sobre los atributos y las alertas de un nodo de administración no principal que ha fallado, puede restaurar la base de datos del nodo de administración desde el nodo de administración principal.

Antes de empezar

- El nodo de administración recuperado está instalado y funcionando.

- El sistema StorageGRID incluye al menos dos nodos de administración.
- Tú tienes el `Passwords.txt` archivo.
- Tienes la contraseña de aprovisionamiento.

Acerca de esta tarea

Si un nodo de administración falla, se pierde la información histórica almacenada en su base de datos. Esta base de datos incluye la siguiente información:

- Historial de alertas
- Datos de atributos históricos, que se utilizan en gráficos de estilo heredado en la página Nodos

Cuando recupera un nodo de administración, el proceso de instalación del software crea una base de datos de nodo de administración vacía en el nodo recuperado. Sin embargo, la nueva base de datos sólo incluye información de los servidores y servicios que actualmente forman parte del sistema o que se agregarán posteriormente.

Si restauró un nodo de administración no principal, puede restaurar la información histórica copiando la base de datos del nodo de administración desde el nodo de administración principal (el *nodo de administración de origen*) al nodo recuperado.



Copiar la base de datos del nodo de administración puede tardar varias horas. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios estén detenidos en el nodo de origen.

Pasos

1. Inicie sesión en el nodo de administración de origen:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
2. Ejecute el siguiente comando desde el nodo de administración de origen. Luego, ingrese la contraseña 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. Desde el nodo de administración de origen, detenga el servicio de interfaz de programación de aplicaciones de administración (mgmt-api): `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 el `Passwords.txt` archivo.
 - iii. Introduzca el siguiente comando para cambiar a root: `su -`
 - iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - b. Detener el servicio MI: `service mi stop`
 - c. Detener el servicio mgmt-api: `service mgmt-api stop`

- d. Agregue la clave privada SSH al agente SSH. Ingresar: `ssh-add`
- e. Ingrese la contraseña de acceso SSH que aparece en el `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 al nodo de administración recuperado. Una vez finalizada la operación de copia, el script inicia el nodo de administración recuperado.

- h. Cuando ya no necesite acceso sin contraseña a otros servidores, elimine la clave privada del agente SSH. Ingresar: `ssh-add -D`

6. Reinicie los servicios en el nodo de administración de origen: `service servermanager start`

Restaurar las métricas de Prometheus al recuperar un nodo de administración no principal

Opcionalmente, puede conservar las métricas históricas mantenidas por Prometheus en un nodo de administración no principal que haya fallado.

Antes de empezar

- El nodo de administración recuperado está instalado y funcionando.
- El sistema StorageGRID incluye al menos dos nodos de administración.
- Tú tienes el `Passwords.txt` archivo.
- Tienes la contraseña de aprovisionamiento.

Acerca de esta tarea

Si un nodo de administración falla, se pierden las métricas mantenidas en la base de datos de Prometheus en el nodo de administración. Cuando recupera el nodo de administración, el proceso de instalación del software crea una nueva base de datos de Prometheus. Una vez iniciado el nodo de administración recuperado, registra las métricas como si hubiera realizado una nueva instalación del sistema StorageGRID .

Si restauró un nodo de administración no principal, puede restaurar las métricas históricas copiando la base de datos de Prometheus desde el nodo de administración principal (el *nodo de administración de origen*) al nodo de administración recuperado.



Copiar la base de datos de Prometheus podría tardar una hora o más. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios estén detenidos en el nodo de administración de origen.

Pasos

1. Inicie sesión en el nodo de administración de origen:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
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 el `Passwords.txt` archivo.
 - iii. Introduzca el siguiente comando para cambiar a root: `su -`
 - iv. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
- b. Detener el servicio Prometheus: `service prometheus stop`
- c. Agregue la clave privada SSH al agente SSH. Ingresar: `ssh-add`
- d. Ingrese la contraseña de acceso SSH que aparece en el `Passwords.txt` archivo.
- e. Copie la base de datos de 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, presione **Enter** para confirmar que desea destruir la nueva base de datos de Prometheus en el nodo de administración recuperado.

La base de datos original de Prometheus y sus datos históricos se copian al nodo de administración recuperado. Una vez finalizada la operación de copia, el script inicia el nodo de administración recuperado. Aparece el siguiente estado:

Base de datos clonada, iniciando servicios

- a. Cuando ya no necesite acceso sin contraseña a otros servidores, elimine la clave privada del agente SSH. Ingresar: `ssh-add -D`

4. Reinicie el servicio Prometheus en el nodo de administración de origen. `service prometheus start`

Recuperarse de fallos del nodo de enlace

Reemplazar el nodo de puerta de enlace

Puede reemplazar un nodo de puerta de enlace fallido con 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 con un nodo de puerta de enlace alojado en un dispositivo de servicios.

El procedimiento de reemplazo de nodo que debe seguir depende de qué plataforma utilizará el nodo de reemplazo. Después de completar el procedimiento de reemplazo de nodo (que es adecuado para todos los tipos de nodo), ese procedimiento lo dirigirá al siguiente paso para la recuperación del nodo de puerta de enlace.

Plataforma de reemplazo	Procedimiento
VMware	"Reemplazar un nodo de VMware"

Plataforma de reemplazo	Procedimiento
Linux	"Reemplazar un nodo Linux"
Servicios de electrodomésticos	"Reemplazar un dispositivo de servicios"
OpenStack	Los archivos de disco de máquina virtual y los scripts proporcionados por NetApp para OpenStack ya no son compatibles con las operaciones de recuperación. Si necesita recuperar un nodo que se ejecuta en una implementación de OpenStack, descargue los archivos para su sistema operativo Linux. A continuación, siga el procedimiento para "Reemplazar un nodo Linux" .

