



Documentación del software StorageGRID 12.0

StorageGRID software

NetApp
August 05, 2026

This PDF was generated from <https://docs.netapp.com/es-es/storagegrid-120/index.html> on August 05, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Documentación del software StorageGRID 12.0	1
Conoce el hardware de los dispositivos StorageGRID	2
Notas de publicación	3
Novedades de StorageGRID 12.0	3
Dispositivos	3
Inteligencia artificial (IA) y aprendizaje automático (ML)	3
Capacidad	3
Actualizaciones de Cassandra	3
Federación	3
Facilidad de gestión	4
Seguridad	4
Grupos de inquilinos	4
Interfaz de usuario	5
Funciones y capacidades eliminadas o en desuso en StorageGRID	5
Definiciones	5
Fin del soporte de funciones de StorageGRID	5
Cambios en la API de gestión de Grid en StorageGRID	7
Nuevos endpoints para los buckets de sucursales	7
Nuevos endpoints privados para Move ADC	7
Nuevos puntos finales privados para convertir a nodo de solo datos	8
Cambios en la API de gestión de inquilinos en StorageGRID	8
Nueva API para la replicación de objetos	8
Empieza a utilizar un sistema StorageGRID	9
Conoce StorageGRID	9
¿Qué es StorageGRID?	9
Nubes híbridas con StorageGRID	11
Arquitectura de StorageGRID y topología de red	12
Nodos y servicios de grid	15
Cómo gestiona StorageGRID los datos	28
Descubre StorageGRID	40
Directrices de redes	48
Directrices de red para StorageGRID	48
Tipos de redes StorageGRID	49
Ejemplos de topología de red	53
Requisitos de red para StorageGRID	59
Requisitos específicos de red para StorageGRID	61
Consideraciones sobre redes específicas de la implementación	63
Instalación y aprovisionamiento de red para StorageGRID	66
Directrices posteriores a la instalación para StorageGRID	67
Referencia de puertos de red	68
Guía de inicio rápido de StorageGRID	77
Instalar, actualizar y aplicar corrección urgente a StorageGRID	80
Instala nodos StorageGRID	80

Conoce el hardware de los dispositivos StorageGRID	80
Instala nodos basados en software	80
Configura la grid y completa la instalación	188
Conoce los pasos obligatorios y opcionales después de instalar StorageGRID	202
Actualizar el software StorageGRID	203
Actualizar el software StorageGRID	203
Planifica y prepárate para la actualización	203
Actualizar software	210
Soluciona problemas de actualización de StorageGRID	227
Aplicar la corrección urgente de StorageGRID	229
Procedimiento de corrección urgente de StorageGRID	229
Cómo se ve afectado StorageGRID cuando aplicas una corrección urgente	230
Obtén los materiales necesarios para una corrección urgente de StorageGRID	231
Descarga un archivo de corrección urgente de StorageGRID	232
Comprueba el estado del sistema antes de aplicar una corrección urgente de StorageGRID	233
Aplica una corrección urgente en StorageGRID	233
Configurar y gestionar un sistema StorageGRID	238
Administrar StorageGRID	238
Administrar StorageGRID	238
Empieza a utilizar Grid Manager	238
Controlar el acceso a StorageGRID	266
Usa la federación de grid	312
Gestiona la seguridad	350
Gestiona inquilinos	423
Configura las conexiones de los clientes	443
Gestiona redes y conexiones	487
Usa AutoSupport	507
Gestionar nodos de almacenamiento	522
Gestionar nodos de administración	535
Gestiona objetos con ILM	537
Administra objetos con ILM en StorageGRID	537
ILM y el ciclo de vida de los objetos	538
Crea y asigna grados de almacenamiento en StorageGRID	561
Usa grupos de almacenamiento	563
Usa grupos de almacenamiento en la nube	571
Administra los perfiles de código de borrado en StorageGRID	592
Configura las regiones de S3 para StorageGRID	595
Crear regla de ILM	597
Gestiona las políticas de ILM	615
Trabaja con políticas ILM y reglas ILM en StorageGRID	631
Usa S3 Object Lock	635
Ejemplos de reglas y políticas de ILM	643
Refuerzo del sistema para StorageGRID	665
Conoce el endurecimiento del sistema para StorageGRID	665
Directrices de refuerzo para las actualizaciones de software de StorageGRID	666

Directrices de refuerzo de la seguridad para redes StorageGRID	667
Directrices de refuerzo de la seguridad para los nodos de StorageGRID	668
Directrices de endurecimiento para TLS y SSH en StorageGRID	672
Directrices de refuerzo para logs, contraseñas y mensajes de auditoría en StorageGRID	673
StorageGRID con FabricPool	674
Flujo de trabajo de configuración para usar StorageGRID con FabricPool	674
Información necesaria para adjuntar StorageGRID como un nivel de nube FabricPool	676
Utiliza el asistente de configuración de FabricPool	677
Configura StorageGRID manualmente	691
Configura ONTAP System Manager para añadir StorageGRID como un cloud tier FabricPool	702
Configura las entradas del servidor DNS para StorageGRID con FabricPool	703
Mejores prácticas de StorageGRID para FabricPool	704
Eliminar datos de FabricPool de StorageGRID	708
Usa inquilinos y clientes de StorageGRID	710
Utiliza una cuenta de inquilino	710
Utiliza una cuenta de StorageGRID	710
Cómo iniciar y cerrar sesión	711
Panel de control de Tenant Manager en StorageGRID	713
API de gestión de inquilinos	716
Usa conexiones de federación de grid	721
Gestiona grupos y usuarios	734
Gestiona claves de acceso de S3	753
Gestiona buckets de S3	758
Gestiona los servicios de la plataforma S3	788
Usa la API de REST de S3	822
Versiones compatibles y actualizaciones de la API de REST de StorageGRID S3	822
Solicitudes de API de S3 compatibles en StorageGRID	826
Prueba la configuración de la API de REST de StorageGRID S3	845
Cómo implementa StorageGRID la API de REST de S3	846
Compatibilidad con la API de REST de Amazon S3	862
Operaciones personalizadas de StorageGRID	914
Gestiona las políticas de acceso	935
Operaciones S3 registradas en los registros de auditoría de StorageGRID	963
Usa la API de REST de Swift (fin de vida útil)	964
Compatibilidad con la API de REST de Swift en StorageGRID	964
Supervisar y solucionar problemas en un sistema StorageGRID	965
Supervisa el sistema StorageGRID	965
Supervisa un sistema StorageGRID	965
Ver y gestionar el panel de control en StorageGRID	965
Ver la página Nodes	968
Información que debes supervisar regularmente	1001
Gestiona alertas	1031
Referencia de los archivos de registro	1070
Configura la gestión de registros y el servidor syslog externo	1090
Usa la supervisión SNMP	1104

Recopila datos adicionales de StorageGRID	1117
Soluciona problemas del sistema StorageGRID	1130
Soluciona problemas en un sistema StorageGRID	1130
Soluciona problemas de objetos y almacenamiento	1137
Soluciona problemas de metadatos en StorageGRID	1156
Soluciona errores de certificado en StorageGRID	1158
Soluciona problemas del nodo de administración y de la interfaz de usuario en StorageGRID	1160
Soluciona problemas de red, hardware y plataforma en StorageGRID	1163
Soluciona los mensajes de error del servidor syslog externo para StorageGRID	1171
Conoce los problemas de almacenamiento en caché del equilibrador de carga en StorageGRID	1174
Revisar los registros de auditoría	1175
Mensajes y registros de auditoría	1175
Cómo los mensajes de auditoría se mueven a través del sistema StorageGRID hasta el archivo audit.log para su retención	1176
Accede a los archivos de registro de auditoría desde la línea de comandos del nodo de administración de StorageGRID	1179
Conoce la rotación de archivos de registro de auditoría en StorageGRID	1180
Formato del archivo de registro de auditoría	1181
Formato de mensaje de auditoría	1193
Mensajes de auditoría y el ciclo de vida de los objetos	1198
Mensajes de auditoría	1204
Amplía la capacidad o las capacidades de tu sistema StorageGRID	1252
Descubre cómo ampliar tu sistema StorageGRID	1252
Planificación de la expansión	1253
Planificación de la ampliación de los datos replicados en StorageGRID	1253
Planificación de la expansión para datos con código de borrado (EC) en StorageGRID	1254
Infórmate sobre el reequilibrio de EC tras la expansión en StorageGRID	1255
Directrices de expansión	1259
Directrices para añadir capacidad de objetos en StorageGRID	1259
Directrices para ampliar la capacidad de metadatos en StorageGRID	1261
Directrices para añadir nodos de grid en StorageGRID	1263
Guía para añadir un nuevo sitio en StorageGRID	1264
Prepárate para ampliar tu sistema StorageGRID	1264
Descarga y descomprime los archivos de instalación de StorageGRID	1265
Verifica el hardware y la red	1271
Agregar nodos de grid o sitio	1272
Resumen del flujo de trabajo para añadir nodos de grid o nuevos sitios a StorageGRID	1272
Agrega o actualiza subredes a la Grid Network para expansión en StorageGRID	1272
Implementar nuevos nodos de grid en StorageGRID	1274
Realiza una ampliación de StorageGRID	1278
Agregar volúmenes de almacenamiento	1283
Agrega volúmenes de almacenamiento a tu sistema StorageGRID	1283
Agrega volúmenes de almacenamiento a los nodos de almacenamiento de VMware en StorageGRID	1286
Agrega volúmenes directos o SAN a los nodos de almacenamiento Linux en StorageGRID	1287
Configura el sistema ampliado	1291

Configura los nodos y sitios recién añadidos en StorageGRID	1291
Comprueba que los nodos de almacenamiento estén activos tras una ampliación de StorageGRID ..	1293
Copia la base de datos del nodo de administración a los nuevos nodos de administración en StorageGRID	1293
Copia las métricas de Prometheus a los nuevos nodos de administración en StorageGRID	1294
Copia los registros de auditoría en los nuevos nodos de administración en StorageGRID	1296
Reequilibra los datos con código de borrado tras añadir nodos a tu sistema StorageGRID	1298
Solucionar errores de expansión en StorageGRID	1300
Mantén un sistema StorageGRID	1302
Mantenimiento de grid de StorageGRID	1302
Antes de empezar	1302
Procedimientos de mantenimiento para los appliances	1302
Descarga el paquete de recuperación StorageGRID	1302
Decomisionar nodos o sitio	1303
Decomisionar un nodo o sitio de StorageGRID	1303
Decomisionar nodos	1303
Descomisionar sitio	1323
Cambiar el nombre de una grid, un sitio o un nodo	1346
Usa el procedimiento de cambio de nombre de StorageGRID	1346
Agrega o actualiza los nombres de visualización de StorageGRID	1350
Procedimientos de nodo	1356
Procedimientos de mantenimiento de nodos StorageGRID	1356
Mover el servicio ADC en StorageGRID	1357
Convertir un nodo de almacenamiento StorageGRID en un nodo solo de datos	1358
Procedimientos de reinicio, apagado y encendido	1359
Procedimientos de reasignación de puertos	1372
Procedimientos de Administrador de servidores	1375
Procedimientos de red	1384
Actualiza las subredes para la red Grid de StorageGRID	1384
Configurar direcciones IP	1386
Agrega interfaces a un nodo existente	1405
Configura servidores DNS en StorageGRID	1409
Modificar la configuración de DNS para un único nodo StorageGRID	1410
Administra los servidores NTP en StorageGRID	1412
Restaura la conectividad de red para nodos StorageGRID aislados	1413
Procedimientos de host y middleware	1415
Migra un nodo StorageGRID a un nuevo host Linux	1415
Configura una máquina virtual VMware para reinicio automático en StorageGRID	1417
Recuperar o sustituir nodos	1418
Advertencias y consideraciones para la recuperación de nodos de StorageGRID	1418
Condiciones previas para la recuperación de los nodos de la red	1418
Orden de recuperación de nodos si falla un servidor que aloja más de un nodo de la red	1419
Direcciones IP de los nodos recuperados	1419
Reúne los materiales necesarios para la recuperación de nodos de grid de StorageGRID	1419
Descargar y descomprimir los archivos de instalación de StorageGRID	1420

Selecciona el procedimiento de recuperación del nodo StorageGRID	1427
Recupérate de fallos en los nodos de almacenamiento	1427
Recupera de fallos en el nodo de almacenamiento StorageGRID	1428
Recuperar el nodo de almacenamiento del appliance	1429
Recupérate de un fallo del volumen de almacenamiento cuando la unidad del sistema está intacta ..	1448
Recupera tu sistema tras un fallo de unidad	1462
Restaura datos de objetos usando StorageGRID Grid Manager	1480
Supervisa los trabajos de reparación de StorageGRID	1484
Recupérate de fallos del nodo de administración	1486
Recuperación del nodo de administración primario o no primario en StorageGRID	1486
Recupérate de fallos del nodo de administración principal	1486
Recupérate de fallos del nodo de administración no principal	1495
Recupera ante fallos del nodo de puerta de enlace	1503
Reemplazar nodo StorageGRID Gateway	1503
Selecciona Iniciar recuperación para configurar el nodo StorageGRID Gateway	1504
Recupera tras fallos en los nodos de archivo	1506
Recupera de fallos del nodo de archivo StorageGRID	1506
Reemplazar nodo Linux	1506
Reemplazar un nodo Linux en StorageGRID	1506
Implementa nuevos hosts Linux para StorageGRID	1506
Restaura los nodos StorageGRID en el host	1507
Realiza los pasos adicionales de recuperación del nodo StorageGRID	1512
Reemplazar un nodo VMware en StorageGRID	1513
Sustituye el nodo averiado por un dispositivo de servicios	1514
Reemplaza el nodo StorageGRID fallido con un dispositivo de servicios	1514
Instala el dispositivo de servicios StorageGRID (solo cambio de plataforma)	1515
Prepara el dispositivo StorageGRID para la reinstalación (solo reemplazo de plataforma)	1515
Inicia la instalación del software StorageGRID en un dispositivo de servicios	1516
Supervisa la instalación del dispositivo de servicios StorageGRID	1518
Cómo el soporte técnico recupera un sitio StorageGRID	1519
Soluciones y recursos de StorageGRID	1522
Cómo gestionar StorageGRID con NetApp Console	1523
Avisos legales	1524
Copyright	1524
Marcas registradas	1524
Patentes	1524
Política de privacidad	1524
Licencia de la API	1524
Código abierto	1524

Documentación del software StorageGRID 12.0

Conoce el hardware de los dispositivos StorageGRID

Ve a "[Documentación de StorageGRID Appliance](#)" para aprender a instalar, configurar y mantener los dispositivos de almacenamiento y servicios de StorageGRID.

Notas de publicación

Novedades de StorageGRID 12.0

StorageGRID 12.0 amplía la capacidad de almacenamiento de objetos, mejora la compatibilidad con cargas de trabajo AI/ML, refuerza la federación de grid, simplifica la administración de sistemas y mejora la seguridad en toda la plataforma.

Para obtener más información sobre los problemas solucionados y los problemas conocidos de las últimas versiones de StorageGRID 12.0, consulta ["StorageGRID 12.0 Notas de la versión"](#). Debes iniciar sesión con tu cuenta de NetApp o crear una cuenta para acceder a las notas de la versión.

Dispositivos

- La capacidad de almacenamiento y la rentabilidad han aumentado considerablemente.
- Las actualizaciones automáticas del firmware de las unidades mejoran la fiabilidad del sistema y reducen la carga de mantenimiento.

Inteligencia artificial (IA) y aprendizaje automático (ML)

- ["Cubos para ramas"](#) Permite versiones de los buckets en un momento específico que facilitan una recuperación más rápida ante ransomware y conjuntos de datos aislados para pruebas y experimentación.
- Una capa de almacenamiento en caché de S3 mejora el rendimiento del entrenamiento de IA/ML.

Capacidad

StorageGRID admite ahora un billón de objetos, lo que supone más del doble del límite anterior. Consulta la ["Herramienta NetApp Fusion"](#) para dimensionar y diseñar StorageGRID.

Actualizaciones de Cassandra

StorageGRID utiliza ahora una versión más reciente de Cassandra para el almacenamiento de metadatos. Esta versión de Cassandra aprovecha el espacio en disco de forma más eficiente para almacenar más metadatos.

Una vez que hayas ["Actualiza de StorageGRID 11.9 a 12.0"](#), se realizará una actualización del formato de metadatos en segundo plano durante uno a tres días. Durante este tiempo, ciertos procedimientos de mantenimiento que implican la transmisión de metadatos, como la expansión, estarán deshabilitados.

Consulta ["Actualizar otros nodos"](#).

Federación

- Ahora puedes ["Importar hasta 100 usuarios federados"](#) en StorageGRID.
- Ahora puedes ["modificar la región predeterminada"](#) para los buckets de S3. Esta función ofrece una mayor flexibilidad a la hora de gestionar la ubicación de los datos y el cumplimiento normativo.
- Ahora puedes configurar la replicación entre grids entre buckets con S3 Object Lock activado. Consulta ["Replicación entre grids con S3 Object Lock"](#).

NetApp recomienda usar esta función solo entre buckets de origen y destino de StorageGRID 12.0. Sin

embargo, esta función es compatible entre buckets de origen de StorageGRID 11.9 con S3 Object Lock desactivado y buckets de destino de StorageGRID 12.0 con S3 Object Lock activado.

Facilidad de gestión

- La versión mejorada de ["procedimiento para decomisionar"](#) reduce el tiempo y la complejidad para mejorar la eficiencia operativa.
- La mejora en el comportamiento de la consistencia global fuerte proporciona tolerancia ante fallo del sitio para las solicitudes de los clientes cuando las grids cuentan con tres o más sitios.
 - Las nuevas instalaciones de StorageGRID 12.0 y versiones posteriores usarán por defecto la semántica de quórum cuando ["consistencia global fuerte"](#) esté configurado.
 - Si actualizas de StorageGRID 11.9 a StorageGRID 12.0, las grids actualizadas mantendrán el comportamiento anterior para la consistencia strong-global.



Si necesitas volver al comportamiento anterior para strong-global consistency, consulta ["Configurar la semántica de quórum de StorageGRID para una consistencia global fuerte"](#) para obtener instrucciones.

- La posibilidad de iniciar la carga de registros en ["AutoSupport"](#) ayuda a mejorar la capacidad de respuesta del soporte.
- El tiempo de reinicio reducido ["appliance"](#) minimiza el tiempo de inactividad para mejorar la disponibilidad general del sistema.
- ["La posibilidad de trasladar el servicio ADC"](#) El traslado a otro nodo de almacenamiento aumenta la flexibilidad y la resiliencia en la gestión de los nodos de almacenamiento que alojan el servicio ADC. Puedes mover el servicio ADC antes de decomisionar un nodo de almacenamiento o convertir un nodo de almacenamiento en un nodo solo de datos.
- Para maximizar la capacidad de almacenamiento de datos, puedes ["Convertir un nodo de almacenamiento en un nodo solo de datos"](#), lo que hace que los metadatos de ese nodo se migren a nodos de almacenamiento combinados o solo de metadatos.
- La posibilidad de que cualquier nodo de administración pueda ["recuperar cualquier otro nodo"](#) (excepto el nodo de administración principal) mejora la recuperación del sistema y la tolerancia a fallos, lo que aumenta la fiabilidad general.
- Los usuarios ya pueden utilizar un depósito de S3 para ["almacenar los registros de auditoría durante un largo periodo de tiempo"](#).

Seguridad

- Un cifrado de datos más sólido y una mayor protección de la integridad ofrecen mayor seguridad y mejor rendimiento.
- Una mayor seguridad de las contraseñas almacenadas reduce el riesgo de acceso no autorizado.
- ["SSH está bloqueado de forma predeterminada"](#) para mejorar la seguridad mientras permites un acceso controlado.

Grupos de inquilinos

- Ahora puedes ["configurar una nueva política de confianza de S3"](#) para admitir la API de AssumeRole. La función AssumeRole proporciona credenciales de corta duración para mayor seguridad y control de acceso flexible.

- El límite de número de objetos por bucket permite un mejor control y gestión de los recursos de almacenamiento.

Interfaz de usuario

- Las opciones de tema oscuro y tema del sistema están disponibles en el menú de usuario de Grid Manager y Tenant Manager.
- La página del servidor de auditoría y syslog, renombrada "[Gestión de registros](#)", se ha rediseñado, con añadidos para almacenar los registros en un bucket del sistema para fines de copia de seguridad.
- Se ha eliminado la página «Topología de la red» (Grid Topology). A lo largo de las últimas versiones de StorageGRID, las operaciones y métricas disponibles en esa página se han migrado a otras páginas del Grid Manager, concretamente a la "[Página de nodos](#)".

Funciones y capacidades eliminadas o en desuso en StorageGRID

Conoce las características y capacidades que han sido eliminadas o desaprobadas en StorageGRID 12.0. Antes de actualizar, revisa si alguna característica eliminada o desaprobadada afecta a tus aplicaciones cliente o a la configuración de tu grid.

Definiciones

En desuso

Esta función **no debe** utilizarse en nuevos entornos de producción. Los entornos de producción existentes pueden seguir utilizando esta función.

Fin de la vida útil

Última versión lanzada que admite esta función. En algunos casos, la documentación de la función podría eliminarse en esta etapa.

Eliminado

Primera versión que **no** admite esta función.

Fin del soporte de funciones de StorageGRID

Las funciones obsoletas se eliminarán en las versiones principales N+2. Por ejemplo, si una función queda obsoleta en la versión N (por ejemplo, 6.3), la última versión en la que la función existirá es la N+1 (por ejemplo, 6.4). La versión N+2 (por ejemplo, 6.5) es la primera versión en la que la función ya no existe en el producto.

Consulta la "[Página de soporte de versiones de software](#)" para obtener información adicional.



En determinadas situaciones, NetApp podría dejar de ofrecer soporte para determinadas funciones antes de lo indicado.

Característica	En desuso	Fin de la vida útil	Eliminado	Enlaces a documentación anterior
Alarmas, heredadas (<i>no Alertas</i>)	11,7	11,8	11,9	"Referencia de alarmas (StorageGRID 11.8)"
Compatibilidad con nodos de archivo	11,7	11,8	11,9	"Aspectos a tener en cuenta para la descomisión de los nodos de archivo (StorageGRID 11.8)" Nota: Antes de iniciar tu actualización, debes: 1. Decomisiona todos los nodos de archivo. Consulta "Decomisionar un nodo de grid (sitio de documentación de StorageGRID 11.8)". 2. Elimina todas las referencias a los nodos de archivo de los grupos de almacenamiento y las políticas de ILM. Consulta "NetApp base de conocimientos: guía de resolución para 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	El soporte para Docker como motor de contenedores para implementaciones exclusivamente de software ha quedado obsoleto. Docker será sustituido por otro motor de contenedores en una futura versión. Consulta la "Requisitos de software para los nodos basados en software" para ver una lista de las versiones de Docker compatibles actualmente.
Configuración del correo electrónico (legacy)	11,9	12,0	12,1	"Configura notificaciones para alarmas (sistema heredado) (StorageGRID 11.8)"
Exportación de auditoría de NFS	11,8	11,9	12,0	"Configura el acceso de clientes de auditoría para NFS (StorageGRID 11.8)"

Característica	En desuso	Fin de la vida útil	Eliminado	Enlaces a documentación anterior
Reasignación de puertos	12,0	12,1	12,2	
Compatibilidad con la API de Swift	11,7	11,9	12,0	"Usa la API de 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	
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	

Consulta también:

- ["Cambios en la API de gestión de grid"](#)
- ["Cambios en la API de gestión de inquilinos"](#)

Cambios en la API de gestión de Grid en StorageGRID

StorageGRID 12.0 utiliza la versión 4 de la API de gestión de Grid. La versión 4 sustituye a la versión 3; sin embargo, las versiones 1, 2 y 3 siguen siendo compatibles.



Puedes seguir utilizando las versiones obsoletas de la API de gestión con StorageGRID 12.0; sin embargo, el soporte para estas versiones de la API se eliminará en una futura versión de StorageGRID. Después de actualizar a StorageGRID 12.0, puedes desactivar las API obsoletas usando la API PUT `/grid/config/management`.

Para obtener más información, visita ["Usa la API de gestión de Grid"](#).

Nuevos endpoints para los buckets de sucursales

Se han añadido los siguientes puntos finales para que puedas ["gestionar los buckets de las ramas"](#):

```
GET /org/containers/{branchBucketName}/branch
```

```
PUT /org/containers/{branchBucketName}/branch
```

Nuevos endpoints privados para Move ADC

Se han añadido los siguientes puntos finales privados para que puedas ["trasladar el servicio ADC"](#) de un nodo

de almacenamiento a otro dentro del mismo sitio:

```
/private/move-adc
```

```
/private/move-adc/start
```

```
/private/move-adc/retry
```

Nuevos puntos finales privados para convertir a nodo de solo datos

Se han añadido los siguientes puntos finales privados para que puedas ["convertir uno o varios nodos de almacenamiento combinados"](#) que no contengan el servicio ADC en nodos de solo datos.

```
/private/convert-to-data-only-node
```

```
/private/convert-to-data-only-node/start
```

```
/private/convert-to-data-only-node/retry
```

Cambios en la API de gestión de inquilinos en StorageGRID

StorageGRID 12.0 utiliza la versión 4 de la Tenant Management API. La versión 4 deja obsoleta la versión 3; sin embargo, las versiones 1, 2 y 3 siguen siendo compatibles.



Puedes seguir utilizando las versiones obsoletas de la API de gestión de inquilinos con StorageGRID 12.0; sin embargo, el soporte para estas versiones de la API se eliminará en una futura versión de StorageGRID. Después de actualizar a StorageGRID 12.0, puedes desactivar las API obsoletas usando la PUT `/grid/config/management API`.

Para obtener más información, visita ["Entiende la API de gestión de inquilinos"](#).

Nueva API para la replicación de objetos

Puedes usar la `/org/cross-grid-replication/{versionId}/replicate` API para replicar manualmente objetos en un bucket existente que tenga la replicación entre grids recién configurada.

Empieza a utilizar un sistema StorageGRID

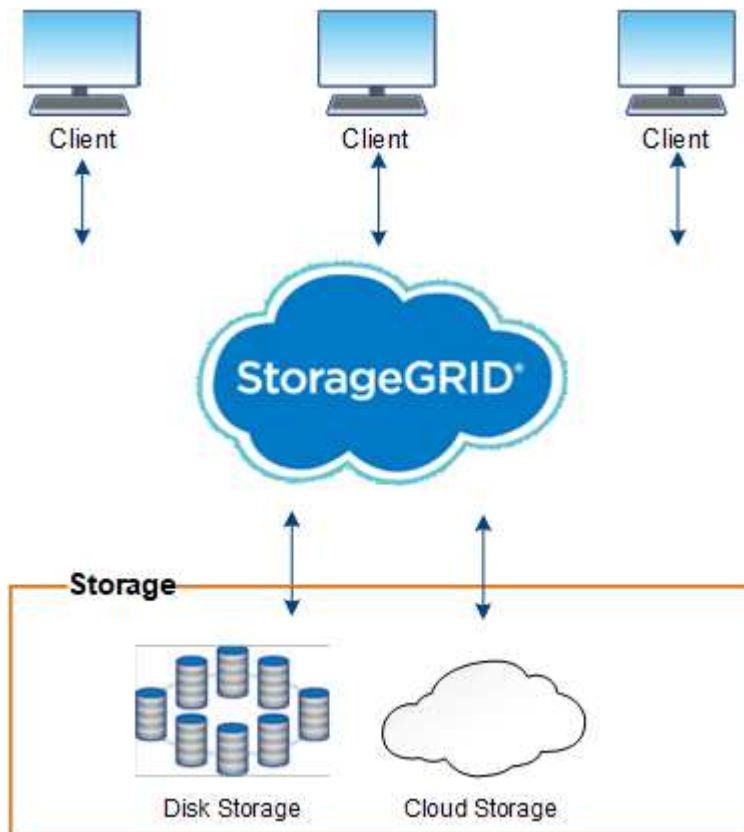
Conoce StorageGRID

¿Qué es StorageGRID?

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

StorageGRID ofrece un almacenamiento seguro y duradero para datos no estructurados a gran escala. Las políticas integradas de gestión del ciclo de vida basadas en metadatos optimizan dónde viven tus datos a lo largo de su vida. El contenido se coloca en la ubicación adecuada, en el momento adecuado y en el nivel de almacenamiento adecuado para reducir costos.

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



Se ha eliminado la compatibilidad con los nodos de archivo. Mover objetos desde un nodo de archivo a un sistema de almacenamiento de archivo externo a través de la API de S3 ha sido reemplazado por "[Grupos de almacenamiento en la nube de ILM](#)", que ofrece más funcionalidad.

Ventajas de StorageGRID

Entre las ventajas del sistema StorageGRID se incluyen las siguientes:

- Un repositorio de datos no estructurados, con escalabilidad masiva y fácil de usar, distribuido geográficamente.
- El protocolo de almacenamiento estándar de objetos Amazon Web Services Simple Storage Service (S3).
- Compatible con la nube híbrida. La gestión del ciclo de vida de la información (ILM) condicionada por políticas almacena objetos en nubes públicas, incluyendo 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 los objetos almacenados en nubes públicas.
- Protección de datos flexible para garantizar la durabilidad y la disponibilidad. Los datos se pueden proteger mediante replicación y código de borrado por capas. La verificación de los datos en reposo y en tránsito garantiza la integridad para la conservación a largo plazo.
- Gestión dinámica del ciclo de vida de los datos para ayudar a controlar los costes de almacenamiento. Puedes crear reglas de ILM que gestionen el ciclo de vida de los datos a nivel de objeto, personalizando la localidad de los datos, la durabilidad, el rendimiento, el coste y el tiempo de retención.
- Alta disponibilidad del almacenamiento de datos y de algunas funciones de gestión, con equilibrio de carga integrado para optimizar la carga de datos entre los recursos de StorageGRID.
- Compatibilidad con múltiples cuentas de inquilinos de almacenamiento para separar los objetos almacenados en tu sistema según las distintas entidades.
- Numerosas herramientas para supervisar el estado de tu sistema StorageGRID, entre las que se incluyen un completo sistema de alertas, un panel de control gráfico y estados detallados para todos los nodos y sitios.
- Compatibilidad con implementaciones basadas en software o en hardware. Puedes implementar StorageGRID en cualquiera de las siguientes:
 - Máquinas virtuales que se ejecutan en VMware.
 - Motores de contenedores en hosts Linux.
 - Dispositivos StorageGRID diseñados.
 - Los dispositivos de almacenamiento proporcionan almacenamiento de objetos.
 - Los dispositivos de servicios proporcionan servicios de administración de grid y de equilibrio de carga.
- Cumple con los requisitos de almacenamiento pertinentes de estas normativas:
 - Securities and Exchange Commission (SEC) en 17 CFR § 240.17a-4(f), que regula a los miembros de las bolsas, los corredores o los intermediarios.
 - La Norma 4511(c) de la Financial Industry Regulatory Authority (FINRA), que se remite a los requisitos de formato y soportes establecidos en la Norma 17a-4(f) de la SEC.
 - La Comisión de Comercio de Futuros sobre Materias Primas (CFTC) en la norma 17 CFR § 1.31(c)-(d), que regula el comercio de futuros sobre materias primas.
- Operaciones de actualización y mantenimiento sin interrupciones. Mantén el acceso al contenido durante los procedimientos de actualización, ampliación, decomisionado y mantenimiento.
- Gestión federada de identidades. Se integra con Active Directory, OpenLDAP u 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

Utiliza StorageGRID en una configuración de nube híbrida implementando una gestión de datos condicionada por políticas para almacenar objetos en Cloud Storage Pools, aprovechando los servicios de la plataforma StorageGRID y clasificando los datos de ONTAP a StorageGRID mediante NetApp FabricPool.

Grupos de almacenamiento en la nube

Los grupos de almacenamiento en la nube te permiten almacenar objetos fuera del sistema StorageGRID. Por ejemplo, podrías querer mover objetos a los que se accede con poca frecuencia a un almacenamiento en la nube de menor coste, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o el nivel de acceso Archive en el almacenamiento de blobs de Microsoft Azure. O quizá quieras mantener una copia de seguridad en la nube de los objetos de StorageGRID, que puede usarse para recuperar datos perdidos por un fallo en un volumen de almacenamiento o en un nodo de almacenamiento.

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



No se admite el uso de Cloud Storage Pools con FabricPool debido a la latencia adicional para recuperar un objeto del destino de Cloud Storage Pool.

Servicios de plataforma S3

Los servicios de la plataforma S3 te permiten utilizar servicios remotos como puntos finales para la replicación de objetos, notificaciones de eventos o integración de búsquedas. Los servicios de la plataforma funcionan independientemente de las reglas de ILM de la grid y se habilitan para cada bucket S3 de forma individual. Se admiten los siguientes servicios:

- El servicio de replicación CloudMirror replica automáticamente los objetos especificados 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 endpoint externo que admite la recepción de eventos de Simple Notification Service (Amazon SNS).
- El servicio de integración de búsquedas envía los metadatos de los objetos a un servicio externo de Elasticsearch, lo que permite buscar, visualizar y analizar dichos metadatos mediante herramientas de terceros.

Por ejemplo, podrías usar la replicación CloudMirror para reflejar registros específicos de clientes en Amazon S3 y luego aprovechar los servicios de AWS para hacer análisis de tus datos.

Organización de niveles de datos en ONTAP usando FabricPool

Puedes reducir el coste del almacenamiento ONTAP clasificando los datos por niveles en StorageGRID mediante FabricPool. FabricPool permite la clasificación automática de los datos en niveles de almacenamiento de objetos de bajo coste, tanto dentro como fuera de las instalaciones.

A diferencia de las soluciones de almacenamiento por niveles manuales, FabricPool reduce el coste total de propiedad al automatizar la clasificación de los datos por niveles para reducir el coste del almacenamiento. Ofrece las ventajas económicas de la nube mediante la clasificación por niveles en nubes públicas y privadas, incluida StorageGRID.

Información relacionada

- ["¿Qué es un grupo de almacenamiento en la nube?"](#)
- ["Gestiona los servicios de la plataforma"](#)
- ["Configura StorageGRID para FabricPool"](#)

Arquitectura de StorageGRID y topología de red

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

Conoce más sobre la ["tipos de nodos de grid"](#).

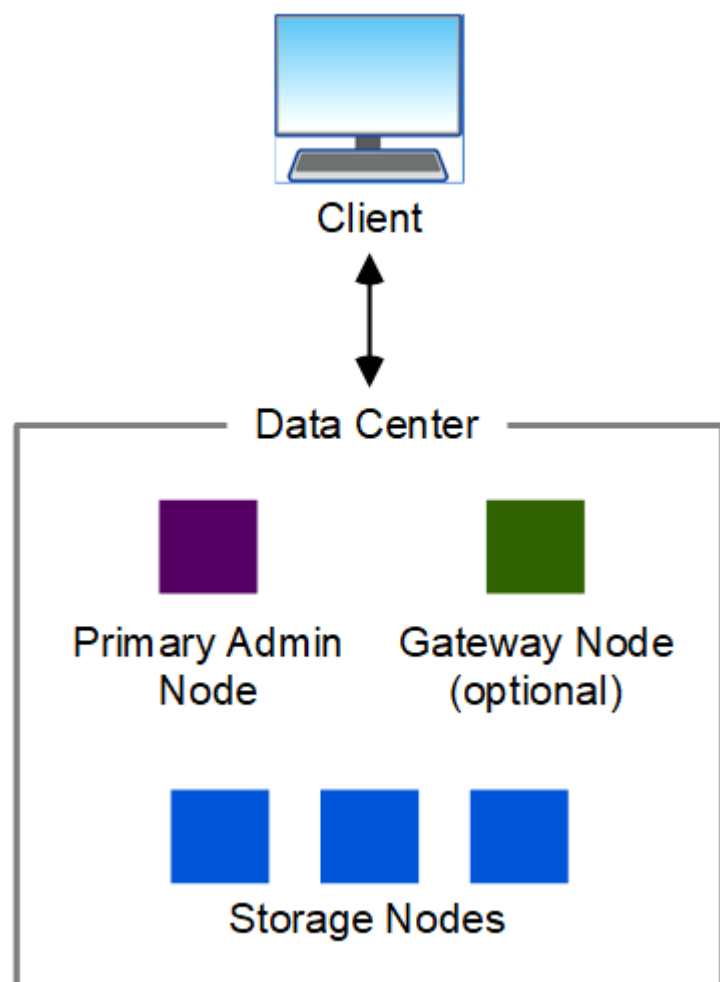
Para obtener más información sobre la topología de red de StorageGRID, los requisitos y las comunicaciones de la red, consulta la ["Directrices de redes"](#).

Topologías de implementación

El sistema StorageGRID puede implementarse en un único centro de datos o en varios centros de datos. El número máximo de sitios por implementación es 16.

Un único sitio

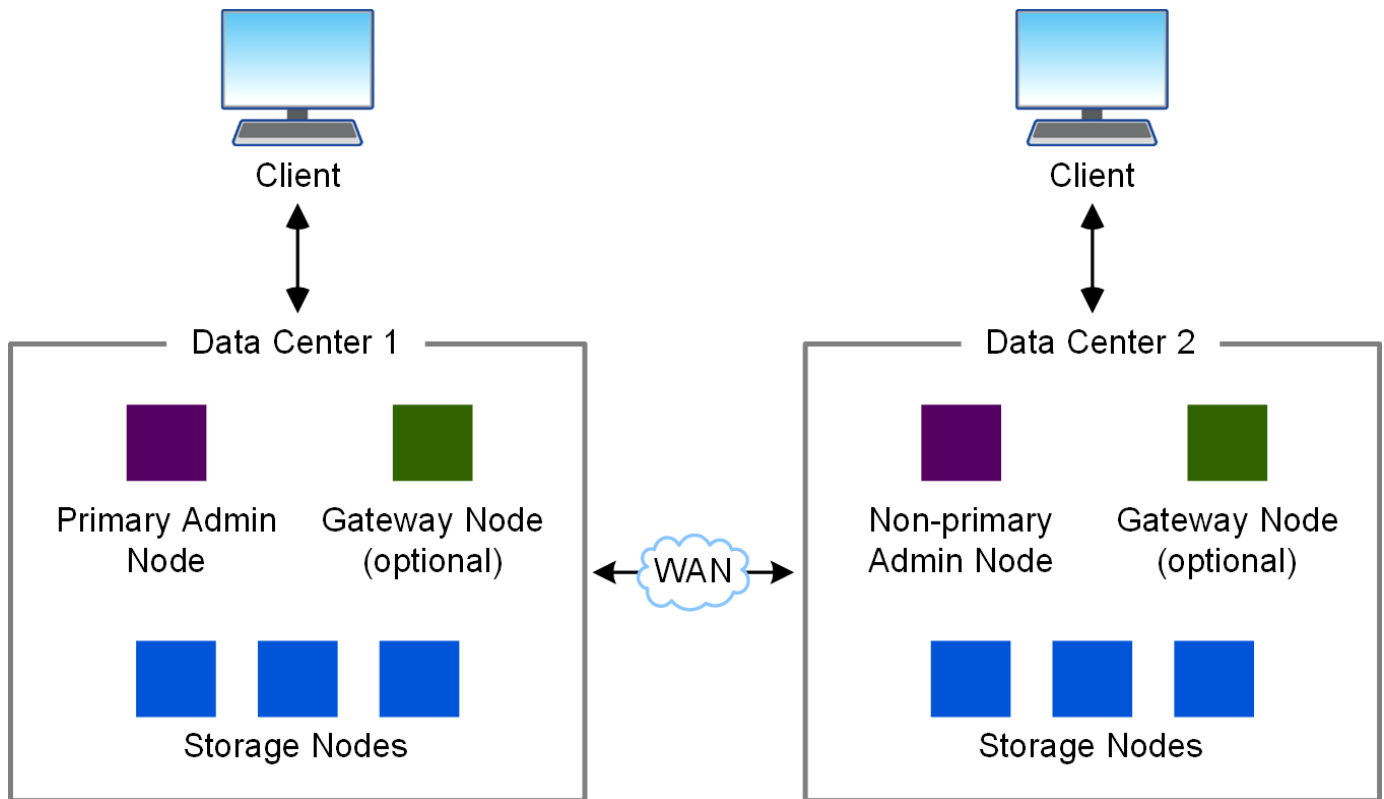
En una implementación con un único emplazamiento, la infraestructura y las operaciones del sistema StorageGRID están centralizadas.



Varias sedes

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

Los centros suelen estar situados en ubicaciones geográficamente distintas, repartidos por diferentes dominios de fallo, 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 centros.



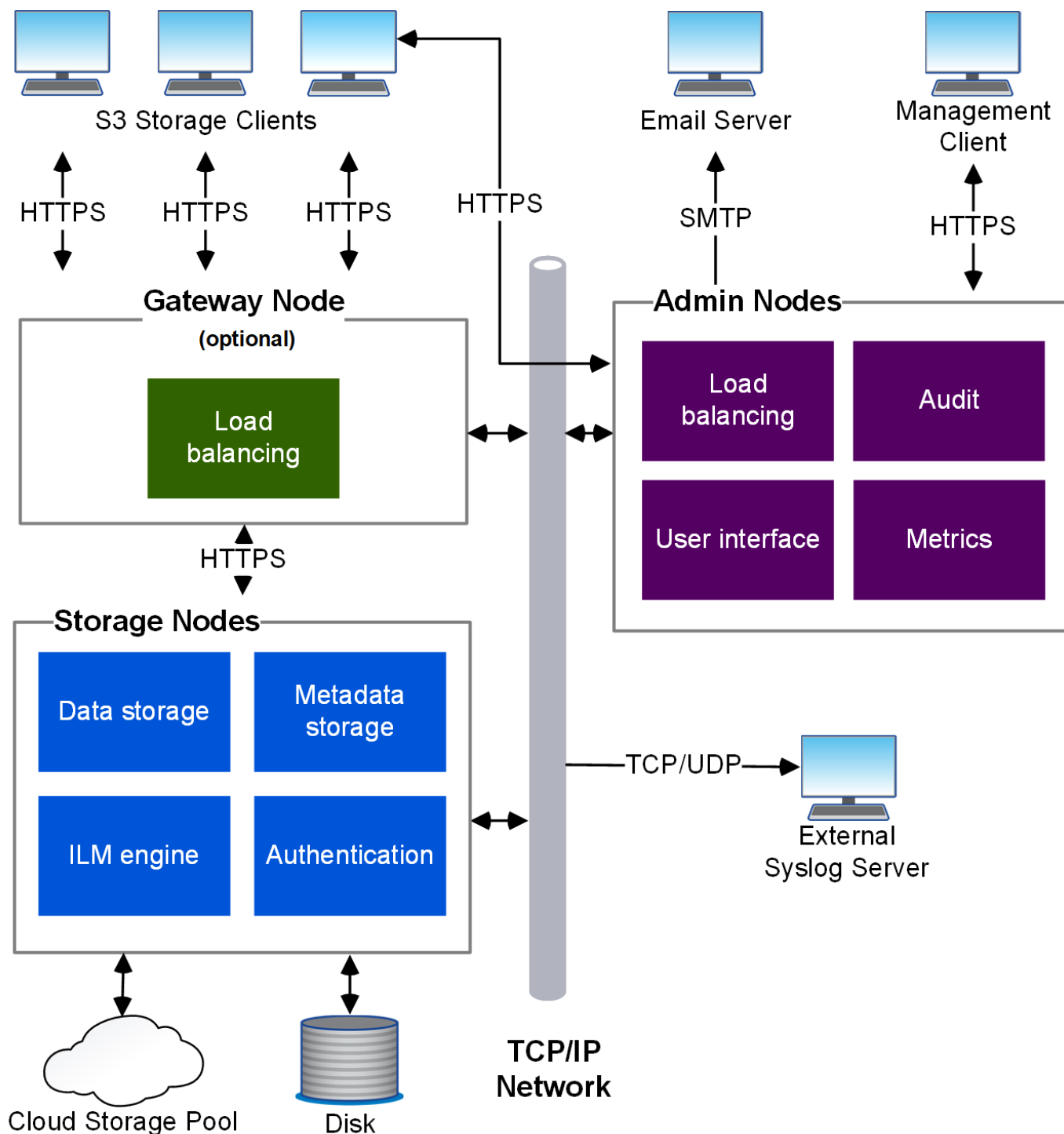
También pueden existir varios sitios lógicos dentro de un mismo centro de datos para permitir el uso de replicación distribuida y codificación de borrado, aumentando así la disponibilidad y la resiliencia.

Redundancia de nodos de la red

En una implementación de un solo sitio o de varios sitios, puedes incluir opcionalmente más de un nodo de administración o nodo de puerta de enlace para redundancia. Por ejemplo, puedes 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 grid en un sistema StorageGRID.



Los clientes S3 almacenan y recuperan objetos en StorageGRID. Otros clientes se usan para enviar notificaciones por correo electrónico, acceder a la interfaz de gestión 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 hacia los nodos de almacenamiento. Alternativamente, los clientes S3 pueden conectarse directamente a los nodos de almacenamiento mediante HTTPS.

Los objetos se pueden almacenar en StorageGRID en nodos de almacenamiento basados en software o en hardware, o en Cloud Storage Pools, que consisten en buckets S3 externos o contenedores de almacenamiento de Azure Blob.

Nodos y servicios de grid

Nodos y servicios de StorageGRID

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

Tipos de nodos de grid

El sistema StorageGRID utiliza tres tipos de nodos de grid:

Nodos de administración

Proporciona servicios de gestión, como la configuración del sistema, la supervisión y el registro. Cuando inicias sesión en Grid Manager, te conectas a un nodo de administración. Cada grid debe tener un nodo de administración principal y puede tener nodos de administración no principales adicionales para la redundancia. Puedes conectarte 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 usando el nodo de administración principal.

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

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

Nodos de almacenamiento

Gestiona y almacena datos y metadatos de objetos. Cada sitio de tu sistema StorageGRID debe tener al menos tres nodos de almacenamiento.

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

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

Nodos de puerta de enlace (opcional)

Proporciona una interfaz de equilibrio de carga que las aplicaciones cliente pueden utilizar para conectarse a StorageGRID. Un equilibrador de carga dirige a los clientes de forma transparente hacia un Storage Node óptimo, así que el fallo de los nodos o incluso de un sitio completo pasa desapercibido.

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

Nodos de hardware y software

Los nodos de StorageGRID pueden implementarse como nodos de dispositivo StorageGRID o como nodos basados en software. El número máximo de nodos (incluidos todos los tipos de nodos) por sistema es 220.

Nodos de la appliance StorageGRID

Los dispositivos de hardware de StorageGRID están diseñados específicamente para su uso en un sistema StorageGRID. Algunos dispositivos pueden utilizarse como Storage Nodes. Otros dispositivos pueden utilizarse como Admin Nodes o Gateway Nodes. Puedes combinar nodos de dispositivo con nodos basados en software o implementar grids totalmente diseñados, compuestos exclusivamente por dispositivos, que no dependen de hipervisores externos, almacenamiento ni hardware de cómputo.