Seleccione Iniciar recuperación para configurar el nodo de puerta de enlace

Después de reemplazar un nodo de puerta de enlace, debe seleccionar Iniciar recuperación en el Administrador de red para configurar el nuevo nodo como reemplazo del nodo fallido.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#) .
- Tú tienes el ["Permiso de mantenimiento o acceso root"](#) .
- Tienes la contraseña de aprovisionamiento.
- Ha implementado y configurado el nodo de reemplazo.

Pasos

1. Desde el Administrador de red, seleccione **MANTENIMIENTO > Tareas > Recuperación**.
2. Seleccione el nodo de la cuadrícula que desea recuperar en la lista de Nodos pendientes.

Los nodos aparecen en la lista después de fallar, pero no puedes seleccionar un nodo hasta que se haya reinstalado y esté listo para la recuperación.

3. Introduzca la **contraseña de aprovisionamiento**.
4. Haga clic en **Iniciar recuperación**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

					Search 
	Name	IPv4 Address	State	Recoverable	
☒	104-217-S1	10.96.104.217	Unknown		

Passphrase

Provisioning Passphrase

Start Recovery

5. Supervise el progreso de la recuperación en la tabla Nodo de cuadrícula en recuperación.



Mientras se ejecuta el procedimiento de recuperación, puede hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparece un cuadro de diálogo que indica que el nodo quedará en un estado indeterminado si restablece el procedimiento.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Si desea volver a intentar la recuperación después de restablecer el procedimiento, debe restaurar el nodo a un estado preinstalado, de la siguiente manera:

- **VMware:** eliminar el nodo de red virtual implementado. Luego, cuando esté listo para reiniciar la recuperación, vuelva a implementar el nodo.
- **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 restablecer el procedimiento, debe restaurar el nodo del dispositivo a un estado preinstalado ejecutando `sgareinstall` en el nodo. Ver ["Preparar el dispositivo para la reinstalación \(solo reemplazo de plataforma\)"](#).

Recuperarse de fallos del nodo de archivo

Recuperarse de fallos del nodo de archivo

Se ha eliminado el soporte para nodos de archivo.

Para obtener información sobre cómo recuperar nodos de archivo, consulte ["Recuperación de errores del nodo de archivo \(sitio de documentación de StorageGRID 11.8\)"](#) .

Reemplazar el nodo Linux

Reemplazar el nodo Linux

Si una falla requiere que implemente uno o más hosts físicos o virtuales nuevos o que reinstale Linux en un host existente, implemente y configure el host de reemplazo antes de poder recuperar el nodo de la red. Este procedimiento es un paso del proceso de recuperación del nodo de la red para todos los tipos de nodos de la red.

"Linux" se refiere a una implementación de Red Hat® Enterprise Linux®, Ubuntu® o Debian®. Para obtener una lista de las versiones compatibles, consulte la ["Herramienta de matriz de interoperabilidad de NetApp \(IMT\)"](#) .

Este procedimiento solo se realiza como un paso en el proceso de recuperación de nodos de almacenamiento basados en software, nodos de administración primarios o no primarios o nodos de puerta de enlace. Los pasos son idénticos independientemente del tipo de nodo de red que esté recuperando.

Si hay más de un nodo de red alojado en un host Linux físico o virtual, puede recuperar los nodos de red en cualquier orden. Sin embargo, recuperar primero un nodo de administración principal, si está presente, evita que la recuperación de otros nodos de la red se detenga mientras intentan comunicarse con el nodo de administración principal para registrarse para la recuperación.

Implementar nuevos hosts Linux

Con algunas excepciones, prepare los nuevos hosts como lo hizo durante el proceso de instalación inicial.

Para implementar hosts Linux físicos o virtuales nuevos o reinstalados, siga el procedimiento para preparar los hosts en las instrucciones de instalación de StorageGRID para su sistema operativo Linux:

- ["Instalar Linux \(Red Hat Enterprise Linux\)"](#)
- ["Instalar Linux \(Ubuntu o Debian\)"](#)

Este procedimiento incluye pasos para realizar las siguientes tareas:

1. Instalar Linux.
2. Configurar la red del host.
3. Configurar el almacenamiento del host.
4. Instalar el motor del contenedor.
5. Instalar el servicio de host StorageGRID .



Deténgase después de completar la tarea "Instalar el servicio de host StorageGRID " en las instrucciones de instalación. No inicie la tarea "Implementar nodos de la red".

Al realizar estos pasos, tenga en cuenta las siguientes pautas importantes:

- Asegúrese de utilizar los mismos nombres de interfaz de host que utilizó en el host original.
- Si utiliza almacenamiento compartido para respaldar sus nodos StorageGRID , o ha movido algunas o todas las unidades o SSD de los nodos fallidos a los nodos de reemplazo, debe restablecer las mismas asignaciones de almacenamiento que estaban presentes en el host original. Por ejemplo, si utilizó WWID y alias en `/etc/multipath.conf` Como se recomienda en las instrucciones de instalación, asegúrese de utilizar los mismos pares alias/WWID en `/etc/multipath.conf` en el host de reemplazo.
- Si el nodo StorageGRID usa almacenamiento asignado desde un sistema NetApp ONTAP , confirme que el volumen no tenga habilitada una política de niveles de FabricPool . Deshabilitar la organización en niveles de FabricPool para los volúmenes utilizados con nodos StorageGRID simplifica la resolución de problemas y las operaciones de almacenamiento.



Nunca use FabricPool para agrupar datos relacionados con StorageGRID en StorageGRID mismo. La organización de los datos de StorageGRID en niveles en StorageGRID aumenta la resolución de problemas y la complejidad operativa.

Restaurar los nodos de la red en el host

Para restaurar un nodo de red fallido en un nuevo host Linux, realice estos pasos para restaurar el archivo de configuración del nodo.

1. [Restaurar y validar el nodo](#) restaurando el archivo de configuración del nodo. Para una nueva instalación, se crea un archivo de configuración de nodo para cada nodo de la red que se instalará en un host. Al restaurar un nodo de la red a un host de reemplazo, se restaura o reemplaza el archivo de configuración del nodo para cualquier nodo de la red que haya fallado.
2. [Iniciar el servicio de host de StorageGRID](#) .
3. Según sea necesario, [recuperar cualquier nodo que no pueda iniciarse](#) .

Si se conservaron volúmenes de almacenamiento en bloque del host anterior, es posible que deba realizar procedimientos de recuperación adicionales. Los comandos de esta sección le ayudarán a determinar qué procedimientos adicionales son necesarios.

Restaurar y validar nodos de la red

Debe restaurar los archivos de configuración de la red para cualquier nodo de red fallido y luego validar los archivos de configuración de la red y resolver cualquier error.

Acerca de esta tarea

Puede importar cualquier nodo de la red que deba estar presente en el host, siempre que su `/var/local` El volumen no se perdió como resultado de la falla del host anterior. Por ejemplo, el `/var/local` El volumen aún podría existir si utilizó almacenamiento compartido para los volúmenes de datos del sistema StorageGRID , como se describe en las instrucciones de instalación de StorageGRID para su sistema operativo Linux. Al importar el nodo se restaura su archivo de configuración al host.

Si no es posible importar los nodos faltantes, deberá volver a crear sus archivos de configuración de cuadrícula.

Luego debe validar el archivo de configuración de la red y resolver cualquier problema de red o almacenamiento que pueda ocurrir antes de continuar reiniciando StorageGRID. Al volver a crear el archivo de configuración para un nodo, debe utilizar para el nodo de reemplazo el mismo nombre que se utilizó para el nodo que está recuperando.

Consulte las instrucciones de instalación para obtener más información sobre la ubicación del `/var/local` volumen para un nodo.

- ["Instalar StorageGRID en Red Hat Enterprise Linux"](#)
- ["Instalar StorageGRID en Ubuntu o Debian"](#)

Pasos

1. En la línea de comandos del host recuperado, enumere todos los nodos StorageGRID configurados actualmente: `sudo storagegrid node list`

Si no se configuran nodos de la red, no habrá salida. Si se configuran algunos nodos de la cuadrícula, se espera una salida en el siguiente formato:

Name	Metadata-Volume
=====	
dc1-adm1	/dev/mapper/sgws-adm1-var-local
dc1-gw1	/dev/mapper/sgws-gw1-var-local
dc1-sn1	/dev/mapper/sgws-sn1-var-local
dc1-arc1	/dev/mapper/sgws-arc1-var-local

Si algunos o todos los nodos de la red que deberían configurarse en el host no aparecen en la lista, deberá restaurar los nodos de la red que faltan.

2. Para importar nodos de cuadrícula que tengan una `/var/local` volumen:

- a. Ejecute el siguiente comando para cada nodo que desee importar: `sudo storagegrid node import node-var-local-volume-path`

El `storagegrid node import` El comando solo tiene éxito si el nodo de destino se apagó correctamente en el host en el que se ejecutó por última vez. Si ese no es el caso, 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 que el nodo es propiedad de otro host, ejecute el comando nuevamente con el `--force` bandera para completar la importación: `sudo storagegrid --force node import node-var-local-volume-path`



Cualquier nodo importado con el `--force` La bandera requerirá pasos de recuperación adicionales antes de que puedan volver a unirse a la red, como se describe en "[¿Qué sigue?: Realice pasos de recuperación adicionales, si es necesario](#)".

3. Para los nodos de la red que no tienen una `/var/local` volumen, vuelva a crear el archivo de

configuración del nodo para restaurarlo en el host. Para obtener instrucciones, consulte:

- ["Crear archivos de configuración de nodo para Red Hat Enterprise Linux"](#)
- ["Crear archivos de configuración de nodo para Ubuntu o Debian"](#)



Al volver a crear el archivo de configuración para un nodo, debe utilizar para el nodo de reemplazo el mismo nombre que se utilizó para el nodo que está recuperando. Para las implementaciones de Linux, asegúrese de que el nombre del archivo de configuración contenga el nombre del nodo. Debe 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 deben copiarse al nodo durante la recuperación, lo que podría hacer que la recuperación sea significativamente más rápida (en algunos casos, minutos en lugar de semanas).



Si utiliza nuevos dispositivos de bloque (dispositivos que el nodo StorageGRID no utilizó anteriormente) como valores para cualquiera de las variables de configuración que comienzan con `BLOCK_DEVICE_` Cuando vuelva a crear el archivo de configuración para un nodo, siga las pautas en [Corregir errores de dispositivos de bloque faltantes](#) .

4. Ejecute el siguiente comando en el host recuperado para enumerar todos los nodos StorageGRID .

```
sudo storagegrid node list
```

5. Valide el archivo de configuración de nodo para cada nodo de la red cuyo nombre se mostró en la salida de la lista de nodos de storagegrid:

```
sudo storagegrid node validate node-name
```

Debe abordar cualquier error o advertencia antes de iniciar el servicio de host StorageGRID . Las siguientes secciones brindan más detalles sobre los errores que podrían tener una importancia especial durante la recuperación.

Corregir errores de interfaz de red faltante

Si la red del host no está configurada correctamente o un nombre está mal escrito, se produce un error cuando StorageGRID verifica la asignación especificada en el `/etc/storagegrid/nodes/node-name.conf` archivo.