Consulta lo siguiente para conocer los appliances disponibles:

- ["Documentación de StorageGRID Appliance"](#)
- ["NetApp Hardware Universe"](#)

Nodos basados en software

Los nodos de red basados en software pueden implementarse como máquinas virtuales de VMware o dentro de motores de contenedores en un host Linux. Consulta ["Instalar StorageGRID en nodos basados en software"](#).

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

Servicios de StorageGRID

A continuación se incluye una lista completa de los servicios de StorageGRID.

Servicio	Descripción	Ubicación
Reenviador del servicio de cuentas	Proporciona una interfaz para que el servicio de Load Balancer consulte el Account Service en hosts remotos y envía notificaciones al servicio de Load Balancer sobre los cambios en la configuración del Load Balancer Endpoint.	Servicio de equilibrado de carga en los nodos de administración y los nodos de puerta de enlace
ADC (Controlador de dominio administrativo)	Mantiene la información sobre la topología, proporciona servicios de autenticación y responde a las consultas de los servicios LDR y CMN.	Al menos tres nodos de almacenamiento que contengan el servicio ADC en cada sitio
AMS (Sistema de gestión de auditorías)	Supervisa y registra todos los eventos y transacciones auditados del sistema en un archivo de registro de texto.	Nodos de administración
Apache Tomcat	Servidor web para aplicaciones basadas en Java.	Nodos de administración
Avahi Daemon	Gestiona mDNS, que se utiliza para la resolución de nombres y la detección de servicios dentro de la red local.	Todos los nodos
Servicio de caché	Se ejecuta en los nodos del equilibrador de carga (Gateway) y gestiona una caché local del contenido de los objetos.	Nodos de puerta de enlace
Cassandra	Gestiona la base de datos distribuida de metadatos de objetos.	Nodos de almacenamiento (excepto los de solo datos)
Cassandra Reaper	Realiza reparaciones automáticas de metadatos de objetos.	Nodos de almacenamiento

Servicio	Descripción	Ubicación
Servicio de fragmentos	Gestiona los datos con código de borrado y los fragmentos de paridad.	Nodos de almacenamiento
CMN (Nodo de gestión de la configuración)	Gestiona las configuraciones de todo el sistema y las tareas de la grid. Cada grid tiene un servicio CMN.	Nodo de administración principal
DDS (Almacén de datos distribuido)	Se conecta con la base de datos Cassandra para gestionar los metadatos de los objetos.	Nodos de almacenamiento
DMV (Data Mover)	Transfiere datos a los puntos finales en la nube.	Nodos de almacenamiento
IP dinámica (dynip)	Supervisa la grid en busca de cambios dinámicos de IP y actualiza las configuraciones locales.	Todos los nodos
Grafana	Se utiliza para la visualización de métricas en el Grid Manager.	Nodos de administración
Alta disponibilidad	Gestiona las direcciones IP virtuales de alta disponibilidad en los nodos configurados en la página High Availability Groups. Este servicio también se conoce como el servicio keepalived.	Nodos de administración y de pasarela
Identidad (idnt)	Gestiona usuarios y grupos locales, la autenticación y federación de identidades de usuario de LDAP y Active Directory.	Nodos de almacenamiento que utilizan el servicio ADC
Árbitro Lambda	Gestiona las solicitudes de S3 Select SelectObjectContent.	Todos los nodos
Equilibrador de carga (nginx-gw)	Proporciona equilibrio de carga del tráfico de S3 procedente de los clientes hacia los Storage Nodes. El servicio de Load Balancer se puede configurar a través de la página de configuración de Load Balancer Endpoints. Este servicio también se conoce como el servicio nginx-gw.	Nodos de administración y de pasarela
LDR (enrutador de distribución local)	Gestiona el almacenamiento y la transferencia de contenido dentro de la grid.	Nodos de almacenamiento

Servicio	Descripción	Ubicación
MISCd Demonio de control del servicio de información	Proporciona una interfaz para consultar y gestionar servicios en otros nodos y para gestionar 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 que diversos servicios de grid (como Prometheus y Dynamic IP) puedan comunicarse con servicios en otros nodos a través de APIs HTTPS.	Todos los nodos
Balanceador de carga nginx-gw	Proporciona equilibrio de carga del tráfico de S3 procedente de los clientes hacia los Storage Nodes. El servicio de Load Balancer se puede configurar a través de la página de configuración de Load Balancer Endpoints. Este servicio también se conoce como el servicio nginx-gw.	Nodos de administración y de pasarela
NMS (Sistema de gestión de redes)	Impulsa las opciones de supervisión, generación de informes y configuración que se muestran a través de Grid Manager.	Nodos de administración
Node Exporter (recopilación de datos de Prometheus)	Publica estadísticas a nivel del sistema para la recopilación de métricas de series temporales de Prometheus.	Todos los nodos
ntp	Servicio de protocolo de tiempo de red (NTP).	Todos los nodos
Persistencia	Gestiona los archivos del disco raíz que deben conservarse tras un reinicio.	Todos los nodos
Prometheus	Recopila métricas de series temporales de los servicios de 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 endpoints.	Nodos de almacenamiento que utilizan el servicio ADC
SSM (Monitor de estado del servidor)	Supervisa el estado del hardware y envía informes al servicio NMS.	Hay una instancia en cada nodo de la red
Administrador de servidores	Gestiona los servicios de StorageGRID.	Todos los nodos
Agente SNMP	Responde a las solicitudes SNMP.	Nodos de administración

Servicio	Descripción	Ubicación
Servicio de gestión de puertos SNMP	Se encarga de la gestión dinámica de los puertos SNMP.	Todos los nodos
SSH (Secure Shell)	Gestiona el acceso seguro y la administración de sistema remota.	Todos los nodos
SSM (Monitor de estado del sistema)	Supervisa el estado del hardware y envía informes al servicio NMS.	Todos los nodos
Estadística	Registra métricas adicionales relacionadas con los buckets de S3.	Nodos de almacenamiento
Trace Agent (jaeger-agent)	Recibe y procesa la información de rastreo enviada por el trace collector (jaeger-collector).	Todos los nodos
Recopilador de trazas (jaeger-collector)	Realiza la recopilación de trazas para recabar información que podrá utilizar soporte técnico. El servicio de recopilación de trazas utiliza el software de código abierto Jaeger.	Nodos de administración

¿Qué es un nodo de administración StorageGRID?

Los nodos de administración proporcionan servicios de gestión, como la configuración del sistema, la supervisión y el registro. Los nodos de administración también pueden usarse para equilibrar la carga del tráfico de los clientes S3. Cada grid debe tener un nodo de administración principal y puede tener cualquier número de nodos de administración no principales para redundancia.

Diferencias entre los nodos de administración primarios y los no primarios

Cuando inicias sesión en Grid Manager o Tenant Manager, te conectas a un nodo de administración. Puedes conectarte a cualquier nodo de administración, y cada nodo de administración muestra una vista similar del sistema StorageGRID. Sin embargo, el nodo de administración principal ofrece más funcionalidad que los nodos de administración no principales. Por ejemplo, la mayoría de los procedimientos de mantenimiento deben realizarse desde el nodo de administración principal.

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

Capacidades	Nodo de administración principal	Nodo de administración no principal
Incluye el servicio AMS	Sí	Sí
Incluye el servicio CMN	Sí	No
Incluye el servicio NMS	Sí	Sí

Capacidades	Nodo de administración principal	Nodo de administración no principal
Incluye el servicio Prometheus	Sí	Sí
Incluye el SSM servicio	Sí	Sí
Incluye los servicios Equilibrador de carga y Alta disponibilidad	Sí	Sí
Es compatible con la Interfaz de programación de aplicaciones de gestión (mgmt-api)	Sí	Sí
Se puede usar para todas las tareas de mantenimiento relacionadas con la red, por ejemplo, el cambio de dirección IP y la actualización de servidores NTP	Sí	No
Puede descargar el paquete de recuperación	Sí	Sí
Puedes realizar un reequilibrio de EC después de la ampliación 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 varios nodos	Sí	Sí
Puede recuperar Storage, Gateway y nodos de administración no principales	Sí	Sí
Se puede recuperar el nodo de administración principal	Sí	No
Envía notificaciones de alerta, paquetes AutoSupport y trampas SNMP, e informa	Sí. Actúa como remitente preferido .	Sí. Actúa como remitente de reserva.

Remitente preferido Admin Node

Si tu implementación de StorageGRID incluye varios nodos de administración, el nodo de administración principal es el emisor preferido para las notificaciones de alertas, los paquetes AutoSupport y las trampas e informes SNMP.

En condiciones normales de funcionamiento del sistema, solo el remitente preferido envía notificaciones. Sin embargo, el resto de nodos de administración supervisan al remitente preferido. Si se detecta un problema, los demás nodos de administración actúan como remitentes de reserva.

En estos casos, es posible que se envíen varias notificaciones:

- Si los nodos de administración quedan «aislados» unos de otros, tanto el remitente preferido como los remitentes de reserva intentarán enviar notificaciones, y es posible que se reciban varias copias de las notificaciones.
- Si un remitente de reserva detecta problemas en el remitente preferido y comienza a enviar notificaciones, es posible que el remitente preferido recupere su capacidad para enviar notificaciones. Si esto ocurre, es posible que se envíen notificaciones duplicadas. El remitente de reserva dejará de enviar notificaciones cuando ya no detecte errores en el remitente preferido.



Cuando pruebas los paquetes de AutoSupport, todos los nodos de administración envían la prueba. Cuando pruebas las notificaciones de alertas, tienes que iniciar sesión en cada nodo de administración para comprobar la conectividad.

Servicios principales para los nodos de administración

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

Servicio	Función clave
Sistema de gestión de auditorías (AMS)	Realiza un seguimiento de la actividad y los eventos del sistema.
Nodo de gestión de la configuración (CMN)	Gestiona la configuración de todo el sistema.
[[alta disponibilidad]]Alta disponibilidad	Gestiona direcciones IP virtuales de alta disponibilidad para grupos de nodos de administración y nodos de puerta de enlace. Nota: Este servicio también está disponible en los nodos de Gateway.
Equilibrador de carga	Proporciona equilibrio de carga del tráfico de S3 procedente de los clientes hacia los nodos de almacenamiento. Nota: Este servicio también está disponible en los nodos de Gateway.
Interfaz de programación de aplicaciones de gestión (mgmt-api)	Procesa las solicitudes procedentes de la API de gestión de la red y de la API de gestión de inquilinos.
Sistema de gestión de redes (NMS)	Proporciona funcionalidad para el Grid Manager.
Prometheus	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 StorageGRID?

Los nodos de almacenamiento gestionan 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 disco.

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

Tipos de nodos de almacenamiento

Durante la instalación, puedes seleccionar el tipo de nodo de almacenamiento que deseas instalar. Estos tipos están disponibles tanto para los nodos de almacenamiento basados en software como para los nodos de almacenamiento basados en dispositivos que admiten esta función:

- Nodo de almacenamiento combinado de datos y metadatos
- Nodo de almacenamiento solo de metadatos
- Nodo de almacenamiento solo para datos

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

- Al instalar por primera vez un nodo de almacenamiento
- Al añadir un nodo de almacenamiento durante la ampliación del sistema StorageGRID

Nodo de almacenamiento de datos y metadatos (combinado)

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

Nodo de almacenamiento solo de metadatos

Utilizar un nodo de almacenamiento exclusivamente para metadatos puede resultar conveniente si tu grid almacena un número muy grande de objetos pequeños. Instalar capacidad dedicada a metadatos proporciona un mejor equilibrio entre el espacio necesario para un número muy grande de objetos pequeños y el espacio necesario para los metadatos de esos objetos. Además, los nodos de almacenamiento solo para metadatos alojados en dispositivos de alto rendimiento pueden aumentar el rendimiento.

Los nodos de almacenamiento exclusivos para metadatos tienen requisitos de hardware específicos:

- Al utilizar dispositivos StorageGRID, los nodos dedicados exclusivamente a metadatos solo se pueden configurar en dispositivos SGF6112 con doce unidades de 1,9 TB o doce de 3,8 TB.
- Cuando se utilizan nodos basados en software, los recursos de nodos solo metadatos deben coincidir con los recursos de Storage Nodes existentes. Por ejemplo:
 - Si el sitio de StorageGRID existente utiliza dispositivos SG6000 o SG6100, los nodos basados en software y dedicados exclusivamente a los metadatos 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 utiliza nodos de almacenamiento virtuales con 24 GB de RAM, 8 núcleos de CPU y 3 TB o 4 TB de almacenamiento de metadatos, los nodos basados en software

dedicados exclusivamente a metadatos deberían utilizar recursos similares (24 GB de RAM, 8 núcleos de CPU y 4 TB de almacenamiento de metadatos (rangedb/0)).

- Al añadir un nuevo sitio de StorageGRID, la capacidad total de metadatos del nuevo sitio debe ser, como mínimo, igual a la de los sitios existentes. Los recursos del nuevo sitio deben coincidir con los Storage Nodes de los sitios existentes.



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

Nodo de almacenamiento solo para datos

Utilizar un nodo de almacenamiento exclusivamente para datos puede tener sentido si tus nodos de almacenamiento presentan características de rendimiento diferentes. Por ejemplo, para aumentar potencialmente el rendimiento, podrías tener nodos de almacenamiento destinados solo a datos, de gran capacidad y con discos giratorios, acompañados de nodos de almacenamiento destinados solo a metadatos y de alto rendimiento.

Además, puedes aumentar la capacidad de metadatos eliminando de Cassandra los nodos con poca memoria RAM, lo que incrementa el límite de capacidad de metadatos por nodo. Consulta "[Gestiona el almacenamiento de metadatos de objetos](#)".

Puedes convertir un nodo de almacenamiento que no contiene el [Servicio ADC](#) en un nodo de almacenamiento solo de datos. Consulta "[Convertir un nodo de almacenamiento en un nodo solo de datos](#)".

Nodos de almacenamiento requeridos por grid y por sitio

A la hora de seleccionar qué Storage Nodes vas a utilizar en tu topología, ten en cuenta que la grid o cada uno de los sitios en la grid deben contener lo siguiente:

- Por sitio (en una red de un solo sitio o de varios sitios): tres [ADC](#) nodos de almacenamiento (puede ser cualquier combinación de nodos de almacenamiento combinados y nodos de almacenamiento exclusivos de metadatos)
- Red de un único sitio: al menos dos nodos de almacenamiento de objetos (puede ser cualquier combinación de nodos combinados y de solo datos)
- Red con múltiples emplazamientos: al menos un nodo de almacenamiento de objetos por emplazamiento (puede ser combinado o solo de datos)

Servicios principales para los nodos de almacenamiento

La siguiente tabla muestra los servicios principales de los nodos de almacenamiento; sin embargo, esta tabla no incluye todos los servicios de los nodos.



Algunos servicios, como el servicio ADC y el servicio RSM, suelen existir únicamente en tres nodos de almacenamiento en cada sitio.

Servicio	Función clave
Cuenta (acct)	Administra las cuentas de los inquilinos. Los nodos de almacenamiento «solo datos» no alojan este servicio.

Servicio	Función clave
Controlador de dominio administrativo (ADC)	Gestiona la topología y la configuración de toda la grid. Los nodos de almacenamiento «solo datos» no alojan este servicio. Detalles El servicio de controlador de dominio administrativo (ADC) autentica los nodos de grid y sus conexiones entre sí. El servicio ADC se aloja en un mínimo de tres Storage Nodes en un sitio. El servicio ADC gestiona la información sobre la topología, incluida la ubicación y la disponibilidad de los servicios. Cuando un nodo de la red necesita información de otro nodo de la red o que otro nodo de la red realice una acción, se pone en contacto con un servicio ADC para encontrar el nodo de la red más adecuado para procesar su solicitud. Además, el servicio ADC conserva una copia de los paquetes de configuración de la implementación de StorageGRID, lo que permite a cualquier nodo de la red recuperar la información de configuración actual. Para facilitar las operaciones distribuidas y en modo aislado, 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 con al menos un servicio ADC. Esto garantiza que los nodos de la red siempre accedan 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 nodos 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 al servicio ADC recopilar información sobre la topología. Esta información sobre los nodos de la red incluye la carga de la CPU, el espacio en disco disponible (si tiene almacenamiento), los servicios compatibles y el ID de sitio del nodo de la red. Otros servicios le piden al servicio ADC información sobre la topología mediante consultas de topología. El servicio ADC responde a cada consulta con la información más reciente recibida del sistema StorageGRID.
Cassandra	Almacena y protege los metadatos de los objetos. Los nodos de almacenamiento «solo datos» no alojan este servicio.
Cassandra Reaper	Realiza reparaciones automáticas de metadatos de objetos. Los nodos de almacenamiento «solo datos» no alojan este servicio.
Fragmento	Gestiona los datos con código de borrado y los fragmentos de paridad.

Servicio	Función clave
Data Mover (dmv)	Traslada los datos a los Cloud Storage Pools.
Almacén de datos distribuido (DDS)	Supervisa el almacenamiento de metadatos de objetos. Detalles Cada nodo de almacenamiento incluye el servicio Distributed Data Store (DDS). Este servicio interactúa con la base de datos Cassandra para realizar tareas en segundo plano sobre los metadatos de los objetos almacenados en el sistema StorageGRID. El servicio DDS realiza un seguimiento del número total de objetos incorporados al sistema StorageGRID, así como del número total de objetos incorporados a través de cada una de las interfaces compatibles con el sistema (S3).
Identidad (idnt)	Federe las identidades de los usuarios de LDAP y Active Directory. Los nodos de almacenamiento «solo datos» no alojan este servicio.

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

Servicio	Función clave
Máquina de estados replicada (RSM)	Garantiza que las solicitudes de los servicios de la plataforma S3 se envíen a sus respectivos endpoints. Los nodos de almacenamiento «solo datos» no alojan este servicio.
Monitor de estado del servidor (SSM)	Supervisa el sistema operativo y el hardware subyacente.

Funciones de tráfico de datos.

¿Qué es un nodo Gateway de StorageGRID?

El servicio LDR se encarga de las siguientes tareas:

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

- Consultas
- Actividad de gestión del ciclo de vida de la información (ILM)
- Eliminación de objetos
- Almacenamiento de datos de objetos

El servicio StorageGRID Load Balancer se ofrece en todos los nodos de administración y en todos los nodos de puerta de enlace. Realiza la terminación de Transport Layer Security (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 a los clientes de forma transparente hacia un nodo de almacenamiento óptimo, así que el fallo de los nodos o incluso de todo un sitio pasa desapercibido.

- Transferencias de datos de objetos desde otro servicio LDR (StorageGRID)
- Gestión del almacenamiento de datos

El servicio LDR también asigna cada objeto de S3 a su UUID único. Configuras uno o varios puntos finales del equilibrador de carga para definir el puerto y el protocolo de red (HTTPS o HTTP) que las solicitudes entrantes y salientes de los clientes usarán para acceder a los servicios del equilibrador de carga en los nodos Gateway y Admin. El punto final del equilibrador de carga también define el tipo de cliente (S3), el modo de enlace y, opcionalmente, una lista de tenants permitidos o bloqueados. Consulta ["Aspectos a tener en cuenta para el equilibrio de carga"](#).

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

Si lo necesitas, puedes agrupar las interfaces de red de varios Gateway Nodes y Admin Nodes en un grupo de alta disponibilidad (HA). Si la interfaz activa del grupo HA falla, una interfaz de respaldo puede gestionar la carga de trabajo de la aplicación cliente. Consulta ["Administra grupos de alta disponibilidad \(HA\)"](#).

Los almacenes de objetos de un nodo de almacenamiento se identifican mediante un número hexadecimal de 0000 a 002F, que se conoce como el ID de volumen. Se reserva espacio en el primer almacén de objetos (volumen 0) para los metadatos de los objetos en una base de datos

Servicios principales para los nodos de puerta de enlace

Cassandra; cualquier espacio restante en ese volumen se usa para los datos de los objetos. Todos los demás almacenes de objetos se usan exclusivamente para los datos de los objetos, lo que incluye copias replicadas y fragmentos con código de borrado.

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

Servicio	Función clave
Servicio de caché	Gestiona una caché local del contenido de los objetos.
Alta disponibilidad	Gestiona direcciones IP virtuales de alta disponibilidad para grupos de nodos de administración y nodos de puerta de enlace. Nota: Este servicio también está disponible en los nodos de administración.

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

Para garantizar la redundancia y así la protección contra la pérdida, se mantienen tres copias de los metadatos de objetos en cada sitio. Esta replicación no es configurable y se realiza automáticamente. Para más detalles, consulta ["Gestiona el almacenamiento de metadatos de"](#)

Servicio	Función clave
Equilibrador de carga	Proporciona equilibrio de carga de capa 7 para el tráfico de S3 procedente de los clientes hacia los nodos de almacenamiento. Este es el mecanismo de equilibrio de carga recomendado. Nota: Este servicio también está disponible en los nodos de administración.
Monitor de estado del servidor (SSM)	Supervisa el sistema operativo y el hardware subyacente.

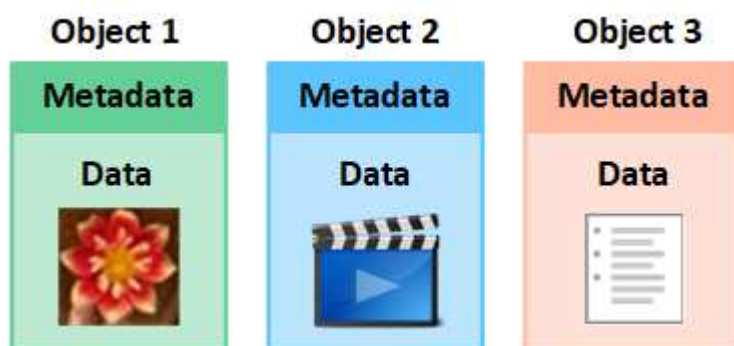
Cómo gestiona StorageGRID los datos

Qué es un objeto StorageGRID

En 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 del almacenamiento en bloques, el almacenamiento de objetos organiza los datos en una estructura plana y no estructurada.

El almacenamiento de objetos separa la ubicación física de los datos del método utilizado para almacenarlos y recuperarlos.

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



¿Qué son los datos de objeto?

Los datos de un objeto pueden ser cualquier cosa; por ejemplo, una fotografía, un vídeo o un historial médico.

¿Qué son los metadatos de un objeto?

Los metadatos de objetos son cualquier información que describe un objeto. StorageGRID utiliza los metadatos de objetos para realizar el seguimiento de las ubicaciones de todos los objetos en todo el grid y gestionar 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, incluidos un identificador único para cada objeto (UUID), el nombre del objeto, el

nombre del bucket de S3, el nombre o el identificador de la cuenta del tenant, el tamaño lógico del objeto, la fecha y hora en que se creó el objeto por primera vez y la fecha y hora en que se modificó por última vez.

- La ubicación actual de almacenamiento de cada copia del objeto o fragmento con código de borrado.
- Cualquier metadato de usuario asociado al objeto.

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

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

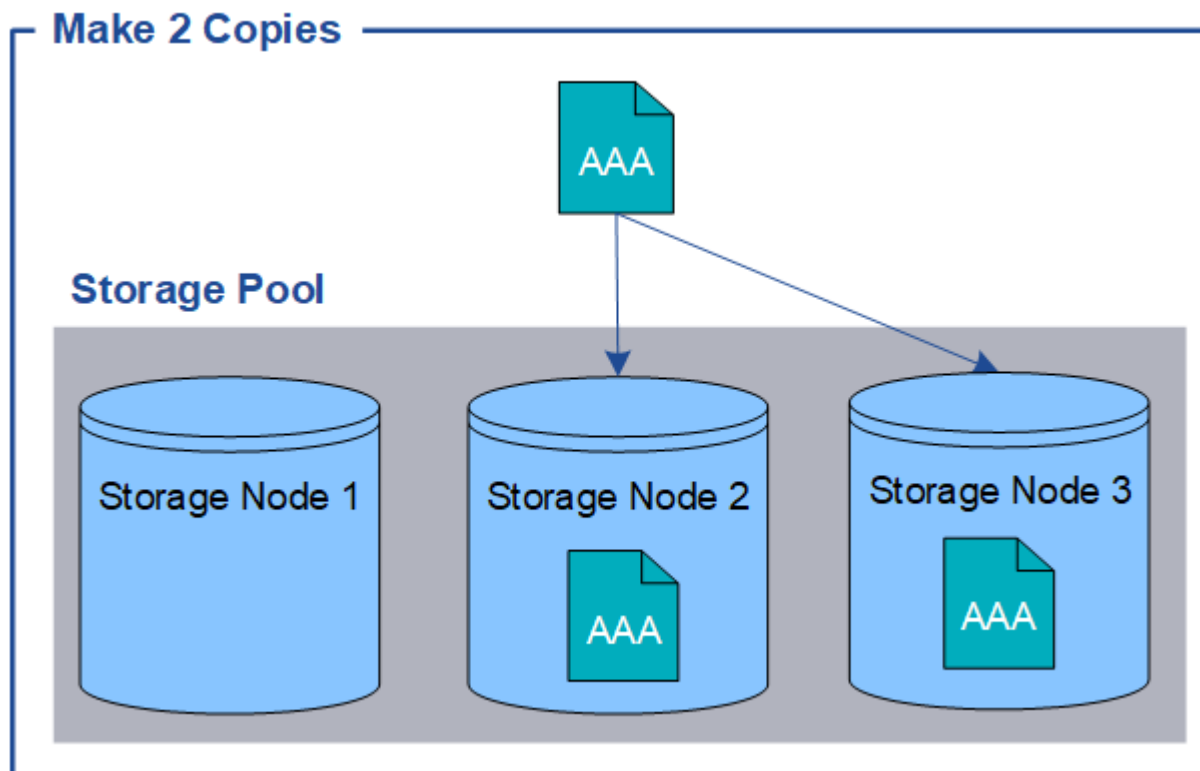
¿Cómo se protegen los datos de los objetos?

El sistema StorageGRID te ofrece dos mecanismos para proteger los datos de los objetos frente a posibles pérdidas: la replicación y el código de borrado.

Replicación

Cuando StorageGRID asocia objetos a una regla de gestión del ciclo de vida de los datos (ILM) configurada para crear copias replicadas, el sistema crea copias exactas de los datos de los objetos y las almacena en Storage Nodes o Cloud Storage Pools. Las reglas ILM determinan el número de copias que se crean, dónde se almacenan dichas copias y durante cuánto tiempo las conserva el sistema. Si se pierde una copia, por ejemplo, como consecuencia de la pérdida de un Storage Node, el objeto sigue estando disponible si existe una copia en otro lugar del sistema StorageGRID.

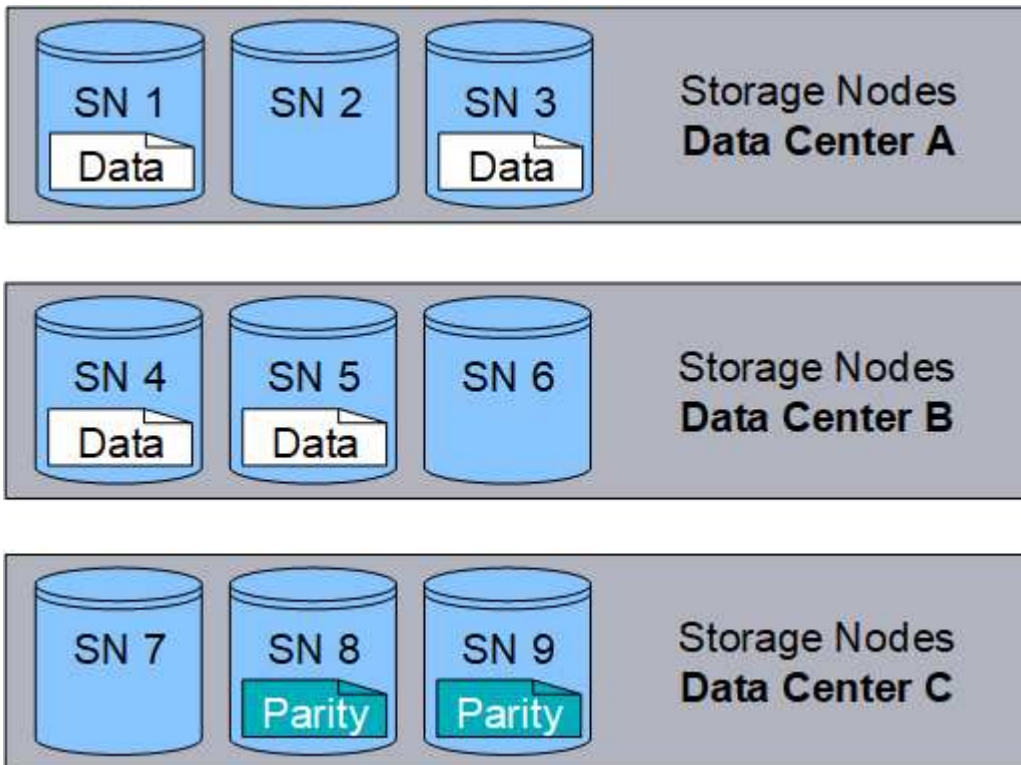
En el siguiente ejemplo, la regla «Make 2 Copies» especifica que se coloquen dos copias replicadas de cada objeto en un grupo de almacenamiento que contiene tres Storage Nodes.



Codificación de borrado

Cuando StorageGRID asocia objetos a una regla de ILM configurada para crear copias con código de borrado, divide los datos del objeto 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, este se vuelve a ensamblar utilizando los fragmentos almacenados. Si un fragmento de datos o de paridad se corrompe o se pierde, el algoritmo de código de borrado puede recrear ese fragmento utilizando un subconjunto de los fragmentos de datos y de paridad restantes. Las reglas de ILM y los perfiles de código de borrado determinan el esquema de código de borrado utilizado.

El siguiente ejemplo ilustra el uso del código de borrado en los datos de un objeto. En este ejemplo, la regla ILM utiliza un esquema de código 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 Storage Node diferente repartidos entre tres centros de datos para garantizar la protección de los datos en caso de fallo de un nodo o pérdida de un sitio.



Información relacionada

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

Ciclo de vida de objetos en StorageGRID

El ciclo de vida de un objeto consta de varias fases. Cada fase representa las operaciones que se llevan a cabo con el objeto.

El ciclo de vida de un objeto incluye las operaciones de incorporación, gestión de copias, recuperación y eliminación.

- **Ingest:** el proceso mediante el cual una aplicación cliente de S3 guarda un objeto a través de HTTP en el sistema StorageGRID. En esta fase, el sistema StorageGRID comienza a gestionar el objeto.

- **Gestión de copias:** el proceso de gestión de copias replicadas y con código de borrado en StorageGRID, tal y como se describe en las reglas de ILM de las políticas de ILM activas. Durante la fase de gestión de copias, StorageGRID protege los datos de los objetos contra la pérdida mediante la creación y el mantenimiento del número y tipo especificados de copias de los objetos en los nodos de almacenamiento o en un Cloud Storage Pool.
- **Recuperación:** El proceso mediante el cual una aplicación cliente accede a un objeto almacenado por el sistema StorageGRID. El cliente lee el objeto, que se recupera de un Storage Node o Cloud Storage Pool.
- **Eliminar:** El proceso de eliminar todas las copias de un objeto de la grid. Los objetos pueden eliminarse como resultado de que la aplicación cliente envíe una solicitud de eliminación al sistema StorageGRID, o como resultado de un proceso automático que StorageGRID realiza cuando expira el ciclo de vida del objeto.



Información relacionada

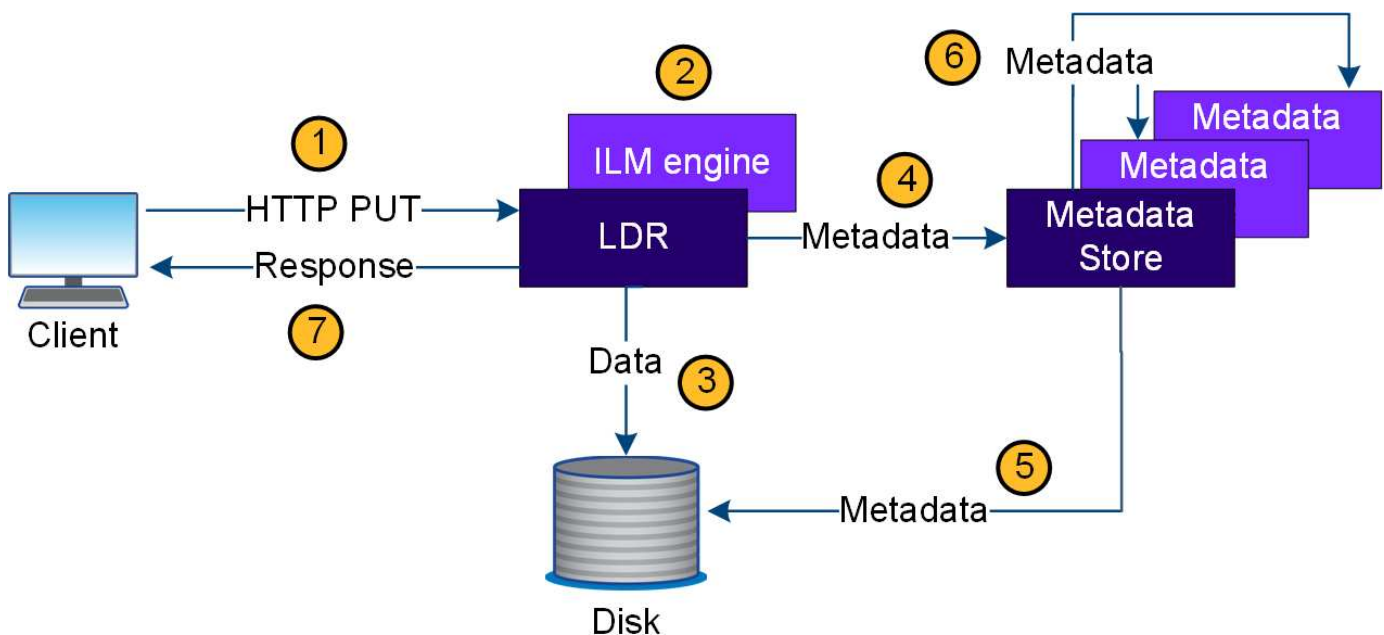
- ["Gestiona objetos con ILM"](#)
- ["Usa la gestión del ciclo de vida de la información"](#)

Cómo StorageGRID gestiona la ingesta de objetos

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

Flujo de datos

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



1. La aplicación cliente crea el objeto y lo envía al sistema StorageGRID mediante una solicitud HTTP PUT.
2. El objeto se evalúa según la política de 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 del almacenamiento de una copia replicada en 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 distribuye copias de los metadatos de los objetos a otros nodos de almacenamiento. Estas copias también se guardan en disco.
7. El servicio LDR devuelve una respuesta HTTP 200 OK al cliente para confirmar que el objeto ha sido ingerido.

Cómo StorageGRID gestiona las copias de objetos

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

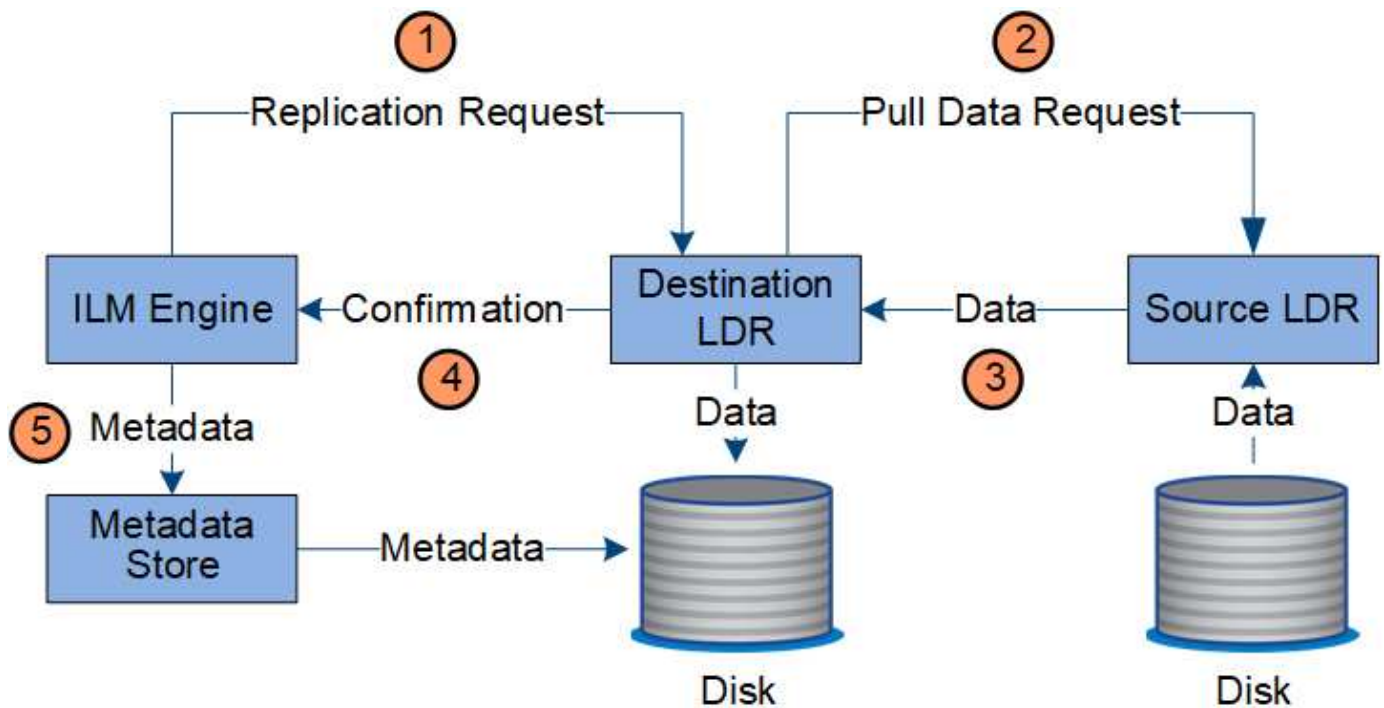
Es posible que, en distintos momentos del ciclo de vida de un objeto, se requieran diferentes tipos o ubicaciones de copias del mismo. Las reglas de ILM se evalúan periódicamente para asegurarse de que los objetos se ubiquen como se requiere.

Los datos de los objetos los gestiona el servicio LDR.

Protección de contenido: replicación

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

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

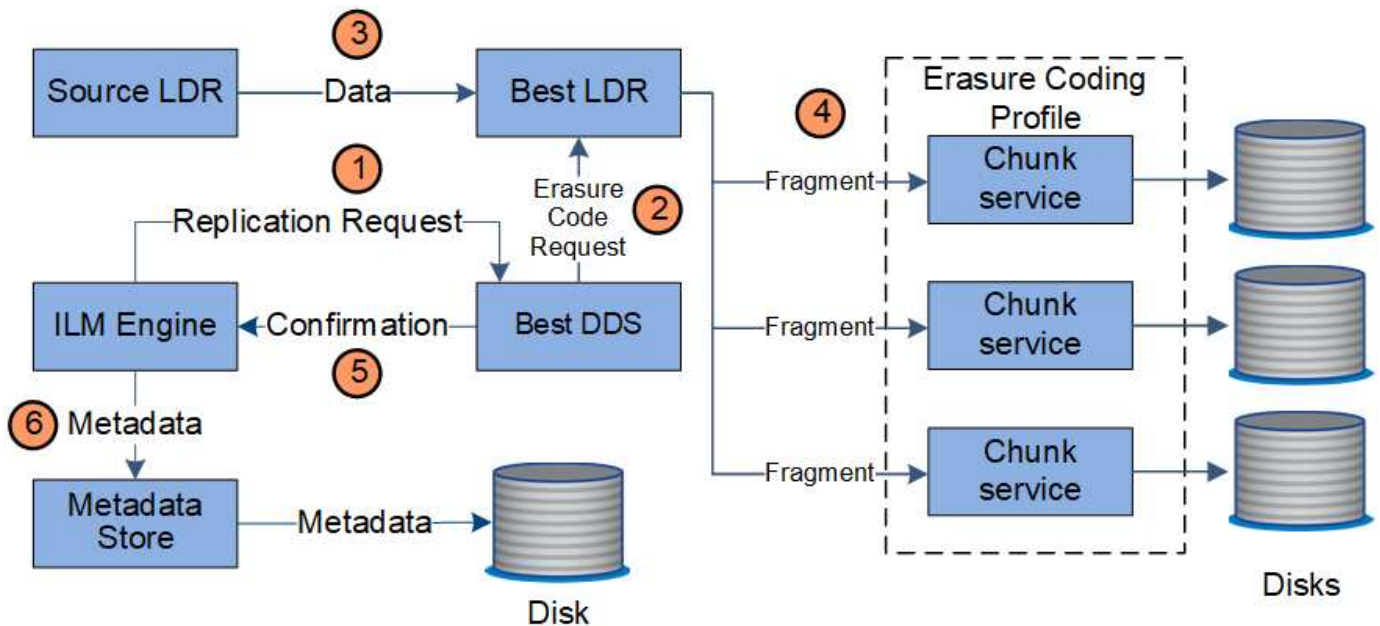


1. El motor ILM consulta el servicio ADC para determinar cuál es el mejor servicio LDR de destino dentro del grupo de almacenamiento especificado por la regla ILM. Luego le envía a ese servicio LDR un comando para iniciar la replicación.
2. El servicio LDR de destino consulta al servicio ADC cuál es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

Protección de contenido: código de borrado

Si una regla de ILM incluye instrucciones para crear copias con código de borrado de los datos de los objetos, el esquema de código de borrado correspondiente divide los datos de los objetos en fragmentos de datos y de paridad y distribuye estos fragmentos entre los Storage Nodes configurados en el perfil de código de borrado.

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

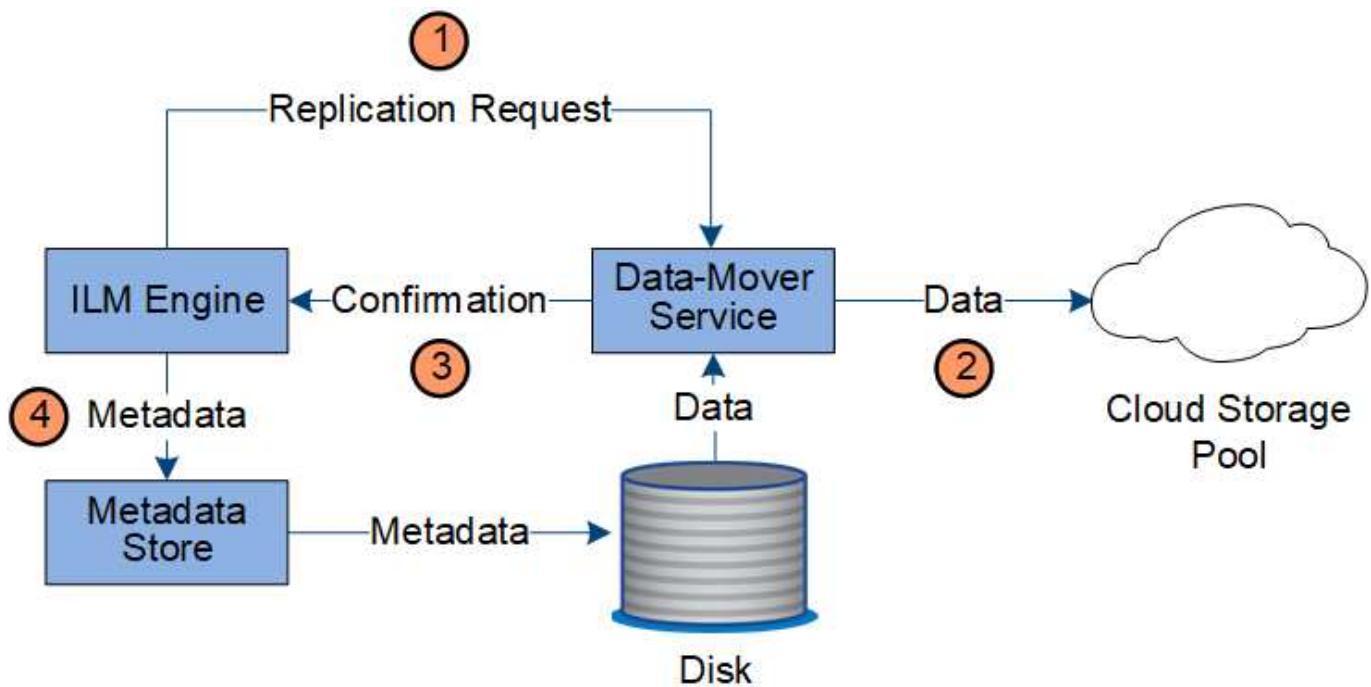


1. El motor ILM consulta al servicio ADC para determinar qué servicio DDS es el más adecuado para realizar la operación de código de borrado. Una vez determinado, el motor ILM envía una solicitud de "initiate" a ese servicio.
2. El servicio DDS indica a un LDR que aplique código de borrado a los datos del objeto.
3. El servicio LDR de origen envía una copia al servicio LDR seleccionado para el borrado por código.
4. Tras crear el número adecuado de fragmentos de paridad y de datos, el servicio LDR distribuye dichos fragmentos entre los Storage Nodes (servicios Chunk) que conforman el storage pool del perfil de erasure-coding.
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 los metadatos de ubicación de los objetos.

Protección de contenido: Cloud Storage Pool

Si las instrucciones de ubicación de contenido de una regla de ILM requieren que se almacene una copia replicada de los datos de objetos en un Cloud Storage Pool, los datos de los objetos se duplican en el bucket externo de S3 o en el contenedor de Azure Blob storage que se haya especificado para el Cloud Storage Pool.

El motor ILM, que es un componente del servicio LDR, y el servicio Data Mover controlan el movimiento de objetos al Cloud Storage Pool.



1. El motor ILM selecciona un servicio Data Mover para replicar en el Cloud Storage Pool.
2. El servicio Data Mover envía los datos de los objetos al Cloud Storage Pool.
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 los metadatos de ubicación de los objetos.