Es posible que vea un error o una advertencia que coincida con este patrón:

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: GRID_NETWORK_TARGET = <host-interface-name>
      <node-name>: Interface <host-interface-name>' does not exist
```

El error podría informarse para la red de cuadrícula, la red de administración o la red del cliente. Este error significa que el `/etc/storagegrid/nodes/node-name.conf` El archivo asigna la red StorageGRID indicada a la interfaz de host denominada `host-interface-name` , pero no hay ninguna interfaz con ese nombre en el host actual.

Si recibe este error, verifique que haya completado los pasos en ["Implementar nuevos hosts Linux"](#) . Utilice los mismos nombres para todas las interfaces de host que los que se usaron en el host original.

Si no puede nombrar las interfaces de 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 proporcione acceso al puerto de red físico o VLAN apropiado, y que la interfaz no haga referencia directa a un dispositivo de enlace o puente. Debe configurar una VLAN (u otra interfaz virtual) sobre el dispositivo de enlace en el host, o utilizar un puente y un par Ethernet virtual (veth).

Corregir errores de dispositivos de bloque faltantes

El sistema verifica que cada nodo recuperado se asigne a un archivo especial de dispositivo de bloque válido o a un enlace simbólico válido a un archivo especial de dispositivo de bloque. Si StorageGRID encuentra una asignación no válida en el `/etc/storagegrid/nodes/node-name.conf` archivo, se muestra un error de dispositivo de bloque faltante.

Si observa un error que coincide con este patrón:

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: BLOCK_DEVICE_PURPOSE = <path-name>
       <node-name>: <path-name> does not exist
```

Eso significa que `/etc/storagegrid/nodes/node-name.conf` asigna el dispositivo de bloque utilizado por *node-name* para `PURPOSE` a la ruta dada en el sistema de archivos de Linux, pero no hay un archivo especial de dispositivo de bloque válido, o un enlace simbólico a un archivo especial de dispositivo de bloque, en esa ubicación.

Verifique que haya completado los pasos en ["Implementar nuevos hosts Linux"](#) . Utilice los mismos nombres de dispositivos persistentes para todos los dispositivos de bloque que se usaron en el host original.

Si no puede restaurar o recrear el archivo especial del dispositivo de bloque faltante, 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 señalar el nuevo archivo especial del dispositivo de bloque.

Determine el tamaño y la categoría de almacenamiento adecuados utilizando las tablas para su sistema operativo Linux:

- ["Requisitos de almacenamiento y rendimiento para Red Hat Enterprise Linux"](#)
- ["Requisitos de almacenamiento y rendimiento para Ubuntu o Debian"](#)

Revise las recomendaciones para configurar el almacenamiento del host antes de continuar con el reemplazo del dispositivo de bloque:

- ["Configurar el almacenamiento del host para Red Hat Enterprise Linux"](#)
- ["Configurar el almacenamiento del host para Ubuntu o Debian"](#)



Si debe proporcionar un nuevo dispositivo de almacenamiento en bloque para cualquiera de las variables del archivo de configuración que comienzan con `BLOCK_DEVICE_`. Debido a que el dispositivo de bloque original se perdió con el host fallido, asegúrese de que el nuevo dispositivo de bloque no esté formateado antes de intentar otros procedimientos de recuperación. El nuevo dispositivo de bloque no estará formateado si está usando almacenamiento compartido y ha creado un nuevo volumen. Si no está seguro, ejecute el siguiente comando contra cualquier archivo especial del nuevo dispositivo de almacenamiento en bloque.



Ejecute el siguiente comando solo para nuevos dispositivos de almacenamiento en bloque. No ejecute este comando si cree que el almacenamiento en bloque aún contiene datos válidos para el nodo que se está recuperando, 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
```

Iniciar el servicio de host de StorageGRID

Para iniciar los nodos StorageGRID y garantizar que se reinicien después de un reinicio del 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 garantizar que la implementación esté en curso:

```
sudo storagegrid node status node-name
```

3. Si algún nodo devuelve un estado de "No en ejecución" o "Detenido", ejecute el siguiente comando:

```
sudo storagegrid node start node-name
```

4. Si ya ha habilitado e iniciado el servicio de host StorageGRID (o si no está seguro de si el servicio se ha habilitado e iniciado), ejecute también el siguiente comando:

```
sudo systemctl reload-or-restart storagegrid
```

Recuperar nodos que no se inician normalmente

Si un nodo StorageGRID no se reincorpora a la red normalmente y no aparece como recuperable, es posible que esté dañado. Puedes forzar el nodo al modo de recuperación.

Pasos

1. Confirme que la configuración de red del nodo sea correcta.

Es posible que el nodo no haya podido reincorporarse a la red debido a asignaciones de interfaz de red incorrectas o a una dirección IP o puerta de enlace de red incorrecta.

2. Si la configuración de la red es correcta, emita el `force-recovery` dominio:

```
sudo storagegrid node force-recovery node-name
```

3. Realice los pasos de recuperación adicionales para el nodo. Ver "[¿Qué sigue?: Realice pasos de recuperación adicionales, si es necesario](#)".

¿Qué sigue?: Realice pasos de recuperación adicionales, si es necesario

Según las acciones específicas que haya realizado para que los nodos StorageGRID se ejecuten en el host de reemplazo, es posible que deba realizar pasos de recuperación adicionales para cada nodo.

La recuperación del nodo está completa si no fue necesario realizar ninguna acción correctiva mientras reemplazaba el host Linux o restauraba el nodo de red fallido en el nuevo host.

Acciones correctivas y próximos pasos

Durante el reemplazo del nodo, es posible que haya sido necesario tomar una de estas acciones correctivas:

- Tuviste que usar el `--force` bandera para importar el nodo.
- Para cualquier `<PURPOSE>`, el valor de la `BLOCK_DEVICE_<PURPOSE>` La variable del archivo de configuración se refiere a un dispositivo de bloque que no contiene los mismos datos que tenía antes de la falla del host.
- Usted emitió `storagegrid node force-recovery node-name` para el nodo.
- Agregó un nuevo dispositivo de bloque.

Si realizó **alguna** de estas acciones correctivas, deberá realizar pasos de recuperación adicionales.

Tipo de recuperación	Siguiente paso
Nodo de administración principal	"Configurar el nodo de administración principal de reemplazo"
Nodo de administración no principal	"Seleccione Iniciar recuperación para configurar el nodo de administración no principal"
Nodo de puerta de enlace	"Seleccione Iniciar recuperación para configurar el nodo de puerta de enlace"

Tipo de recuperación	Siguiente paso
Nodo de almacenamiento (basado en software): • Si tuviera que usar el <code>--force</code> bandera para importar el nodo, o usted emitió <code>storagegrid node force-recovery node-name</code> • Si tuviera que hacer una reinstalación completa del nodo o necesitara restaurar <code>/var/local</code>	"Seleccione Iniciar recuperación para configurar el nodo de almacenamiento"
Nodo de almacenamiento (basado en software): • Si agregó un nuevo dispositivo de bloque. • Si, por cualquier <code><PURPOSE></code>, el valor de la <code>BLOCK_DEVICE_<PURPOSE></code> La variable del archivo de configuración se refiere a un dispositivo de bloque que no contiene los mismos datos que tenía antes de la falla del host.	"Recuperarse de una falla del volumen de almacenamiento donde la unidad del sistema está intacta"

Reemplazar el nodo VMware

Cuando recupera un nodo StorageGRID fallido que estaba alojado en VMware, elimina el nodo fallido e implementa un nodo de recuperación.

Antes de empezar

Ha determinado que la máquina virtual no se puede restaurar y debe reemplazarse.

Acerca de esta tarea

Utilice VMware vSphere Web Client para eliminar primero la máquina virtual asociada con el nodo de red fallido. Luego, puedes implementar una nueva máquina virtual.

Este procedimiento es solo un paso en el proceso de recuperación del nodo de la red. El procedimiento de eliminación e implementación de nodos es el mismo para todos los nodos de VMware, incluidos los nodos de administración, los nodos de almacenamiento y los nodos de puerta de enlace.

Pasos

1. Inicie sesión en VMware vSphere Web Client.
2. Navegue hasta la máquina virtual del nodo de red fallido.
3. Tome nota de toda la información necesaria para implementar el nodo de recuperación.
 - a. Haga clic con el botón derecho en la máquina virtual, seleccione la pestaña **Editar configuración** y anote las configuraciones en uso.
 - b. Seleccione la pestaña **Opciones de vApp** para ver y registrar la configuración de red del nodo de la cuadrícula.
4. Si el nodo de red fallido es un nodo de almacenamiento, determine si alguno de los discos duros virtuales utilizados para el almacenamiento de datos no está dañado y consérvelos para volver a conectarlos al nodo de red 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 nueva máquina virtual para que sea el nodo de reemplazo y conéctela a una o más redes StorageGRID . Para obtener instrucciones, consulte ["Implementación de un nodo StorageGRID como máquina virtual"](#) .

Al implementar el nodo, puede opcionalmente reasignar los puertos del nodo o aumentar la configuración de CPU o memoria.



Después de implementar el nuevo nodo, puede agregar nuevos discos virtuales según sus requisitos de almacenamiento, volver a conectar cualquier disco duro virtual preservado del nodo de red fallido eliminado anteriormente, o ambas cosas.

8. Complete el procedimiento de recuperación de nodo, según el tipo de nodo que esté recuperando.

Tipo de nodo	Ir a
Nodo de administración principal	"Configurar el nodo de administración principal de reemplazo"
Nodo de administración no principal	"Seleccione Iniciar recuperación para configurar el nodo de administración no principal"
Nodo de puerta de enlace	"Seleccione Iniciar recuperación para configurar el nodo de puerta de enlace"
Nodo de almacenamiento	"Seleccione Iniciar recuperación para configurar el nodo de almacenamiento"

Reemplazar el nodo fallido con un dispositivo de servicios

Reemplazar el nodo fallido con un dispositivo de servicios

Puede usar un dispositivo de servicios para recuperar un nodo de puerta de enlace fallido, un nodo de administración no principal fallido o un nodo de administración principal fallido que estaba alojado en VMware, un host Linux o un dispositivo de servicios. Este procedimiento es un paso del procedimiento de recuperación del nodo de la red.

Antes de empezar

- Ha determinado que una de las siguientes situaciones es verdadera:
 - No se puede restaurar la máquina virtual que aloja el nodo.
 - El host Linux físico o virtual del nodo de la red ha fallado y debe reemplazarse.
 - Se debe reemplazar el dispositivo de servicios que aloja el nodo de la red.
- Ha confirmado que la versión del instalador del dispositivo StorageGRID en el dispositivo de servicios coincide con la versión del software de su sistema StorageGRID . Ver ["Verificar y actualizar la versión del instalador del dispositivo StorageGRID"](#) .



No implemente un dispositivo de servicios SG110 y uno SG1100, ni un dispositivo de servicios SG100 y uno SG1000 en el mismo sitio. Podría producirse un rendimiento impredecible.

Acerca de esta tarea

Puede utilizar un dispositivo de servicios para recuperar un nodo de red fallido en los siguientes casos:

- El nodo fallido estaba alojado en VMware o Linux ("[cambio de plataforma](#)")
- El nodo fallido estaba alojado en un dispositivo de servicios ("[reemplazo de plataforma](#)")

Instalar dispositivo de servicios (solo cambio de plataforma)

Cuando recupera un nodo de red fallido que estaba alojado en VMware o un host Linux y está usando un dispositivo de servicios para el nodo de reemplazo, primero debe instalar el nuevo hardware del dispositivo usando el mismo nombre de nodo (nombre del sistema) que el nodo fallido.

Antes de empezar

Tiene la siguiente información sobre el nodo fallido:

- **Nombre del nodo:** debe instalar el dispositivo de servicios utilizando el mismo nombre de nodo que el nodo fallido. El nombre del nodo es el nombre del host (nombre del sistema).
- **Direcciones IP:** puede asignar al dispositivo de servicios las mismas direcciones IP que el nodo fallido, que es la opción preferida, o puede seleccionar una nueva dirección IP no utilizada en cada red.

Acerca de esta tarea

Realice este procedimiento solo si está recuperando un nodo fallido que estaba alojado en VMware o Linux y lo está reemplazando por un nodo alojado en un dispositivo de servicios.

Pasos

1. Siga las instrucciones para instalar un nuevo dispositivo de servicios. Ver "[Inicio rápido para la instalación de hardware](#)".
2. Cuando se le solicite un nombre de nodo, utilice el nombre del nodo que falló.

Preparar el dispositivo para la reinstalación (solo reemplazo de plataforma)

Al recuperar un nodo de red que estaba alojado en un dispositivo de servicios, primero debe preparar el dispositivo para la reinstalación del software StorageGRID .

Realice este procedimiento solo si está reemplazando un nodo fallido que estaba alojado en un dispositivo de servicios. No siga estos pasos si el nodo fallido originalmente estaba alojado en VMware o en un host Linux.

Pasos

1. Inicie sesión en el nodo de red fallido:
 - a. Introduzca el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
 - c. Introduzca el siguiente comando para cambiar a root: `su -`
 - d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

Cuando inicia sesión como root, el mensaje cambia de `$` a `#` .

2. Prepare el dispositivo para la instalación del software StorageGRID . Ingresar: `sgareinstall`

3. Cuando se le solicite continuar, ingrese: `y`

El dispositivo se reinicia y su sesión SSH finaliza. Por lo general, el instalador del dispositivo StorageGRID tarda unos 5 minutos en estar disponible, aunque en algunos casos es posible que tengas que esperar hasta 30 minutos.

El dispositivo de servicios se reinicia y los datos en el nodo de la red ya no son accesibles. Las direcciones IP configuradas durante el proceso de instalación original deben permanecer intactas; sin embargo, se recomienda que lo confirme una vez completado el procedimiento.

Después de ejecutar el `sgareinstall` comando, se eliminan todas las cuentas, contraseñas y claves SSH proporcionadas por StorageGRID y se generan nuevas claves de host.

Iniciar 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, utilice el instalador de dispositivos StorageGRID , que está incluido en el dispositivo.

Antes de empezar

- El dispositivo está instalado en un rack, conectado a sus redes y encendido.
- Los enlaces de red y las direcciones IP se configuran para el dispositivo mediante el instalador de dispositivos StorageGRID .
- Si está instalando un nodo de puerta de enlace o un nodo de administración no principal, conoce la dirección IP del nodo de administración principal para la red StorageGRID .
- Todas las subredes de la red Grid que aparecen en la página de configuración de IP del instalador del dispositivo StorageGRID se definen en la lista de subredes de la red Grid en el nodo de administración principal.

Ver "[Inicio rápido para la instalación de hardware](#)" .

- Estás usando un "[navegador web compatible](#)" .
- Tiene una de las direcciones IP asignadas al dispositivo. Puede utilizar la dirección IP para la red de administración, la red de cuadrícula o la red de cliente.
- Si está instalando un nodo de administración principal, tendrá disponibles los archivos de instalación de Ubuntu o Debian para esta versión de StorageGRID .



Una versión reciente del software StorageGRID se precarga en el dispositivo de servicios durante la fabricación. Si la versión precargada del software coincide con la versión que se utiliza en su implementación de StorageGRID , no necesita los archivos de instalación.

Acerca de esta tarea

Para instalar el software StorageGRID en un dispositivo de servicios:

- Para un nodo de administración principal, especifique el nombre del nodo y luego cargue los paquetes de software adecuados (si es necesario).
- Para un nodo de administración no principal 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 mientras se configuran los volúmenes y se instala el software.
- A mitad 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 fallido.
- Una vez configurado el nodo, se completa el proceso de instalación del dispositivo y éste se reinicia.

Pasos

1. Abra un navegador e ingrese una de las direcciones IP del dispositivo de servicios.

`https://Controller_IP:8443`

Aparece la página de inicio del instalador del dispositivo StorageGRID .

NetApp® StorageGRID® Appliance Installer Help ▾

Home Configure Networking ▾ Configure Hardware ▾ Monitor Installation Advanced ▾

Home

This Node

Node type Gateway ▾

Node name NetApp-SGA

Cancel Save

Primary Admin Node connection

Enable Admin Node discovery ☒ Uncheck to manually enter the Primary Admin Node IP

Connection state Admin Node discovery is in progress

Cancel Save

Installation

Current state Unable to start installation. The Admin Node connection is not ready.

Start installation

2. Para instalar un nodo de administración principal:
 - a. En la sección Este nodo, para **Tipo de nodo**, seleccione **Administrador principal**.
 - b. En el campo **Nombre del nodo**, ingrese el mismo nombre que se utilizó para el nodo que está recuperando y haga clic en **Guardar**.

- c. En la sección Instalación, verifique la versión del software que aparece en Estado actual