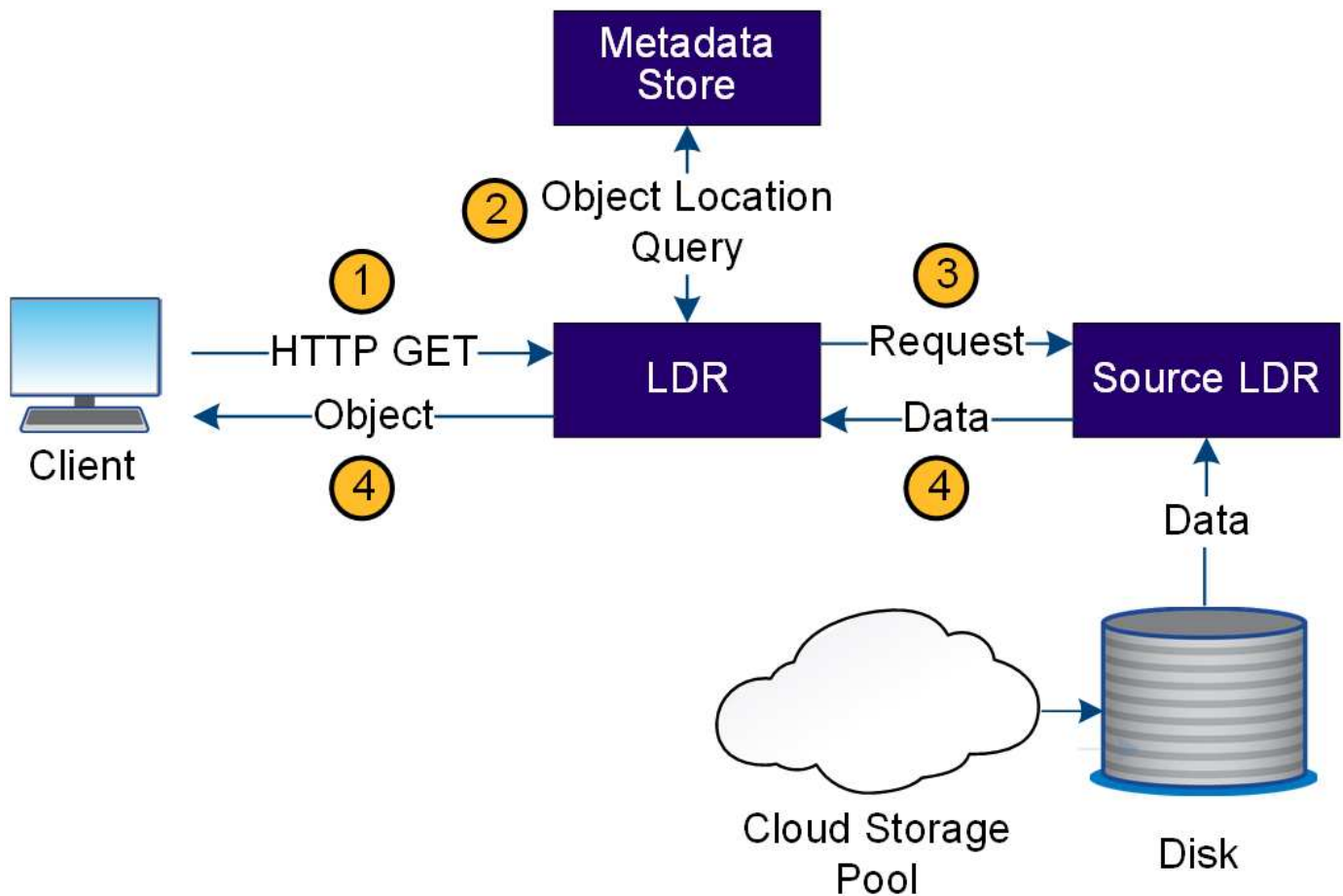
Cómo StorageGRID gestiona la recuperación de objetos

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

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 es desde un nodo de almacenamiento. Si el objeto no está disponible en un nodo de almacenamiento, la solicitud de recuperación se dirige a un Cloud Storage Pool.



Si la única copia del objeto está en el almacenamiento de AWS Glacier o en el nivel de archivo de Azure, la aplicación cliente debe enviar una solicitud S3 RestoreObject para restaurar una copia recuperable en el Cloud Storage Pool.



1. El servicio LDR recibe una solicitud de recuperación de la aplicación cliente.
2. El servicio LDR consulta el almacén de metadatos para obtener 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.

Cómo StorageGRID gestiona la eliminación de objetos

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

Jerarquía de eliminación

StorageGRID ofrece varios métodos para controlar cuándo se conservan o se eliminan los objetos. Los objetos pueden eliminarse a petición del cliente o de forma automática. StorageGRID siempre da prioridad a cualquier configuración de S3 Object Lock frente a las solicitudes de eliminación del cliente, las cuales tienen prioridad sobre el ciclo de vida del bucket de S3 y las instrucciones de ubicación de ILM.

- **S3 Object Lock:** Si la configuración global de S3 Object Lock está habilitada para la red, los clientes de S3 pueden crear buckets con S3 Object Lock habilitado y luego usar la API de REST de S3 para especificar la configuración de retain-until-date y legal hold para cada versión de objeto añadida a ese

bucket.

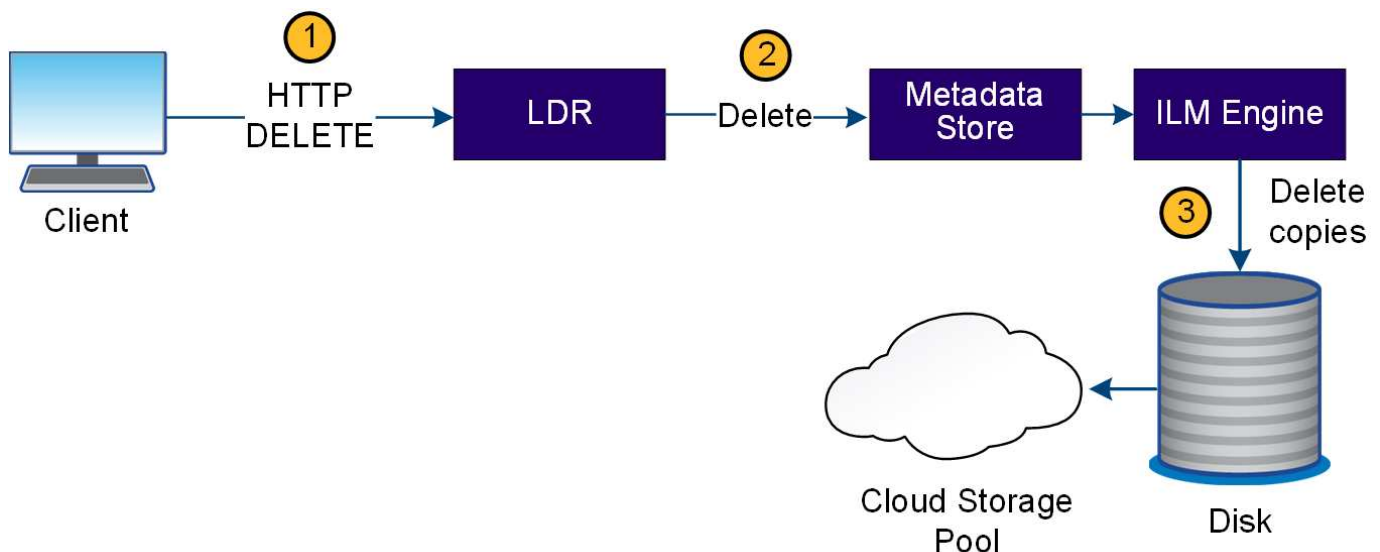
- Una versión de objeto que está bajo retención legal no puede eliminarse por ningún método.
 - Antes de que se alcance la fecha límite de retención de una versión de un objeto, esa versión no puede eliminarse por ningún método.
 - Los objetos de los buckets en los que se ha activado S3 Object Lock se conservan «para siempre» mediante ILM. Sin embargo, después de que se alcance la fecha límite de conservación, una versión del objeto puede eliminarse por una solicitud del cliente o al expirar el ciclo de vida del bucket.
 - Si los clientes de S3 aplican una fecha de retención predeterminada al bucket, no necesitan especificar una fecha de retención para cada objeto.
- **Solicitud de eliminación del cliente:** Un cliente de S3 puede enviar una solicitud de eliminación de un objeto. Cuando un cliente elimina un objeto, todas las copias del objeto se eliminan del sistema StorageGRID.
 - **Eliminar objetos del depósito:** Los usuarios de Tenant Manager pueden utilizar esta opción para eliminar de forma permanente todas las copias de los objetos y las versiones de los mismos en los depósitos seleccionados del sistema StorageGRID.
 - **Ciclo de vida de un bucket de S3:** los clientes de S3 pueden añadir una configuración de ciclo de vida a sus buckets que especifique una acción de caducidad. Si existe un ciclo de vida para el bucket, StorageGRID elimina automáticamente todas las copias de un objeto cuando se alcanza la fecha o el número de días especificados en la acción de caducidad, a menos que el cliente elimine el objeto antes.
 - **Instrucciones de asignación de ILM:** Suponiendo que el bucket no tenga activado S3 Object Lock y que no haya ningún ciclo de vida del bucket, StorageGRID elimina automáticamente un objeto cuando finaliza el último periodo de tiempo de la regla de ILM y no hay más asignaciones especificadas para dicho objeto.



Cuando se configura el ciclo de vida de un bucket de S3, las acciones de caducidad del ciclo de vida prevalecen sobre la política de ILM para los objetos que coinciden con el filtro del ciclo de vida. Como resultado, un objeto podría mantenerse en el grid incluso después de que hayan expirado las instrucciones de ILM para ubicar el objeto.

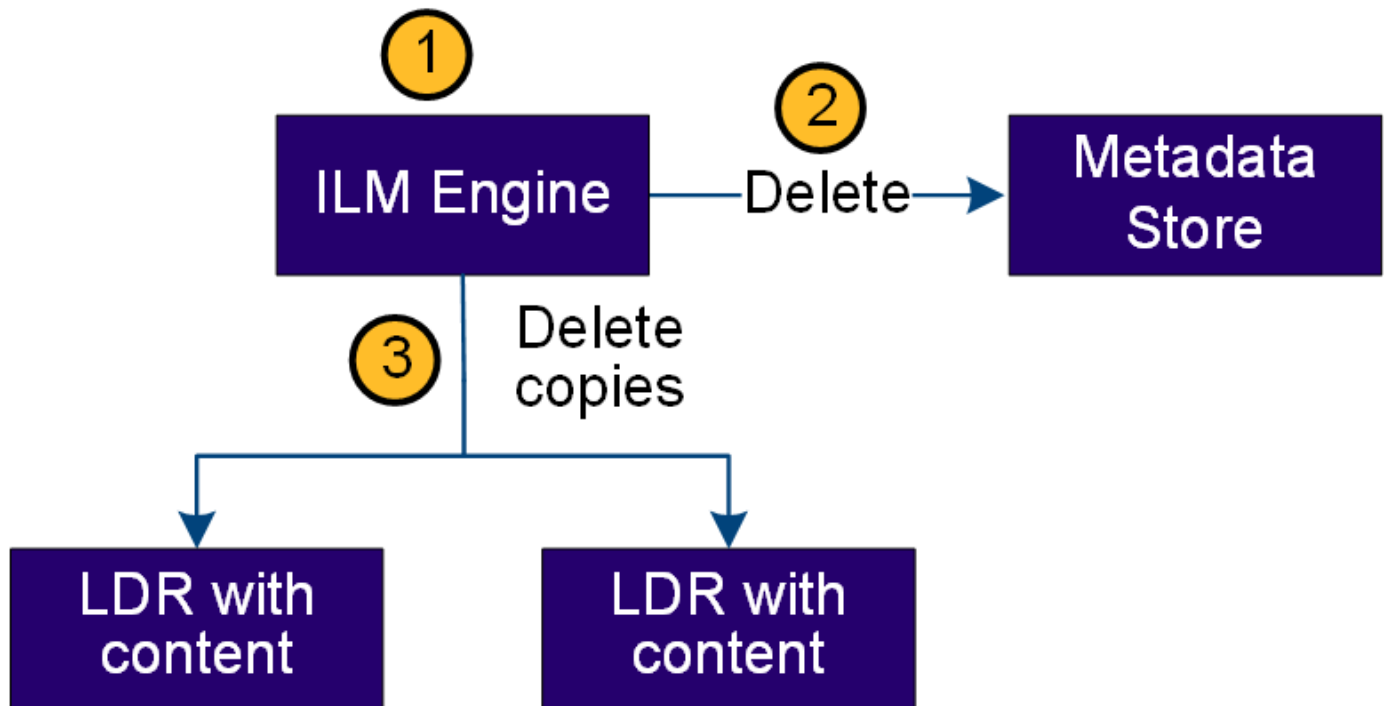
Consulta ["Cómo se eliminan los objetos"](#) para más información.

Flujo de datos para las 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 aparezca como eliminado ante las solicitudes de los clientes, y ordena 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.

Flujo de datos para las eliminaciones de ILM



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 de los clientes.
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 en StorageGRID

Utilizas 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 tu sistema StorageGRID. Las reglas de ILM determinan cómo StorageGRID almacena los objetos a lo largo del tiempo. Configuras una o varias reglas de ILM y luego las agregas a una política de ILM. Una grid puede tener más de una política activa al mismo tiempo.

Las reglas de ILM definen:

- Qué objetos deben almacenarse. Una regla puede aplicarse a todos los objetos, o puedes especificar filtros para identificar a qué objetos se aplica una regla. Por ejemplo, una regla puede aplicarse solo a objetos asociados con ciertas cuentas de tenant, buckets específicos de S3 o valores de metadatos específicos.
- El tipo y la ubicación del almacenamiento. Los objetos se pueden almacenar en Storage Nodes o en Cloud

Storage Pools.

- El tipo de copias de objetos que se realizan. Las copias pueden ser replicadas o codificadas por borrado.
- Para las copias replicadas, el número de copias realizadas.
- En el caso de las copias con código de borrado, el esquema de código de borrado utilizado.
- 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 estos se incorporan a la grid (colocación síncrona o doble confirmación).

Ten en cuenta que los metadatos de los objetos no se gestionan mediante reglas de ILM. En su lugar, los metadatos de los objetos se almacenan en una base de datos Cassandra en lo que se conoce como almacén de metadatos. Se mantienen automáticamente tres copias de los metadatos de los objetos en cada sitio para proteger los datos contra la pérdida.

Ejemplo de regla ILM

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

- Aplícalo únicamente a los objetos que pertenecen a Tenant A.
- Crea dos copias replicadas de esos objetos y almacena cada copia en una ubicación diferente.
- Conservar las dos copias «para siempre», lo que significa que StorageGRID no las eliminará automáticamente. En su lugar, StorageGRID conservará estos objetos hasta que sean eliminados mediante una solicitud de eliminación del cliente o hasta que expire el ciclo de vida del bucket.
- Utiliza la opción Equilibrada para el comportamiento de ingesta: la instrucción de distribución en dos sitios se aplica en cuanto Tenant A guarda un objeto en StorageGRID, a menos que no sea posible crear inmediatamente ambas copias requeridas.

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

Cómo evalúa los objetos una política de ILM

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

Cuando los clientes guardan objetos en StorageGRID, los objetos se evalúan según el conjunto ordenado de reglas de ILM de 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 incorpora según el comportamiento de incorporación de esa regla y se almacena según las instrucciones de ubicación de esa regla.
2. Si los filtros de la primera regla no coinciden con el objeto, el objeto se evalúa con cada una de las reglas siguientes 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 de 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 buckets y todas las versiones de los objetos.

Ejemplo de política de ILM

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

- **Regla 1: Copias replicadas para Tenant A**

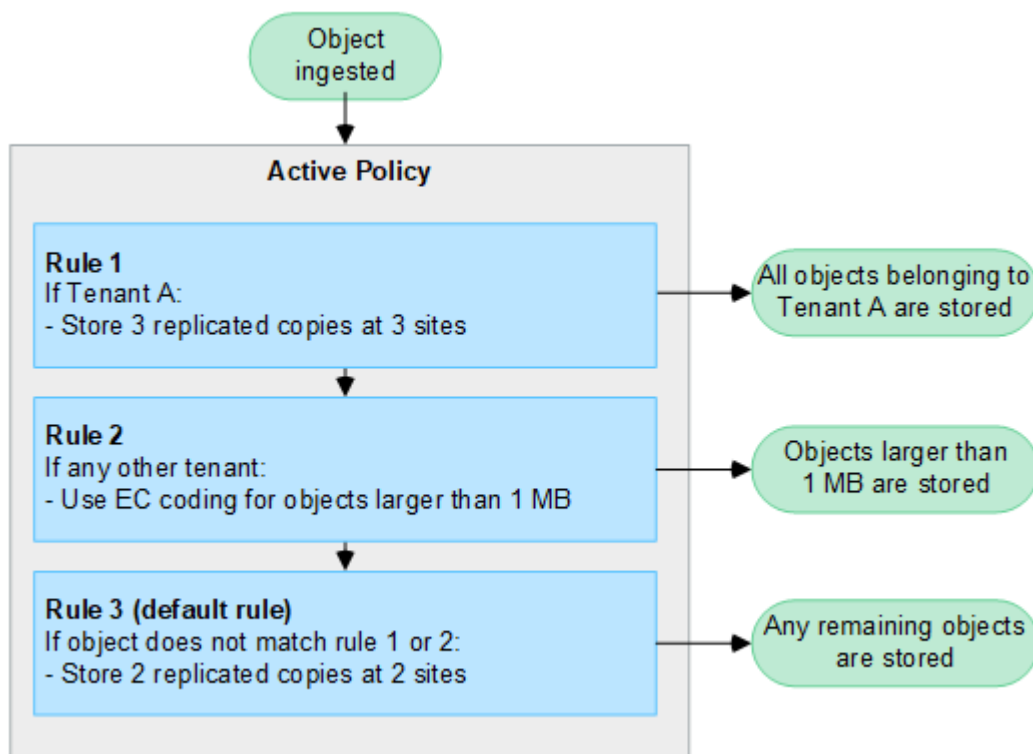
- Selecciona todos los objetos que pertenezcan a Tenant A.
- Almacena estos objetos como tres copias replicadas en tres ubicaciones.
- Los objetos que pertenecen a otros inquilinos no se ajustan a la Regla 1, así que se evalúan según la Regla 2.

- **Regla 2: código de borrado para objetos de más de 1 MB**

- Selecciona todos los objetos de otros tenants, pero solo si superan 1 MB. Estos objetos de mayor tamaño se almacenan utilizando erasure coding 6+3 en tres sitios.
- No coincide con los objetos de 1 MB o menos, así que estos objetos se evalúan según la Regla 3.

- **Regla 3: 2 copias 2 centros de datos** (por defecto)

- Es la última y predeterminada regla de la política. No utiliza filtros.
- Crea dos copias replicadas de todos los objetos que no se ajusten a la Regla 1 ni a la Regla 2 (objetos que no pertenezcan a Tenant A y que tengan un tamaño igual o inferior a 1 MB).



Información relacionada

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

Descubre StorageGRID

Explora el Grid Manager de StorageGRID

Grid Manager es la interfaz gráfica basada en navegador que te permite configurar, gestionar y supervisar tu sistema StorageGRID.



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

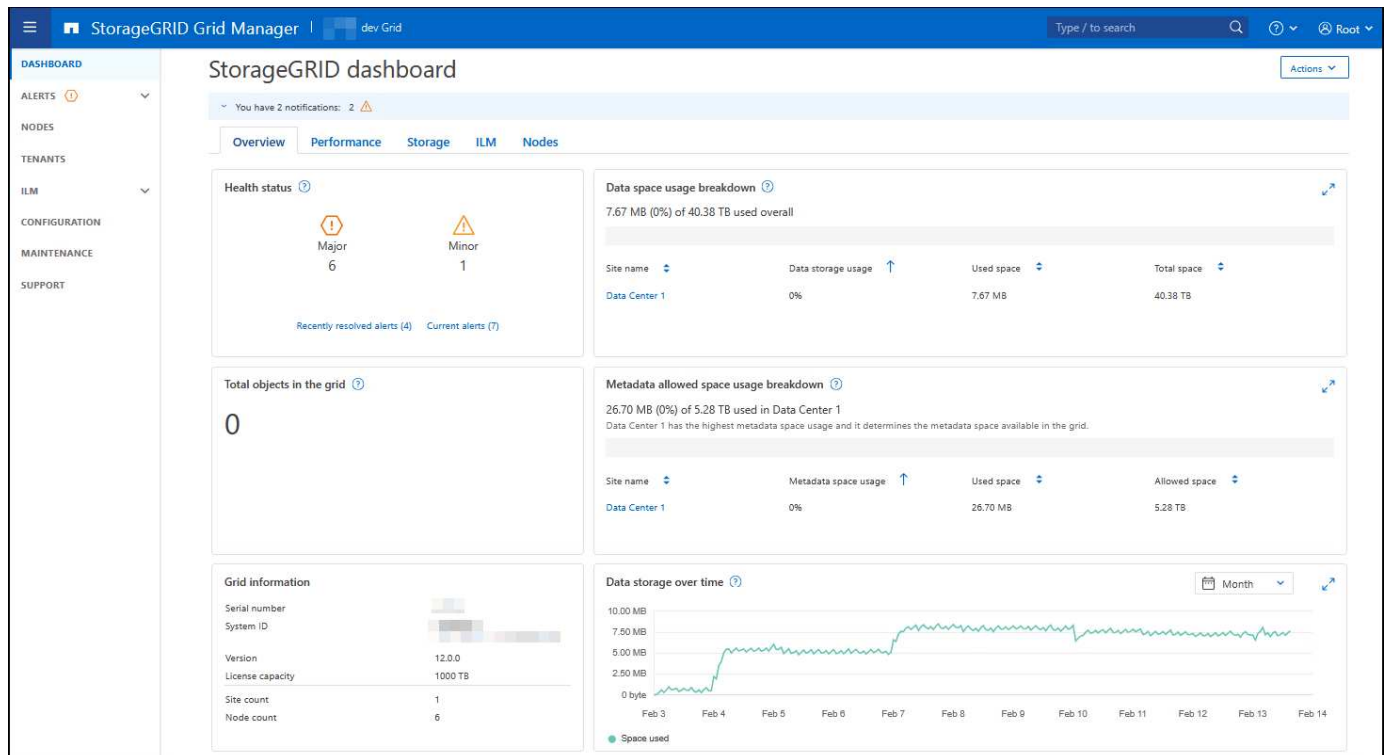
Cuando inicias sesión en Grid Manager, te conectas a un nodo de administración. Cada sistema StorageGRID incluye un nodo de administración principal y cualquier cantidad de nodos de administración no principales. Puedes conectarte a cualquier nodo de administración, y cada nodo de administración muestra una vista similar del sistema StorageGRID.

Puedes acceder al Grid Manager mediante un ["navegador web compatible"](#).

Panel de control de Grid Manager

La primera vez que inicies sesión en Grid Manager, puedes usar el panel de control para ["supervisar las actividades del sistema"](#) de un solo vistazo.

El panel de control contiene información sobre el estado y el rendimiento del sistema, el uso del almacenamiento, los procesos de ILM, las operaciones de S3 y los nodos de la red. Puedes ["configurar el panel de control"](#) seleccionando entre una serie de tarjetas que contienen la información que necesitas para supervisar eficazmente tu sistema.



Para obtener una explicación de la información que aparece en cada tarjeta, selecciona el icono de ayuda (?) para esa tarjeta.

Campo de búsqueda

El campo **Buscar** de la barra de encabezado te permite navegar rápidamente a una página concreta dentro de Grid Manager. Por ejemplo, puedes escribir **km** para acceder a la página del servidor de gestión de claves (KMS).

Puedes usar **Buscar** para encontrar entradas en la barra lateral del Grid Manager y en los menús de Configuration, Maintenance y Support. También puedes buscar por nombre elementos como nodos de grid y

cuentas de tenant.