Si la versión del software que está listo para instalar es correcta, salte a la [Paso de instalación](#) .

- d. Si necesita cargar una versión diferente del software, en el menú **Avanzado**, seleccione *Cargar software StorageGRID *.

Aparece la página Cargar software StorageGRID .

NetApp® StorageGRID® Appliance Installer

Help ▾

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Upload StorageGRID Software

If this node is the primary Admin Node of a new deployment, you must use this page to upload the StorageGRID software installation package, unless the version of the software you want to install has already been uploaded. If you are adding this node to an existing deployment, you can avoid network traffic by uploading the installation package that matches the software version running on the existing grid. If you do not upload the correct package, the node obtains the software from the grid's primary Admin Node during installation.

Current StorageGRID Installation Software

Version

None

Package Name

None

Upload StorageGRID Installation Software

Software Package

Browse

Checksum File

Browse

a. Haga clic en **Explorar** para cargar el **Paquete de software** y el **Archivo de suma de comprobación** para el software StorageGRID .

Los archivos se cargan automáticamente después de seleccionarlos.

b. Haga clic en **Inicio** para regresar a la página de inicio del instalador del dispositivo StorageGRID .

3. Para instalar un nodo de puerta de enlace o un nodo de administración no principal:

a. En la sección Este nodo, para **Tipo de nodo**, seleccione **Puerta de enlace** o **Administrador no principal**, según el tipo de nodo que esté restaurando.

b. En el campo **Nombre del nodo**, ingrese el mismo nombre que se utilizó para el nodo que está recuperando y haga clic en **Guardar**.

c. En la sección de conexión del nodo de administración principal, determine si necesita especificar la dirección IP para el nodo de administración principal.

El instalador del dispositivo StorageGRID puede descubrir esta dirección IP automáticamente, suponiendo que el nodo de administración principal, o al menos otro nodo de la red con ADMIN_IP configurado, esté presente en la misma subred.

d. Si esta dirección IP no se muestra o necesita cambiarla, especifique la dirección:

1632

Opción	Descripción
Entrada manual de IP	a. Desmarque la casilla de verificación Habilitar descubrimiento de nodo de administración. b. Introduzca la dirección IP manualmente. c. Haga clic en Guardar. d. Espere mientras el estado de conexión de la nueva dirección IP pasa a ser "listo".
Descubrimiento automático de todos los nodos de administración principales conectados	a. Seleccione la casilla de verificación Habilitar descubrimiento de nodo de administración. b. De la lista de direcciones IP descubiertas, seleccione el nodo de administración principal para la red donde se implementará este dispositivo de servicios. c. Haga clic en Guardar. d. Espere mientras el estado de conexión de la nueva dirección IP pasa a ser "listo".

4. En la sección Instalación, confirme que el estado actual sea Listo para iniciar la instalación del nombre del nodo y que el botón **Iniciar instalación** esté habilitado.

Si el botón **Iniciar instalación** no está habilitado, es posible que necesite cambiar la configuración de red o la configuración del puerto. Para obtener instrucciones, consulte las instrucciones de mantenimiento de su aparato.

5. Desde la página de inicio del instalador del dispositivo StorageGRID , haga clic en **Iniciar instalación**.

El estado actual cambia a "La instalación está en curso" y se muestra la página de instalación del monitor.



Si necesita acceder manualmente a la página de instalación del monitor, haga clic en **Instalación del monitor** en la barra de menú.

Instalación de dispositivos de servicios de monitorización

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 **Supervisar instalación** en la barra de menú.

La página de instalación del monitor muestra el progreso de la instalación.

Monitor Installation

1. Configure storage		Complete
2. Install OS		Running
Step	Progress	Status
Obtain installer binaries		Complete
Configure installer		Complete
Install OS		Installer VM running
3. Install StorageGRID		Pending
4. Finalize installation		Pending

La barra de estado azul indica qué tarea está actualmente en progreso. Las barras de estado verdes indican tareas que se han completado correctamente.



El instalador garantiza que las tareas completadas en una instalación anterior no se vuelvan a ejecutar. Si está volviendo a ejecutar una instalación, cualquier tarea que no necesite volver a ejecutarse se mostrará con una barra de estado verde y un estado de "Omitido".

2. Revise el progreso de las dos primeras etapas de instalación.

◦ 1. Configurar almacenamiento

Durante esta etapa, el instalador borra cualquier configuración existente de las unidades y configura los ajustes del host.

◦ 2. Instalar sistema operativo

Durante esta etapa, 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 para el nodo de administración principal.

3. Continúe monitoreando el progreso de la instalación hasta que ocurra uno de los siguientes eventos:

- En el caso de los nodos de puerta de enlace del dispositivo o los nodos de administración del dispositivo no principal, la etapa **Instalar StorageGRID** se pausa y aparece un mensaje en la consola integrada que le solicita que apruebe este nodo en el nodo de administración mediante el Administrador de Grid.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

- Para los nodos de administración principales del dispositivo, aparece una quinta fase (Cargar instalador de StorageGRID). Si la quinta fase está en curso durante más de 10 minutos, actualice la página manualmente.

NetApp® StorageGRID® Appliance Installer
Help

Home
Configure Networking
Configure Hardware
Monitor Installation
Advanced

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Complete
4. Finalize installation	Complete
5. Load StorageGRID Installer	Running

Step	Progress	Status
Starting StorageGRID Installer		Do not refresh. You will be redirected when the installer is ready

4. Vaya al siguiente paso del proceso de recuperación para el tipo de nodo de red del dispositivo que está recuperando.

Tipo de recuperación	Referencia