Menú de ayuda

El menú de ayuda  permite acceder a:

- Los asistentes "[FabricPool](#)" y "[Configuración de S3](#)"
- El sitio web 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» ofrece una interfaz fácil de usar para detectar, evaluar y resolver problemas que puedan surgir durante el funcionamiento de StorageGRID.

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

- Revisa las alertas actuales
- Revisar las alertas resueltas
- Configura los silencios para suprimir las notificaciones de alerta
- Define reglas de alerta para las condiciones que activan las alertas
- Configura el servidor de correo electrónico para las notificaciones de alertas

Página de nodos

El "[Página de nodos](#)" muestra información sobre toda la grid, cada sitio en la grid y cada nodo en un sitio. Para ver información de un sitio o nodo en particular, selecciona el sitio o el nodo.

Página de inquilinos

El "[Página de inquilinos](#)" te permite "[crear y supervisar las cuentas de inquilinos de almacenamiento](#)" para tu sistema StorageGRID. Debes crear al menos una cuenta de inquilino para especificar quién puede almacenar y recuperar objetos y qué funcionalidades están disponibles para ellos.

La página Tenants también ofrece detalles de uso para cada tenant, incluyendo la cantidad de almacenamiento utilizada y el número de objetos. Si configuraste una cuota al crear el tenant, puedes ver cuánto de esa cuota se ha utilizado.

Menú de ILM

El "[Menú de ILM](#)" te permite "[configura las reglas y políticas de gestión del ciclo de vida de la información \(ILM\)](#)" que regulan la durabilidad y la disponibilidad de los datos. También puedes introducir un identificador de objeto para ver los metadatos de ese objeto.

Desde el menú de ILM puedes consultar y gestionar ILM:

- Reglas
- Políticas
- Etiquetas de políticas
- Grupos de almacenamiento

- Grados de almacenamiento
- Regiones
- Búsqueda de metadatos de objetos

Menú de configuración

El menú «Configuración» te permite especificar los ajustes de red, los ajustes de seguridad, los ajustes del sistema, las opciones de supervisión y las opciones de control de acceso.

Tareas de red

Las tareas de red incluyen:

- ["Gestiona grupos de alta disponibilidad"](#)
- ["Gestiona los puntos de conexión del equilibrador de carga"](#)
- ["Configura los nombres de dominio de los endpoints S3"](#)
- ["Gestiona las políticas de clasificación del tráfico"](#)
- ["Configurar interfaces VLAN"](#)
- ["Habilita StorageGRID CORS para una interfaz de gestión"](#)

Tareas de seguridad

Las tareas de seguridad incluyen:

- ["Gestiona certificados de seguridad"](#)
- ["Gestiona los controles del firewall interno"](#)
- ["Configura servidores de gestión de claves"](#)
- Configura los ajustes de seguridad, incluidos ["Política de TLS y SSH"](#), ["Opciones de seguridad de red y de objetos"](#), ["Configuración de seguridad de la interfaz"](#) y ["Opciones de acceso SSH"](#)
- Configura los ajustes de un ["proxy de almacenamiento"](#) o un ["proxy de administración"](#)

Tareas del sistema

Las tareas del sistema incluyen:

- Utiliza ["federación de grid"](#) para clonar la información de las cuentas de los inquilinos y replicar los datos de los objetos entre dos sistemas StorageGRID
- Si lo deseas, activa la opción ["Comprimir los objetos almacenados"](#)
- Si lo deseas, configura el ["Configuración predeterminada de consistencia del bucket"](#)
- ["Gestiona S3 Object Lock"](#)
- Entiende los ajustes de almacenamiento, como ["marcas de nivel de agua en el volumen de almacenamiento"](#)
- ["Gestiona perfiles de código de borrado"](#)

Tareas de monitorización

Las tareas de seguimiento incluyen:

- ["Configura la gestión de registros"](#)
- ["Usa la supervisión SNMP"](#)

Tareas de control de acceso

Las tareas de control de acceso incluyen:

- ["Gestiona grupos de administradores"](#)
- ["Gestionar usuarios administradores"](#)
- Cambia el ["frase de contraseña de aprovisionamiento"](#) o ["contraseñas de la consola del nodo"](#)
- ["Usa la federación de identidades"](#)
- ["Configura SSO"](#)

Menú de mantenimiento

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

Tareas

Las tareas de mantenimiento incluyen:

- ["Operaciones de descomisionamiento"](#) para eliminar nodos y sitios de grid que no se usen
- ["Operaciones de expansión"](#) para añadir nuevos nodos de grid y sitios
- ["Procedimientos de recuperación de nodos de la grid"](#) para sustituir un nodo averiado y restaurar datos
- ["Procedimientos para cambiar el nombre"](#) para cambiar los nombres que se muestran de tu grid, sitios y nodos
- ["Operaciones de comprobación de la existencia de objetos"](#) para verificar la existencia (aunque no la corrección) de los datos de un objeto
- Ejecuta un ["reinicio progresivo"](#) para reiniciar varios nodos de la grid
- ["Operaciones de restauración de volumen"](#)

Sistema

Entre las tareas de mantenimiento del sistema que puedes realizar se incluyen:

- ["Ver la información de la licencia de StorageGRID"](#) o ["Actualizar la información de la licencia"](#)
- Generar y descargar el ["paquete de recuperación"](#)
- Realizar actualizaciones del software StorageGRID, incluidas las actualizaciones de versión, las correcciones urgentes y las actualizaciones del software SANtricity OS en dispositivos seleccionados
 - ["Procedimiento de actualización"](#)
 - ["Procedimiento de corrección urgente"](#)
 - ["Actualiza SANtricity OS en los controladores de almacenamiento SG6000 usando Grid Manager"](#)
 - ["Actualiza SANtricity OS en los controladores de almacenamiento SG5700 usando Grid Manager"](#)

Red

Las tareas de mantenimiento de red que puedes realizar incluyen:

- ["Configura los servidores DNS"](#)
- ["Actualizar las subredes de Grid Network"](#)
- ["Gestionar servidores NTP"](#)

Menú de soporte

El menú Soporte ofrece opciones que ayudan al soporte técnico a analizar y solucionar los problemas de tu sistema.

Herramientas

Desde la sección Herramientas del menú Soporte, puedes:

- ["Configura AutoSupport"](#)
- ["Ejecutar diagnósticos"](#) sobre el estado actual de la grid
- ["Recopilar archivos de registro y datos del sistema"](#)
- ["Revisar las métricas de soporte"](#)



Las herramientas disponibles en la opción **Métricas** están destinadas al soporte técnico. Algunas funciones y opciones de menú de estas herramientas no están operativas de forma intencionada.

Otros

Desde la sección Other del menú Support, puedes:

- Configurar ["Priorización de E/S"](#)
- Configura ["AutoSupport configuración del correo electrónico \(antigua\)"](#)
- Gestionar ["coste del enlace"](#)
- Ver los ID de los servicios de los nodos
- Gestionar ["marcas de agua de almacenamiento"](#)

Explora el Tenant Manager de StorageGRID

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



Tenant Manager se actualiza con cada versión y puede que no coincida con las capturas de pantalla de ejemplo de esta página.

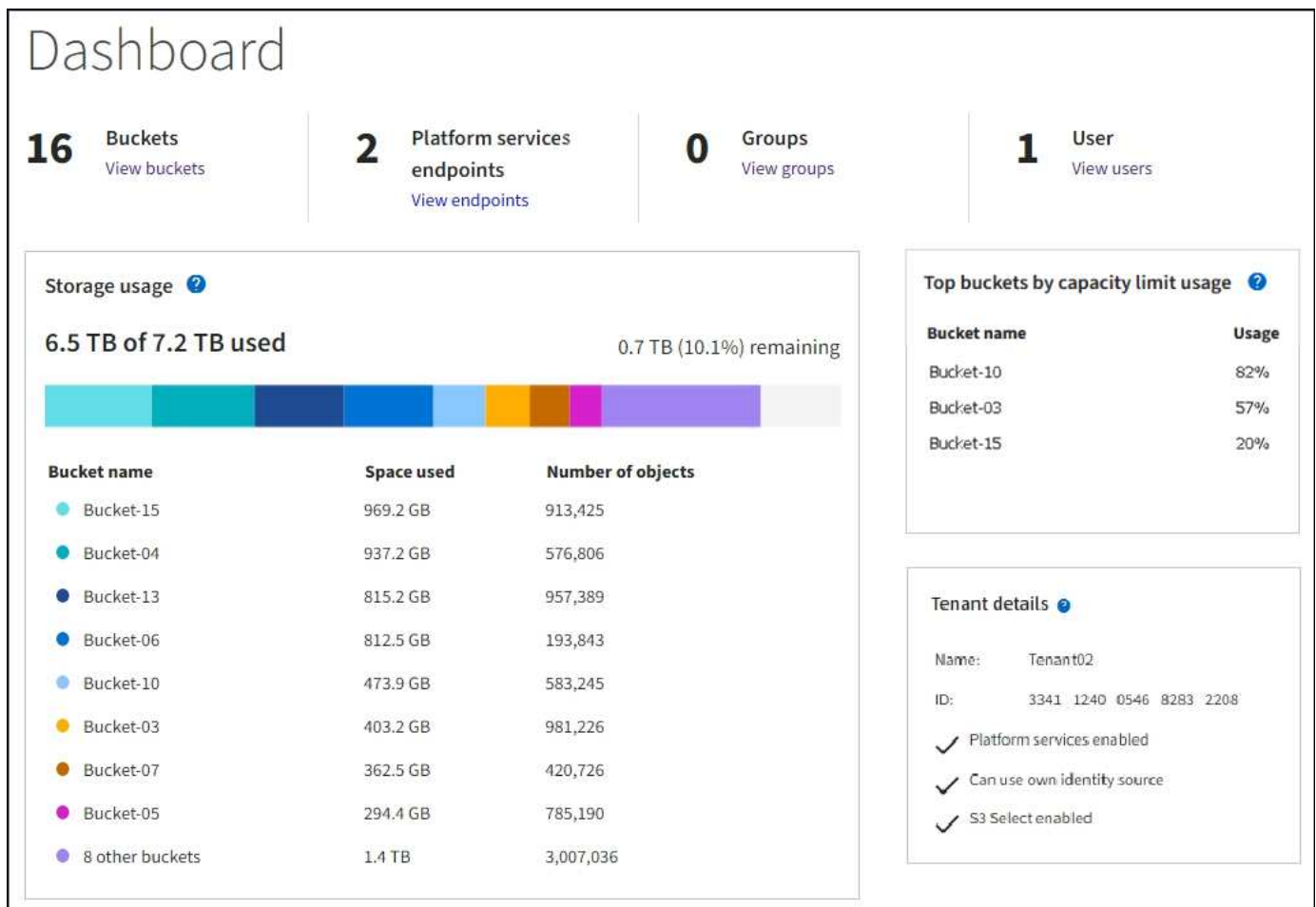
Cuando los usuarios de un inquilino inician sesión en el Tenant Manager, se conectan a un Admin Node.

Panel de control de Tenant Manager

Después de que un administrador de grid crea una cuenta de tenant usando el Grid Manager o la Grid Management API, los usuarios del tenant pueden iniciar sesión en el Tenant Manager.

El panel de control de Tenant Manager permite a los usuarios del inquilino supervisar el uso del almacenamiento de un solo vistazo. El panel «Uso del almacenamiento» contiene una lista de los buckets de S3 más grandes del inquilino. El valor «Espacio utilizado» es la cantidad total de datos de los objetos que hay en el bucket o contenedor. El gráfico de barras representa los tamaños relativos de estos buckets o contenedores.

El valor que aparece encima del gráfico de barras es la suma del espacio utilizado por todos los buckets o contenedores del inquilino. Si al crear la cuenta se especificó el número máximo de gigabytes, terabytes o petabytes disponibles para el inquilino, también se muestran la cantidad de cuota utilizada y la restante.



Menú de almacenamiento (S3)

Este menú permite a los usuarios de S3:

- Gestionar claves de acceso
- Crear, gestionar y eliminar buckets
- Gestiona los puntos de conexión de los servicios de la plataforma
- Ver cualquier conexión de la federación de grid que tengan permiso para usar

Mis claves de acceso

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

- Los usuarios que tengan el permiso «Gestionar tus propias credenciales de S3» pueden crear o eliminar sus propias claves de acceso a S3.
- Los usuarios que disponen de permisos de acceso root pueden gestionar las claves de acceso de la cuenta root de S3, de su propia cuenta y de todos los demás usuarios. Las claves de acceso root también proporcionan acceso completo a los buckets y objetos del tenant, a menos que una política de bucket lo desactive explícitamente.



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

Buckets

Los usuarios de un tenant de S3 que cuenten con los permisos adecuados pueden realizar las siguientes tareas en sus buckets:

- Crear buckets
- Habilita S3 Object Lock para un nuevo bucket (se da por hecho que S3 Object Lock está habilitado para el sistema StorageGRID)
- Actualizar los valores de consistencia
- Activar y desactivar las actualizaciones del tiempo de acceso
- Activar o suspender el control de versiones de los objetos
- Actualizar la retención predeterminada de S3 Object Lock
- Configura el intercambio de recursos entre orígenes (CORS)
- Eliminar todos los objetos de un bucket
- Eliminar contenedores vacíos
- Utiliza la "[Consola de S3](#)" para gestionar los objetos del bucket

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

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

Puntos de conexión de los servicios de plataforma

Si un administrador de grid ha habilitado el uso de servicios de plataforma para la cuenta de tenant, un usuario de S3 con el permiso de Manage endpoints puede configurar un endpoint de destino para cada servicio de plataforma.

Conexiones de grid federation

Si un administrador de grid ha habilitado el uso de una conexión de federación de grid para la cuenta de tenant, un usuario de S3 con permiso de acceso Root puede ver el nombre de la conexión, acceder a la página de detalles del bucket para cada bucket que tenga habilitada la replicación entre grids y ver el error más reciente que haya ocurrido al replicar los datos del bucket al otro grid en la conexión. Consulta ["Ver conexiones de la federación de grid"](#).

Menú de gestión de accesos

El menú «Gestión de accesos» permite a los inquilinos de StorageGRID importar grupos de usuarios desde una fuente de identidad federada y asignar permisos de gestión. Los inquilinos también pueden gestionar grupos y usuarios locales del inquilino, salvo que se haya habilitado el inicio de sesión único (SSO) para todo el sistema StorageGRID.

Directrices de redes

Directrices de red para StorageGRID

Utiliza estas directrices para conocer la arquitectura y las topologías de red de StorageGRID y para conocer los requisitos para la configuración y el aprovisionamiento de red.

Acerca de estas instrucciones

Estas directrices proporcionan información que puedes usar para crear la infraestructura de red de StorageGRID antes de implementar y configurar los nodos de StorageGRID. Usa estas directrices para ayudar a asegurar que la comunicación pueda ocurrir entre todos los nodos de la grid y entre la grid y los clientes y servicios externos.

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

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

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

Antes de empezar

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

Antes de configurar la red, familiarízate con la arquitectura de StorageGRID tal y como se describe en

["Conoce StorageGRID"](#).

Una vez que determines qué redes StorageGRID quieres usar y cómo se configurarán esas redes, puedes instalar y configurar los nodos de StorageGRID siguiendo las instrucciones adecuadas.

Instala nodos de appliance

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

Instala nodos basados en software

- ["Instalar StorageGRID en nodos basados en software"](#)

Configura y administra el software StorageGRID

- ["Administrar StorageGRID"](#)
- ["Notas de publicación"](#). Debes iniciar sesión con tu cuenta de NetApp o crear una cuenta para acceder a las notas de la versión.

Tipos de redes StorageGRID

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

Tipos de tráfico

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

Puedes configurar la red de las siguientes maneras:

- Solo red de grid
- Redes Grid y de administración
- Red de grid y de clientes
- Redes Grid, Admin y Client

La red Grid es obligatoria y puede gestionar todo el tráfico de red. Las redes Admin y Client pueden incluirse en el momento de la instalación o añadirse después para adaptarse a los cambios en los requisitos. Aunque las redes Admin y Client son opcionales, cuando usas estas redes para manejar el tráfico administrativo y de

los clientes, la red Grid puede quedar aislada y segura.

Solo se puede acceder a los puertos internos a través de la Grid Network. Se puede acceder a los puertos externos desde cualquier tipo de red. Esta flexibilidad ofrece múltiples opciones para diseñar una implementación de StorageGRID y configurar el filtrado de direcciones IP y puertos externos en switches y firewalls. Consulta ["comunicaciones internas entre nodos de la grid"](#) y ["comunicaciones externas"](#).

Interfaces de red

Los nodos de StorageGRID se conectan a cada red mediante las siguientes interfaces específicas:

Red	Nombre de la interfaz
Red de grid (obligatorio)	eth0
Red de administración (opcional)	eth1
Red de clientes (opcional)	eth2

Para obtener más información sobre cómo asignar puertos virtuales o físicos a las interfaces de red de los nodos, consulta ["Instalar StorageGRID en nodos basados en software"](#).

Nodos de appliance

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

Información de red de cada nodo

Debes configurar lo siguiente para cada red que actives en un nodo:

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

Solo puedes configurar una combinación de dirección IP, máscara y puerta de enlace para cada una de las tres redes en cada nodo de la red. Si no quieres configurar una puerta de enlace para una red, deberías usar la dirección IP como dirección de puerta de enlace.

Grupos de alta disponibilidad

Los grupos de alta disponibilidad (HA) permiten añadir direcciones IP virtuales (VIP) a la interfaz de red Grid o Client. Para obtener más información, consulta ["Gestiona grupos de alta disponibilidad"](#).

Red de grid

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



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

La red Grid se puede utilizar para todo el tráfico de administración y todo el tráfico de cliente, incluso si se han configurado la red de administración y la red de cliente. 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 de cliente.



Al configurar la red Grid, debes asegurarte de que la red esté protegida frente a clientes no fiables, como los que se encuentran en la internet pública.

Ten en cuenta los siguientes requisitos y detalles para la pasarela de Grid Network:

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

Red de administración

La red de administración es opcional. Cuando se configura, puede usarse para el tráfico de administración y mantenimiento del sistema. La red de administración suele ser una red privada y no necesita ser enrutable entre nodos.

Puedes elegir en qué nodos de la grid se debe activar la red de administración.

Cuando usas la red de administración, el tráfico administrativo y de mantenimiento no necesita viajar a través de la Grid Network. Entre los usos habituales de la red de administración se 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 externos de gestión de claves (KMS) y servidores Lightweight Directory Access Protocol (LDAP).
- Acceso a los registros de auditoría en los nodos de administración.
- Acceso mediante el protocolo Secure Shell (SSH) para tareas de mantenimiento y soporte.

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

Ten en cuenta los siguientes requisitos y detalles para la pasarela de red de administración:

- La puerta de enlace de la red de administración es necesaria si se van a establecer conexiones desde fuera de la subred de la red de administración o si se han configurado varias subredes de la red de administración.
- Se crean rutas estáticas para cada subred configurada en la lista de subredes de red de administración del nodo.

Red de clientes

La red de clientes es opcional. Cuando se configura, se utiliza para proporcionar acceso a los servicios de grid a aplicaciones cliente como S3. Si planeas hacer que los datos de StorageGRID sean accesibles para un recurso externo (por ejemplo, un Cloud Storage Pool o el servicio de replicación StorageGRID CloudMirror), el recurso externo también puede usar la red de clientes. Los nodos de grid pueden comunicarse con cualquier subred a la que se pueda acceder a través de la puerta de enlace de la red de clientes.

Puedes elegir en qué nodos de la grid quieres habilitar la Client Network. No es necesario que todos los nodos estén en la misma Client Network, y los nodos nunca se comunicarán entre sí a través de la Client Network. La Client Network no se vuelve operativa hasta que se completa la instalación de la grid.

Para mayor seguridad, puedes especificar que la interfaz de red de cliente de un nodo no sea de confianza, de modo que la red de cliente sea más restrictiva a la hora de permitir conexiones. Si la interfaz de red de cliente de un nodo no es de confianza, la interfaz acepta conexiones salientes, como las que utiliza la replicación de CloudMirror, pero solo acepta conexiones entrantes en los puertos que se hayan configurado explícitamente como puntos finales del equilibrador de carga. Consulta ["Gestiona los controles del cortafuegos"](#) y ["Configura los puntos de conexión del equilibrador de carga"](#).

Cuando usas una Client Network, el tráfico de los clientes no tiene que pasar por la Grid Network. El tráfico de la Grid Network puede separarse en una red segura y no enrutable. Los siguientes tipos de nodos suelen configurarse con una Client Network:

- Nodos de puerta de enlace, ya que estos nodos proporcionan acceso al servicio StorageGRID Load Balancer y acceso de cliente S3 a la grid.
- Nodos de almacenamiento, porque estos nodos proporcionan acceso al protocolo S3, a los Cloud Storage Pools y al servicio de replicación CloudMirror.
- Nodos de administración, para garantizar que los usuarios del inquilino puedan conectarse al Tenant Manager sin necesidad de utilizar la Admin Network.

Ten en cuenta lo siguiente respecto a la puerta de enlace de la red de clientes:

- La pasarela de la red de clientes es necesaria si se ha configurado la red de clientes.
- La pasarela de la red de clientes se convierte en la ruta predeterminada para el nodo de la red cuando se completa la configuración de la red.

Redes VLAN opcionales

Si es necesario, puedes utilizar opcionalmente redes LAN virtuales (VLAN) para el tráfico de clientes y para algunos tipos de tráfico de administración. Sin embargo, el tráfico de Grid no puede usar una interfaz VLAN. El tráfico interno de StorageGRID entre nodos debe usar siempre la red Grid en eth0.

Para habilitar el uso de VLAN, debes configurar una o varias interfaces de un nodo como interfaces de enlace troncal en el conmutador. Puedes configurar la interfaz de red Grid Network (eth0) o la interfaz de red Client Network (eth2) como enlace troncal, o bien puedes añadir interfaces de enlace troncal al nodo.

Si eth0 está configurada como un trunk, el tráfico de red Grid fluye a través de la interfaz nativa del trunk,

como está configurado en el switch. De manera similar, si eth2 está configurada como un trunk y la Client Network también está configurada en el mismo nodo, la Client Network usa la VLAN nativa del puerto trunk como está configurado en el switch.

Solo se admite el tráfico de administración entrante, como el utilizado para SSH, Grid Manager o Tenant Manager, en las redes VLAN. El tráfico saliente, como el utilizado para NTP, DNS, LDAP, KMS y Cloud Storage Pools, no es compatible con las redes VLAN.



Las interfaces VLAN solo se pueden añadir a los nodos de administración y a los nodos de puerta de enlace. No puedes usar una interfaz VLAN para el acceso de clientes o de administración a los nodos de almacenamiento.

Consulta ["Configurar interfaces VLAN"](#) para obtener instrucciones y directrices.

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

Ejemplos de topología de red

Topología de red Grid para StorageGRID

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

Cuando configuras la Grid Network, estableces la dirección IP del host, la máscara de subred y la dirección IP de la puerta de enlace para la interfaz eth0 de cada nodo de grid.

Durante la configuración, debes añadir 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 proporcionan acceso a servicios críticos como NTP, DNS o LDAP.

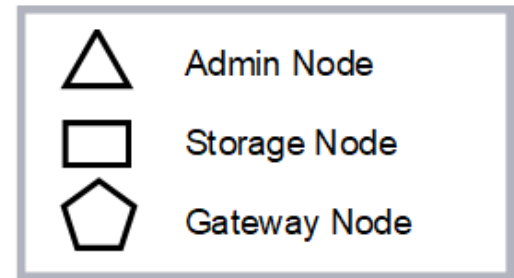
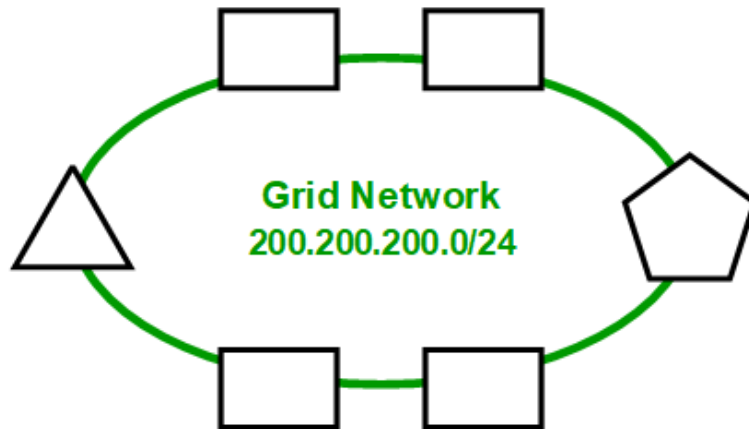
Durante la instalación, la interfaz de Grid Network aplica rutas estáticas para todas las subredes en la GNSL y establece la ruta predeterminada del nodo hacia la puerta de enlace de Grid Network si se ha configurado una. La GNSL no es necesaria si no hay red de clientes y la puerta de enlace de Grid Network es la ruta predeterminada del nodo. También se generan rutas de host hacia todos los demás nodos en el grid.

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



Esta topología es adecuada para implementaciones en un único sitio que no estén disponibles externamente, para implementaciones de prueba de concepto o de prueba, o cuando un equilibrador de carga de terceros actúa como límite de acceso de los clientes. Siempre que sea posible, la red Grid debe usarse exclusivamente para el tráfico interno. Tanto la red Admin como la red Client tienen restricciones adicionales de firewall que bloquean el tráfico externo hacia 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 red de administración para StorageGRID

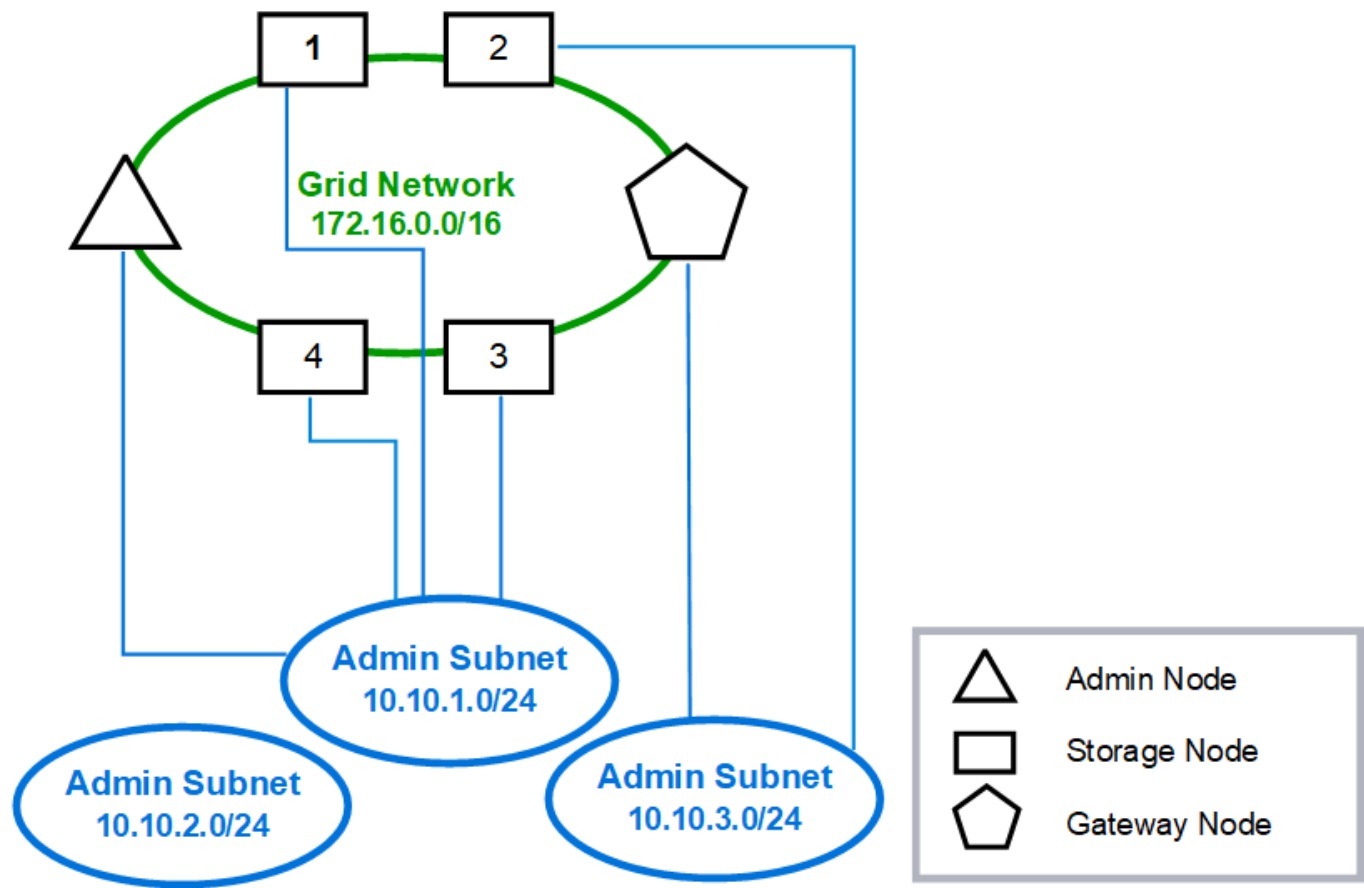
Disponer de una red de administración es opcional. Una forma de utilizar una red de administración y una red de Grid es configurar una red de Grid enrutable y una red de administración delimitada para cada nodo.

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

La red de administración puede ser única para cada nodo y puede estar formada por varias subredes. Cada nodo puede configurarse con una Admin External Subnet List (AESL). La AESL enumera las subredes a las que se puede acceder a través de la red de administración para cada nodo. La AESL también debe incluir las subredes de cualquier servicio al que la grid acceda a través de la red de administración, como NTP, DNS, KMS y LDAP. Se aplican rutas estáticas para cada subred de la AESL.

En este ejemplo, la red Grid se utiliza para el tráfico relacionado con las solicitudes de clientes S3 y la gestión de objetos, mientras que la red Admin 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 de cliente para StorageGRID

Disponer de una red de cliente es opcional. Usar una red de cliente permite que el tráfico de red de cliente (por ejemplo, S3) se separe del tráfico interno de la grid, lo que permite que la red de la grid sea más segura. El tráfico administrativo puede gestionarse tanto por la red de cliente como por la red de la grid cuando la red de administración no está configurada.

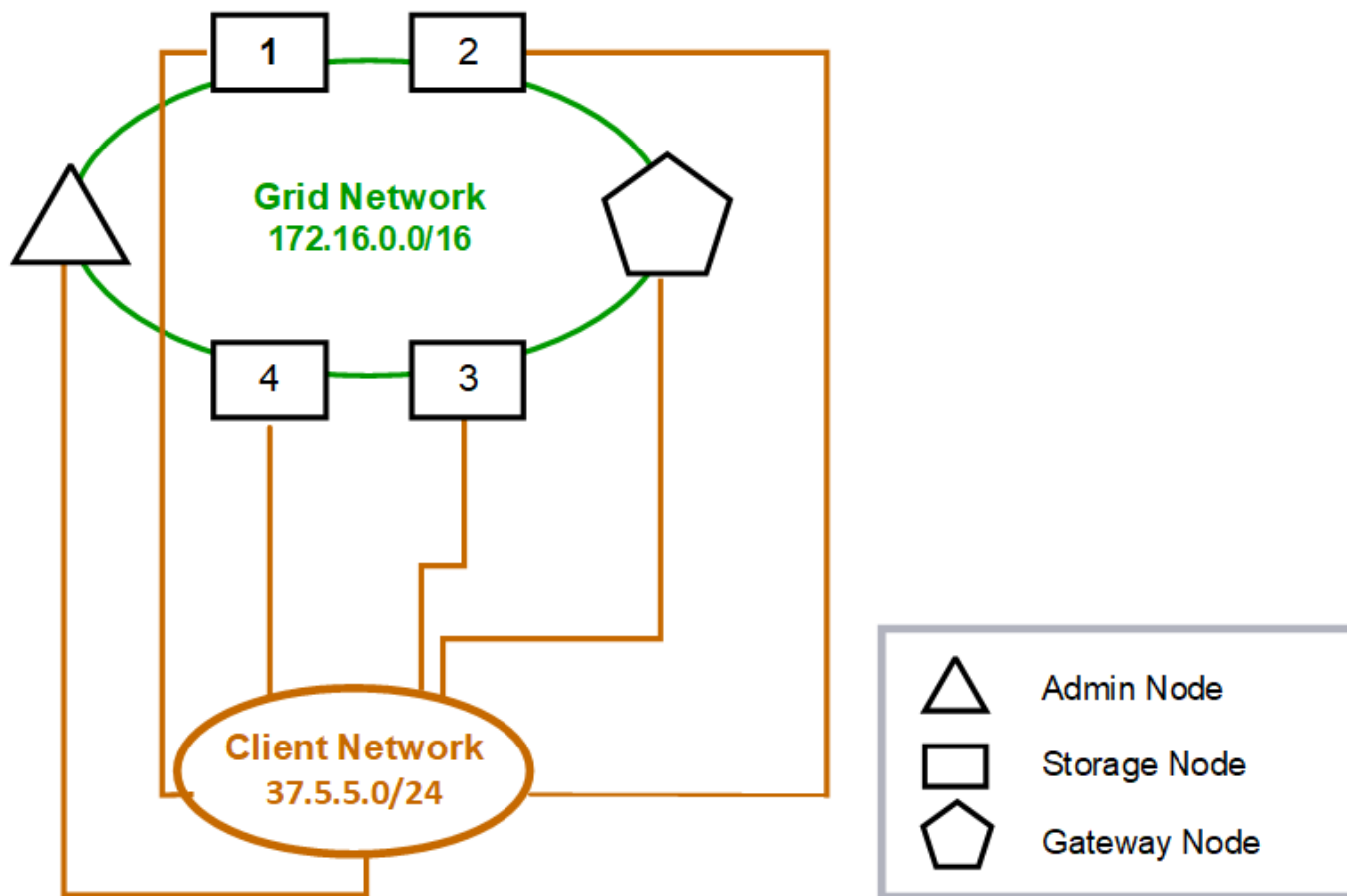
Cuando configuras la red de cliente, estableces la dirección IP del host, la máscara de subred y la dirección IP de la puerta de enlace para la interfaz eth2 del nodo configurado. La red de cliente de cada nodo puede ser independiente de la red de cliente de cualquier otro nodo.

Si configuras una Client Network para un nodo durante la instalación, la puerta de enlace predeterminada del nodo cambia de la puerta de enlace de la Grid Network a la puerta de enlace de la Client Network cuando termina la instalación. Si se añade una Client Network después, la puerta de enlace predeterminada del nodo cambia de la misma manera.

En este ejemplo, la Client Network se utiliza para las solicitudes de clientes S3 y para funciones

administrativas, mientras que la Grid Network se dedica a las operaciones internas de gestión de objetos.

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

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

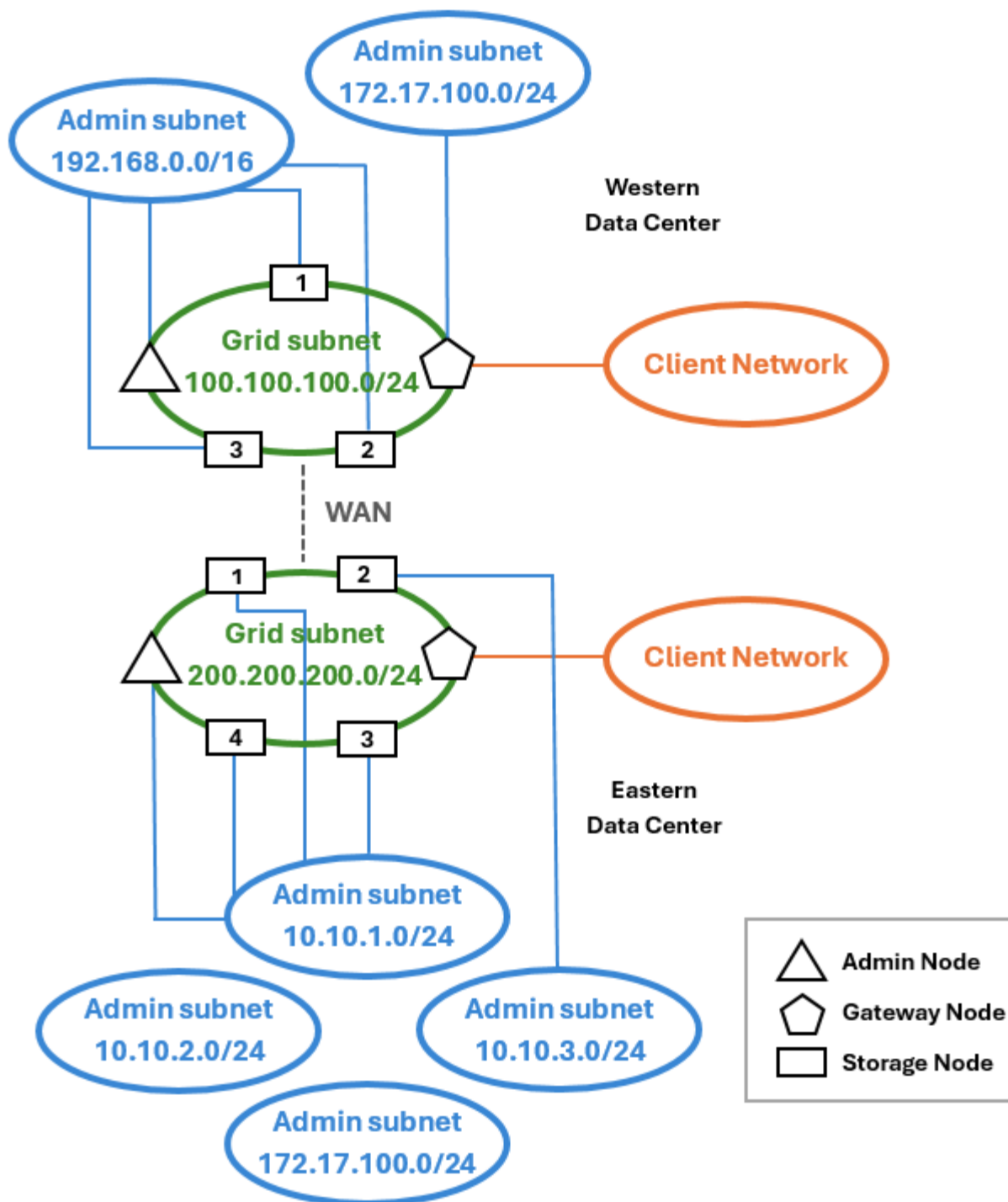
Topología de red para las tres redes StorageGRID

Puedes configurar las tres redes en una topología de red compuesta por una red Grid privada, redes Admin específicas de cada sitio y redes Client abiertas. Usar endpoints de load balancer y redes Client no confiables puede proporcionar seguridad adicional si es necesario.

En este ejemplo:

- La red Grid se utiliza para el tráfico de red relacionado con las operaciones internas de gestión de objetos.
- La red de administración se utiliza para el tráfico relacionado con las funciones administrativas.
- La red de clientes se usa para el tráfico relacionado con las solicitudes de cliente S3.

Ejemplo de topología: Grid, Admin y Client Networks



Requisitos de red para StorageGRID

Debes comprobar que la infraestructura de red y la configuración actuales pueden admitir el diseño de red de StorageGRID previsto.

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 combinaciones de estas redes como se muestra en los ejemplos de topología de red.

- **Conexiones de administración:** Conexiones entrantes desde un administrador al nodo, normalmente a través de SSH. Acceso web al Grid Manager, al Tenant Manager y al StorageGRID Appliance Installer.
- **Conexiones al servidor NTP:** Conexión UDP saliente que recibe una respuesta UDP entrante.

Al menos un servidor NTP debe ser accesible por el nodo de administración principal.

- **Conexiones al servidor DNS:** conexión UDP saliente que recibe una respuesta UDP entrante.
- **Conexiones con el 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 hacia `support.netapp.com` o un proxy configurado por el cliente.
- **Servidor externo de gestión de claves:** Conexión TCP saliente desde cada nodo del appliance con el cifrado de nodo habilitado.
- Conexiones TCP entrantes de clientes S3.
- Solicitudes salientes de servicios de la plataforma StorageGRID, como la replicación de CloudMirror o de Cloud Storage Pools.

Si StorageGRID no puede establecer contacto con ninguno de los servidores NTP o DNS provisionados utilizando las reglas de enrutamiento predeterminadas, intentará automáticamente establecer contacto en todas las redes (Grid, Admin y Client), siempre y cuando se hayan especificado las direcciones IP de los servidores DNS y NTP. Si se puede acceder a los servidores NTP o DNS desde cualquier red, StorageGRID creará automáticamente reglas de enrutamiento adicionales para garantizar que se utilice esa red en todos los intentos futuros de conexión.



Aunque puedes utilizar estas rutas de host detectadas automáticamente, en general deberías configurar manualmente las rutas de DNS y NTP para garantizar la conectividad en caso de que falle la detección automática.

Si aún no estás preparado para configurar las redes opcionales de administración y de clientes durante la implementación, puedes configurarlas cuando apruebes los nodos de la red durante los pasos de configuración. Además, puedes configurar estas redes después de la instalación, usando la herramienta Change IP (consulta "[Configurar direcciones IP](#)").

Solo se admiten las conexiones de cliente S3 y las conexiones administrativas de SSH, Grid Manager y Tenant Manager a través de interfaces VLAN. Las conexiones salientes, como a NTP, DNS, LDAP, AutoSupport y servidores KMS, deben ir directamente por las interfaces Client, Admin o Grid Network. Si la interfaz está configurada como un tronco para admitir interfaces VLAN, este tráfico irá por la VLAN nativa de la interfaz, según lo configurado en el switch.

Redes de área amplia (WAN) para múltiples sitios

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

Los requisitos mínimos reales de ancho de banda WAN dependen de la actividad de los clientes y del esquema de protección ILM. Si necesitas ayuda para calcular los requisitos mínimos de ancho de banda WAN, contacta a tu consultor de Servicios Profesionales de NetApp.

Conexiones para los nodos de administración y los nodos de gateway

Los nodos de administración deben protegerse siempre frente a clientes no fiables, como los que se encuentran en la red pública de Internet. Debes asegurarte de que ningún cliente no fiable 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 planeas añadir a grupos de alta disponibilidad deben configurarse con una dirección IP estática. Para más información, consulta ["Gestiona grupos de alta disponibilidad"](#).

Uso de la traducción de direcciones de red (NAT)

No utilices la traducción de direcciones de red (NAT) en la Grid Network entre nodos de la grid o entre sitios de StorageGRID. Cuando uses direcciones IPv4 privadas para la Grid Network, esas direcciones deben ser directamente enrutables desde cada nodo de la grid en cada sitio. Sin embargo, si es necesario, puedes usar NAT entre clientes externos y nodos de la grid, por ejemplo, para proporcionar una dirección IP pública a un Gateway Node. El uso de NAT para conectar un segmento de red pública solo está permitido cuando empleas una aplicación de túnel que sea transparente para todos los nodos de la grid, es decir, los nodos de la grid no necesitan conocer las direcciones IP públicas.

Requisitos específicos de red para StorageGRID

Sigue los requisitos para cada tipo de red StorageGRID.

Pasarelas de red y routers

- Si se configura, la puerta de enlace de una red determinada debe estar dentro de la subred de esa red.
- Si configuras una interfaz con direccionamiento estático, debes especificar una dirección de puerta de enlace distinta de 0.0.0.0.
- Si no dispones de una puerta de enlace, lo más recomendable es configurar la dirección de la puerta de enlace como la dirección IP de la interfaz de red.

Subredes



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

El Grid Manager aplica las siguientes restricciones durante la implementación. Se incluyen aquí para ayudarte en la planificación de la red previa a la implementación.

- La máscara de subred de cualquier dirección IP de red no puede ser 255.255.255.254 ni 255.255.255.255 (/31 o /32 en notación CIDR).
- La subred definida por la dirección IP y la máscara de subred (CIDR) de una interfaz de red no puede solaparse con la subred de ninguna otra interfaz configurada en el mismo nodo.
- No utilices subredes que contengan las siguientes direcciones IPv4 para la Grid Network, Admin Network o Client Network de ningún nodo:
 - 192.168.130.101
 - 192.168.130.121
 - 192.168.131.101
 - 192.168.131.121

- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 198.51.100.2
- 198.51.100.4

Por ejemplo, no utilices los siguientes rangos de subred para la Grid Network, Admin Network o Client Network 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 Grid Network correspondiente a cada nodo debe figurar en el GNSL.
- La subred Admin Network no puede solaparse con la subred Grid Network, la subred Client Network ni con ninguna subred del GNSL.
- Las subredes de la AESL no pueden solaparse con ninguna subred de la GNSL.
- La subred de la Client Network no puede solaparse con la subred de la Grid Network, la subred de la Admin Network, ninguna subred en el GNSL ni ninguna subred en el AESL.

Red de grid

- En el tiempo de puesta en marcha, cada nodo de grid debe estar conectado a la Grid Network y debe poder comunicarse con el primary Admin Node utilizando la configuración de red que especifiques al implementar el nodo.
- Durante el funcionamiento normal de la grid, cada nodo de la grid debe poder comunicarse con todos los demás nodos a través de la Grid Network.



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 Grid está formada por varias subredes, añádelas a la lista de subredes de la red Grid (GNSL). Se crean rutas estáticas en todos los nodos para cada subred de la GNSL.
- Si la interfaz de red Grid está configurada como un trunk para admitir interfaces VLAN, la trunk native VLAN debe ser la VLAN utilizada para el tráfico de red Grid. Todos los nodos de la red Grid deben ser accesibles a través de la trunk native VLAN.

Red de administración

La red de administración es opcional. Si planeas configurar una red de administración, sigue estos requisitos y directrices.

Entre los usos habituales de la red de administración se incluyen las conexiones de gestión, AutoSupport, KMS y las conexiones a servidores críticos como NTP, DNS y LDAP si estas conexiones no se proporcionan a través de la red de grid o la red de clientes.



La red de administración y la AESL pueden ser únicas para cada nodo, siempre y cuando los servicios de red y los clientes deseados sean accesibles.



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

Red de clientes

La red de clientes es opcional. Si planeas configurar una red de clientes, ten en cuenta las siguientes consideraciones.

- La red de clientes está diseñada para gestionar el tráfico procedente de clientes de S3. Si se configura, la puerta de enlace de la red de clientes se convierte en la puerta de enlace predeterminada del nodo.
- Si utilizas una red de clientes, puedes ayudar a proteger StorageGRID frente a ataques hostiles aceptando el tráfico entrante de clientes únicamente en los endpoints del equilibrador de carga configurados explícitamente. Consulta ["Configura los puntos de conexión del equilibrador de carga"](#).
- Si la interfaz de red del cliente está configurada como un enlace troncal para admitir interfaces VLAN, plantéate si es necesario configurar la interfaz de red del cliente (eth2). Si se configura, el tráfico de red del cliente discurrirá por la VLAN nativa del enlace troncal, como se haya configurado en el conmutador.