Nodo de puerta de enlace	" Seleccione Iniciar recuperación para configurar el nodo de puerta de enlace "
Nodo de administración no principal	" Seleccione Iniciar recuperación para configurar el nodo de administración no principal "
Nodo de administración principal	" Configurar el nodo de administración principal de reemplazo "

Cómo el soporte técnico recupera un sitio

Si falla un sitio completo de StorageGRID o si fallan varios nodos de almacenamiento, debe comunicarse con el soporte técnico. El soporte técnico evaluará su situación, desarrollará un plan de recuperación y luego recuperará los nodos o el sitio fallidos de una manera que cumpla con sus objetivos comerciales, optimice el tiempo de recuperación y evite la pérdida innecesaria de datos.

!

La recuperación del sitio sólo puede ser realizada por soporte técnico.

Los sistemas StorageGRID son resistentes a una amplia variedad de fallas, y usted mismo puede realizar con éxito muchos procedimientos de recuperación y mantenimiento. Sin embargo, es difícil crear un procedimiento de recuperación del sitio simple y generalizado porque los pasos detallados dependen de factores específicos de su situación. Por ejemplo:

- Sus objetivos comerciales:** después de la pérdida total de un sitio de StorageGRID , debe evaluar cuál es la mejor manera de cumplir con sus objetivos comerciales. Por ejemplo, ¿quieres reconstruir el sitio perdido en el lugar? ¿Desea reemplazar el sitio StorageGRID perdido en una nueva ubicación? La situación de cada cliente es diferente y su plan de recuperación debe estar diseñado para abordar sus prioridades.

- **Naturaleza exacta de la falla:** antes de comenzar una recuperación del sitio, establezca si alguno de los nodos en el sitio fallido está intacto o si algún nodo de almacenamiento contiene objetos recuperables. Si reconstruye nodos o volúmenes de almacenamiento que contienen datos válidos, podría producirse una pérdida de datos innecesaria.
- **Políticas ILM activas:** la cantidad, el tipo y la ubicación de las copias de objetos en su cuadrícula están controlados por sus políticas ILM activas. Los detalles de sus políticas 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 del bucket (o contenedor):** la consistencia aplicada a un bucket (o contenedor) afecta si StorageGRID replica completamente los metadatos del objeto a todos los nodos y sitios antes de informar a un cliente que la ingesta del objeto fue exitosa. Si el valor de consistencia permite una consistencia eventual, es posible que se hayan perdido algunos metadatos del objeto en la falla del sitio. Esto puede afectar la cantidad de datos recuperables y potencialmente los detalles del procedimiento de recuperación.
- **Historial de cambios recientes:** Los detalles de su procedimiento de recuperación pueden verse afectados por si había algún procedimiento de mantenimiento en curso en el momento de la falla o si se realizaron cambios recientes en sus políticas de ILM. El soporte técnico debe evaluar el historial reciente de su red así como su situación actual antes de comenzar la recuperación del sitio.



La recuperación del sitio sólo puede ser realizada por soporte técnico.

Esta es una descripción general del proceso que utiliza el soporte técnico para recuperar un sitio fallido:

1. Apoyo técnico:
 - a. Realiza una evaluación detallada del fallo.
 - b. Trabaja con usted para revisar sus objetivos comerciales.
 - c. Desarrolla un plan de recuperación adaptado a su situación.
2. Si el nodo de administración principal ha fallado, el soporte técnico lo recupera.
3. El soporte técnico recupera todos los nodos de almacenamiento, siguiendo este esquema:
 - a. Reemplace el hardware del nodo de almacenamiento o las máquinas virtuales según sea necesario.
 - b. Restaurar los metadatos del objeto en el sitio fallido.
 - c. Restaurar datos de objetos en los nodos de almacenamiento recuperados.



Se producirá pérdida de datos si se utilizan los procedimientos de recuperación para un solo nodo de almacenamiento fallido.



Cuando falla un sitio completo, el soporte técnico utiliza comandos especializados para restaurar exitosamente los objetos y los metadatos de los objetos.

4. El soporte técnico recupera otros nodos fallidos.

Una vez recuperados los metadatos y datos de los objetos, el soporte técnico utiliza procedimientos estándar para recuperar nodos de puerta de enlace fallidos o nodos de administración no primarios.

Información relacionada

["Desmantelamiento del sitio"](#)

Cómo habilitar StorageGRID en su entorno

Ir a ["Cómo habilitar StorageGRID"](#) para aprender a probar y habilitar aplicaciones en su entorno StorageGRID .

Cómo administrar StorageGRID mediante la consola de NetApp

Ir a ["Administración de StorageGRID mediante la consola de NetApp"](#) para aprender a administrar sus sistemas StorageGRID desde la consola de NetApp usando Grid Manager y usar los servicios de datos de la consola de NetApp para copias de seguridad, niveles de datos y más.

- BlueXP ahora es NetApp Console*

La consola NetApp , construida sobre la base BlueXP mejorada y reestructurada, proporciona una gestión centralizada del almacenamiento NetApp y de los servicios de datos NetApp en entornos locales y en la nube a nivel empresarial, brindando información en tiempo real, flujos de trabajo más rápidos y una administración simplificada, que es altamente segura y compatible.

Para obtener más detalles sobre lo que ha cambiado, consulte la ["Notas de la versión de la consola de NetApp"](#) .

Avisos legales

Los avisos legales proporcionan acceso a declaraciones de derechos de autor, marcas comerciales, patentes y más.

Copyright

["https://www.netapp.com/company/legal/copyright/"](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. Otros nombres de empresas y productos pueden ser marcas comerciales de sus respectivos propietarios.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patentes

Puede encontrar una lista actualizada 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/"](https://www.netapp.com/company/legal/privacy-policy/)

Código abierto

Los archivos de aviso proporcionan información sobre derechos de autor y licencias de terceros utilizados en el software de NetApp .

https://library.netapp.com/ecm/ecm_download_file/ECMLP3330669

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.