Información relacionada

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

Consideraciones sobre redes específicas de la implementación

Configuración de red para implementaciones de StorageGRID Linux

Para garantizar la eficiencia, la fiabilidad y la seguridad, el sistema StorageGRID se ejecuta en Linux como un conjunto de motores de contenedores. En un sistema StorageGRID no es necesario realizar ninguna configuración de red relacionada con los motores de contenedores.

Utiliza un dispositivo no vinculado, como una VLAN o un par de interfaces Ethernet virtuales (veth), como interfaz de red del contenedor. Especifica este dispositivo como la interfaz de red en el archivo de configuración del nodo.



No utilices dispositivos «bond» o «bridge» directamente como interfaz de red del contenedor. Si lo haces, podrías impedir el arranque del nodo debido a un problema del núcleo relacionado con el uso de «macvlan» con dispositivos «bond» y «bridge» en el espacio de nombres del contenedor.

Consulta el ["instrucciones de instalación"](#).

Configuración de la red del host para implementaciones del motor de contenedores

Antes de iniciar la implementación de StorageGRID en una plataforma de motor de contenedores, determina qué redes (Grid, Admin, Client) utilizará cada nodo. Debes asegurarte de que la interfaz de red de cada nodo esté configurada en la interfaz del host virtual o física correcta y de que cada red disponga de ancho de banda suficiente.

Servidores físicos

Si utilizas servidores físicos para alojar los nodos de la red:

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



Una interfaz física del host puede ser utilizada tanto por el propio host como por uno o varios nodos que se ejecuten en el host. Las direcciones IP asignadas al host o a los nodos que utilicen esta interfaz deben ser únicas. El host y el nodo no pueden compartir direcciones IP.

- Abre los puertos necesarios para el host.
- Si tienes previsto utilizar interfaces VLAN en StorageGRID, el host debe tener una o más interfaces trunk que proporcionen acceso a las VLAN deseadas. Estas interfaces pueden pasarse al contenedor del nodo como eth0, eth2 o como interfaces adicionales. Para añadir interfaces trunk o de acceso, consulta lo siguiente:
 - **Linux (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Linux (después de instalar el nodo):** ["Agrega interfaces trunk o de acceso a un nodo"](#)



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Recomendaciones sobre el ancho de banda mínimo

La siguiente tabla recoge las recomendaciones de ancho de banda mínimo de LAN para cada tipo de nodo de StorageGRID y cada tipo de red. Debes dotar a cada host físico o virtual de suficiente ancho de banda de red para cumplir los requisitos mínimos de ancho de banda de agregado correspondientes al número total y al tipo de nodos de StorageGRID que tengas previsto ejecutar en dicho host.

Tipo de nodo	Tipo de red		
	Grid	Administrador	Cliente
	Ancho de banda LAN mínimo	Administrador	10 Gbps
1 Gbps	1 Gbps	Pasarela	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 estás usando almacenamiento compartido al que se accede por Ethernet (iSCSI o FCoE), deberías aprovisionar interfaces físicas independientes en cada host para proporcionar suficiente ancho de banda SAN. Para evitar introducir un cuello de botella, el ancho de banda SAN para un host determinado debería coincidir aproximadamente con el ancho de banda de red agregado de los Storage Node para todos los Storage Node que se ejecutan en ese host.

Usa la tabla para determinar el número mínimo de interfaces de red que debes habilitar en cada host, según el número y tipo de nodos de StorageGRID que planeas 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 único host:

- Conecta las redes Grid y Admin en el nodo de administración (se requieren $10 + 1 = 11$ Gbps)
- Conecta las redes Grid y de clientes en el nodo de gateway (se requieren $10 + 10 = 20$ Gbps)
- Conecta la red Grid en el nodo de almacenamiento (requiere 10 Gbps)

En este escenario, deberías proporcionar un mínimo de $11 + 20 + 10 = 41$ Gbps de ancho de banda de red, lo que podría cubrirse con dos interfaces de 40 Gbps o cinco de 10 Gbps, que podrían agregarse en troncales y luego compartirse entre las tres o más VLANs que transportan las subredes Grid, Admin y Client, locales al centro de datos físico que contiene el host.

Para conocer algunas recomendaciones sobre cómo configurar los recursos físicos y de red en los hosts de tu clúster de StorageGRID con el fin de preparar la implementación de StorageGRID, consulta ["Configura la red del host"](#).

Redes y puertos para servicios de plataforma y Cloud Storage Pools

Si tienes previsto utilizar los servicios de la plataforma StorageGRID o los Cloud Storage Pools, debes configurar la red de grid y los cortafuegos para garantizar que se pueda acceder a los endpoints de destino.

Redes para servicios de plataforma

Tal y como se describe en ["Gestiona los servicios de la plataforma para los inquilinos"](#) y ["Gestiona 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 la plataforma requieren que los nodos de almacenamiento que alojan el servicio StorageGRID ADC tengan acceso a los puntos finales de los servicios externos. Entre los ejemplos de cómo proporcionar dicho acceso se incluyen:

- En los nodos de almacenamiento con servicios ADC, configura redes de administración únicas con entradas AESL que enruten hacia los endpoints de destino.
- Utiliza la ruta predeterminada que proporciona una Client Network. Si utilizas la ruta predeterminada, puedes usar el ["Función untrusted Client Network"](#) para restringir las conexiones entrantes.

Redes para Cloud Storage Pools

Los grupos de almacenamiento en la nube también requieren que los nodos de almacenamiento tengan acceso a los puntos finales proporcionados por el servicio externo utilizado, como Amazon S3 Glacier o el

almacenamiento de blobs de Microsoft Azure. Para obtener más información, consulta "[¿Qué es un grupo de almacenamiento en la nube?](#)".

Puertos para servicios de plataforma y Cloud Storage Pools

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

- **80:** Para los URI de puntos finales que comienzan con `http`
- **443:** Para los URI de puntos finales que comienzan con `https`

Se puede especificar un puerto diferente al crear o editar el punto final. Consulta "[Referencia de puertos de red](#)".

Si utilizas un proxy no transparente, también debes "[configura los ajustes del proxy de almacenamiento](#)" para permitir el envío de mensajes a puntos finales externos, como un punto final en internet.

VLANs, servicios de plataforma y Cloud Storage Pools

No puedes usar redes VLAN para servicios de plataforma ni para Cloud Storage Pools. Los endpoints de destino deben ser accesibles a través de la red Grid, Admin o Client.

Configuración de red para nodos de StorageGRID appliance

Puedes configurar los puertos de red de los dispositivos StorageGRID para que utilicen los modos de agrupación de puertos que mejor se adapten a tus necesidades de rendimiento, redundancia y conmutación por error.

Los puertos de 10/25 GbE de los dispositivos StorageGRID pueden configurarse en modo Fixed o Aggregate para las conexiones a la Grid Network y Client Network.

Los puertos de red de administración de 1 GbE pueden configurarse en modo independiente o en modo activo-backup para las conexiones a la red de administración.

Consulta la información sobre los modos de enlace de puertos de tu dispositivo:

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

Instalación y aprovisionamiento de red para StorageGRID

Debes comprender cómo se utilizan la Grid Network y las redes opcionales Admin y Client durante el despliegue de nodos y la configuración de la grid.

Primera puesta en marcha de un nodo

Cuando implementas un nodo por primera vez, debes conectarlo a la red Grid y asegurarte de que tenga acceso al nodo de administración principal. Si la red Grid está aislada, puedes configurar la red de administración en el nodo de administración principal para acceder a la configuración y la instalación desde fuera de la red Grid.

Una Grid Network con una gateway configurada se convierte en la gateway predeterminada para un nodo durante la implementación. La gateway predeterminada permite que los grid nodes en subredes separadas se comuniquen con el primary Admin Node antes de que el grid haya sido configurado.

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

Registro automático de nodos en el nodo de administración principal

Una vez que los nodos están desplegados, se registran ellos mismos en el nodo de administración principal usando la Grid Network. Luego puedes usar el Grid Manager, el `configure-storagegrid.py` script de Python o la Installation API para configurar la grid y aprobar los nodos registrados. Durante la configuración de la grid, puedes configurar varias subredes de grid. Las rutas estáticas a estas subredes a través de la puerta de enlace de la Grid Network se crearán en cada nodo cuando completes la configuración de la grid.

Desactivar la red de administración o la red de clientes

Si deseas desactivar la red de administración o la red de clientes, puedes eliminar la configuración correspondiente durante el proceso de aprobación del nodo o puedes usar la herramienta Cambiar IP una vez finalizada la instalación (consulta "[Configurar direcciones IP](#)").

Directrices posteriores a la instalación para StorageGRID

Una vez completada la implementación y configuración de los nodos de la red, sigue estas directrices para la asignación de direcciones DHCP y los cambios en la configuración de la red.

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

Solo puedes configurar DHCP durante la fase de implementación. No puedes configurar DHCP durante la configuración.



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

- Debes seguir los procedimientos de «Cambiar IP» si deseas modificar las direcciones IP, las máscaras de subred y las puertas de enlace predeterminadas de un nodo de la red. Consulta "[Configurar direcciones IP](#)".
- Si realizas cambios en la configuración de red, incluidos los relacionados con el enrutamiento y la puerta de enlace, es posible que se pierda la conectividad de los clientes con el nodo de administración principal y con otros nodos de la grid. Dependiendo de los cambios de red aplicados, es posible que tengas que restablecer estas conexiones.

Referencia de puertos de red

Comunicaciones internas de los nodos de grid para StorageGRID

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



NetApp recomienda que habilites 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 del ICMP y de los puertos que figuran en la tabla, StorageGRID utiliza el Protocolo de Redundancia de Enrutadores Virtuales (VRRP). El VRRP es un protocolo de Internet que utiliza el número de protocolo IP 112. StorageGRID utiliza el VRRP únicamente en modo unidifusión. El VRRP solo es necesario si ["grupos de alta disponibilidad"](#) están configurados.

Directrices para nodos basados en Linux

Si las políticas de red empresarial restringen el acceso a alguno de estos puertos, puedes reasignar los puertos en el tiempo de puesta en marcha mediante un parámetro de configuración de puesta en marcha. Para obtener más información sobre la reasignación de puertos y los parámetros de configuración de puesta en marcha, consulta ["Instalar StorageGRID en nodos basados en software"](#).



La compatibilidad con la reasignación de puertos está en desuso y se eliminará en una futura versión. Para eliminar los puertos reasignados, consulta ["Eliminar las reasignaciones de puertos en los hosts bare metal"](#).

Directrices para nodos basados en VMware

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

Si las políticas de red empresarial restringen el acceso a alguno de estos puertos, puedes reasignar los puertos al implementar nodos usando el cliente web de VMware vSphere o mediante un ajuste en el archivo de configuración al automatizar la puesta en marcha de nodos de la red. Para más información sobre la reasignación de puertos y los parámetros de configuración de la puesta en marcha, consulta las instrucciones para ["Instalar StorageGRID en VMware"](#).



La compatibilidad con la reasignación de puertos está en desuso y se eliminará en una futura versión. Para eliminar los puertos reasignados, consulta ["Eliminar las reasignaciones de puertos en los hosts bare metal"](#).

Directrices para los nodos de appliance

Si las políticas de red empresarial restringen el acceso a alguno de estos puertos, puedes reasignar los puertos mediante el instalador de StorageGRID Appliance. Consulta ["Opcional: reasigna los puertos de red del dispositivo"](#).



La compatibilidad con la reasignación de puertos está en desuso y se eliminará en una futura versión. Para eliminar los puertos reasignados, consulta ["Eliminar las reasignaciones de puertos en los dispositivos StorageGRID"](#).

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	Dispositivos	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.
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 la instalación, expansión, 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 del tráfico interno.
1502	TCP	Todos los nodos	Nodos de almacenamiento	Tráfico interno relacionado con S3.
1504	TCP	Todos los nodos	Nodos de administración	Informes y configuración del servicio NMS del 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.

Puerto	TCP o UDP	De	A	Detalles
1507	TCP	Todos los nodos	Nodos de puerta de enlace	Tráfico interno del equilibrador de carga.
1508	TCP	Todos los nodos	Nodo de administración principal	Gestión de la configuración del tráfico interno.
1511	TCP	Todos los nodos	Nodos de almacenamiento	Tráfico interno de metadatos.
5353	UDP	Todos los nodos	Todos los nodos	Proporciona el servicio DNS multicast (mDNS) que se usa para los cambios de IP en toda la grid y para la detección del nodo de administración principal durante la instalación, expansión y recuperación. Nota: Configurar este puerto es opcional.
7001	TCP	Nodos de almacenamiento	Nodos de almacenamiento	Comunicación entre nodos del clúster de Cassandra mediante TLS.
7443	TCP	Todos los nodos	Nodo de administración principal	Tráfico interno para la instalación, la ampliación, la recuperación, otros procedimientos de mantenimiento y la notificación de errores.
8011	TCP	Todos los nodos	Nodo de administración principal	Tráfico interno para la instalación, expansión, recuperación y otros procedimientos de mantenimiento.
8443	TCP	Nodo de administración principal	Nodos de appliance	Tráfico interno relacionado con el procedimiento del modo de mantenimiento.
9042	TCP	Nodos de almacenamiento	Nodos de almacenamiento	Puerto del cliente de 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	Lo utilizan los dispositivos StorageGRID para reenviar paquetes AutoSupport desde SANtricity System Manager de E-Series al nodo de administración principal.

Puerto	TCP o UDP	De	A	Detalles
10342	TCP	Todos los nodos	Nodo de administración principal	Tráfico interno para la instalación, expansión, recuperación y otros procedimientos de mantenimiento.
18000	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento con ADC	Tráfico interno del servicio de cuentas.
18001	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento con ADC	Tráfico interno de la federación de identidades.
18002	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento	Tráfico interno de la API relacionado con los protocolos de objetos.
18003	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento con ADC	Tráfico interno de los servicios de plataforma.
18017	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento	Tráfico interno del servicio Data Mover para Cloud Storage Pools.
18019	TCP	Todos los nodos	Todos los nodos	Tráfico interno del servicio de fragmentos para codificación de borrado y replicación
18082	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento	Tráfico interno relacionado con S3.
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 las solicitudes de los clientes.

Puerto	TCP o UDP	De	A	Detalles
19000	TCP	Nodos de administración/almacenamiento	Nodos de almacenamiento con ADC	Tráfico interno del servicio Keystone.

Información relacionada

["Comunicaciones externas"](#)

Comunicaciones externas para StorageGRID

Los clientes deben comunicarse con los nodos de la red para cargar 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 alguno de los puertos, puedes realizar una de las siguientes acciones:

- Utiliza ["puntos de conexión del equilibrador de carga"](#) para permitir el acceso a los puertos definidos por el usuario.
- Reasigna los puertos al implementar nodos. Sin embargo, no debes reasignar los puntos finales del equilibrador de carga. Consulta la información sobre la reasignación de puertos para tu nodo de StorageGRID:



La compatibilidad con la reasignación de puertos está obsoleta y se eliminará en una futura versión. Para eliminar los puertos reasignados, consulta ["Eliminar las reasignaciones de puertos en los dispositivos StorageGRID"](#) o ["Eliminar las reasignaciones de puertos en los hosts bare metal"](#).

- ["Claves de reasignación de puertos para StorageGRID en Red Hat Enterprise Linux"](#)
- ["Reasignar puertos para StorageGRID en VMware"](#)
- ["Opcional: reasigna los puertos de red del dispositivo"](#)

Puertos utilizados para las comunicaciones externas

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



Esta lista no incluye los puertos que podrían estar configurados como ["puntos de conexión del equilibrador de carga"](#).

Puerto	TCP o UDP	Protocolo	De	A	Detalles
22	TCP	SSH	Portátil de servicio	Todos los nodos	Se requiere acceso SSH o a la consola para los procedimientos que incluyen pasos que se realizan en la consola. Opcionalmente, puedes usar el puerto 2022 en lugar del 22. Nota: Este puerto solo es necesario cuando necesitas habilitar el acceso SSH para ciertas operaciones de mantenimiento.
25	TCP	SMTP	Nodos de administración	Servidor de correo electrónico	Se utiliza para alertas y para AutoSupport por correo electrónico. Puedes cambiar la configuración predeterminada del puerto 25 desde la página Servidores de correo electrónico.
53	TCP/ UDP	DNS	Todos los nodos	Servidores DNS	Se usa para DNS.
67	UDP	DHCP	Todos los nodos	Servicio DHCP	Se utiliza de forma opcional para admitir la configuración de red basada en DHCP. El servicio dhclient no se ejecuta en grids configurados de forma estática.
68	UDP	DHCP	Servicio DHCP	Todos los nodos	Se utiliza de forma opcional para admitir la configuración de red basada en DHCP. El servicio dhclient no se ejecuta para grids que usan 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	Dispositivos	El puerto 80 redirige al puerto 8443 para el instalador de StorageGRID Appliance.
80	TCP	HTTP	Nodos de almacenamiento con ADC	AWS	Se utiliza para los mensajes de servicios de plataforma enviados a AWS u otros servicios externos que utilizan HTTP. Los inquilinos pueden modificar la configuración predeterminada del puerto HTTP de 80 al crear un endpoint.
80	TCP	HTTP	Nodos de almacenamiento	AWS	Las solicitudes de Cloud Storage Pools se envían a destinos de AWS que usan HTTP. Los administradores del grid pueden anular la configuración predeterminada del puerto HTTP de 80 al configurar un Cloud Storage Pool.

Puerto	TCP o UDP	Protocolo	De	A	Detalles
123	UDP	NTP	Nodos NTP primarios	NTP externo	Servicio de protocolo de tiempo de red (NTP). Los nodos seleccionados como fuentes NTP primarias también sincronizan la hora de sus relojes con las fuentes de tiempo NTP externas.
161	TCP/ UDP	SNMP	Cliente SNMP	Todos los nodos	Se utiliza para el sondeo SNMP. Todos los nodos proporcionan información básica; los nodos de administración también proporcionan datos de alertas. Por defecto, utiliza el puerto UDP 161 cuando se configura. Nota: Este puerto solo es necesario y solo se abre en el cortafuegos del nodo si se ha configurado SNMP. Si planeas usar SNMP, puedes configurar puertos alternativos. Nota: Para obtener información sobre el uso de SNMP con StorageGRID, ponte en contacto con tu representante de cuenta de NetApp.
162	TCP/ UDP	Notificaciones SNMP	Todos los nodos	Destinatarios de las notificaciones	Las notificaciones y traps SNMP salientes usan por defecto el puerto UDP 162. Nota: Este puerto solo es necesario si SNMP está habilitado y se han configurado los destinos de notificación. Si planeas usar SNMP, puedes configurar puertos alternativos. Nota: Para obtener información sobre el uso de SNMP con StorageGRID, ponte en contacto con tu representante de cuenta de NetApp.
389	TCP/ UDP	LDAP	Nodos de almacenamiento con ADC	Active Directory/LDAP	Se utiliza para conectarse a un servidor de Active Directory o LDAP para la federación de identidades.

Puerto	TCP o UDP	Protocolo	De	A	Detalles
443	TCP	HTTPS	Explorador	Nodos de administración	Lo utilizan los navegadores web y los clientes de la API de gestión para acceder al Grid Manager y al Tenant Manager. Nota: Si cierras los puertos 443 u 8443 de Grid Manager, cualquier usuario que esté conectado en ese momento a un puerto bloqueado, incluido tú, perderá el acceso a Grid Manager a menos que su dirección IP se haya añadido a la lista de direcciones privilegiadas. Consulta "Configura los controles del cortafuegos" para configurar las direcciones IP privilegiadas.
443	TCP	HTTPS	Nodos de administración	Active Directory	Lo utilizan los nodos de administración que se conectan a Active Directory si está habilitado el inicio de sesión único (SSO).
443	TCP	HTTPS	Nodos de almacenamiento con ADC	AWS	Se utiliza para los mensajes de servicios de plataforma enviados a AWS u otros servicios externos que utilizan HTTPS. Los inquilinos pueden modificar la configuración predeterminada del puerto HTTP de 443 al crear un endpoint.
443	TCP	HTTPS	Nodos de almacenamiento	AWS	Las solicitudes de Cloud Storage Pools se envían a destinos de AWS que usan HTTPS. Los administradores de grid pueden sobrescribir la configuración predeterminada del puerto HTTPS de 443 al configurar un Cloud Storage Pool.
5353	UDP	mDNS	Todos los nodos	Todos los nodos	Proporciona el servicio DNS multicast (mDNS) que se usa para los cambios de IP en toda la grid y para la detección del nodo de administración principal durante la instalación, expansión y recuperación. Nota: Configurar este puerto es opcional.
5696	TCP	KMIP	Dispositivo	KMS	Tráfico externo del Protocolo de Interoperabilidad de Gestión de Claves (KMIP) desde los dispositivos configurados para el cifrado de nodos hacia el Key Management Server (KMS), a menos que se especifique un puerto diferente en la página de configuración del KMS del StorageGRID Appliance Installer.

Puerto	TCP o UDP	Protocolo	De	A	Detalles
8443	TCP	HTTPS	Explorador	Nodos de administración	Opcional. Lo utilizan los navegadores web y los clientes de la API de gestión para acceder al Grid Manager. Se puede usar para separar las comunicaciones entre Grid Manager y Tenant Manager. Nota: Si cierras los puertos 443 u 8443 de Grid Manager, cualquier usuario que esté conectado en ese momento a un puerto bloqueado, incluido tú, pierde el acceso a Grid Manager a menos que su dirección IP se haya añadido a la lista de direcciones privilegiadas. Consulta "Configura los controles del cortafuegos" para configurar las direcciones IP privilegiadas.
8443	TCP	HTTPS	Explorador	Dispositivos	Lo utilizan los navegadores web y los clientes de la API de gestión para acceder al instalador de StorageGRID Appliance. Nota: El puerto 443 redirige al puerto 8443 para el instalador de StorageGRID Appliance.
9022	TCP	SSH	Portátil de servicio	Dispositivos	Permite el acceso a los dispositivos StorageGRID en modo de preconfiguración para soporte y solución de problemas. No es necesario que este puerto esté accesible entre los nodos de la cuadrícula ni durante las operaciones normales.
9091	TCP	HTTPS	Servicio externo de Grafana	Nodos de administración	Lo utilizan los servicios externos de Grafana para acceder de forma segura al servicio Prometheus de StorageGRID. Nota: Este puerto solo es necesario si se ha habilitado el acceso a Prometheus mediante certificado.
9092	TCP	Kafka	Nodos de almacenamiento con ADC	Clúster de Kafka	Se utiliza para los mensajes de servicios de plataforma enviados a un clúster de Kafka. Los inquilinos pueden modificar la configuración predeterminada del puerto de Kafka de 9092 al crear un endpoint.
9443	TCP	HTTPS	Explorador	Nodos de administración	Opcional. Lo utilizan los navegadores web y los clientes de la API de gestión para acceder al Tenant Manager. Se puede usar para separar las comunicaciones entre Grid Manager y Tenant Manager.

Puerto	TCP o UDP	Protocolo	De	A	Detalles
18082	TCP	HTTPS	Clientes de S3	Nodos de almacenamiento	El tráfico del cliente S3 va directamente a los nodos de almacenamiento (HTTPS).
18084	TCP	HTTP	Clientes de S3	Nodos de almacenamiento	Tráfico del cliente S3 directamente a los nodos de almacenamiento (HTTP).
23000-23999	TCP	HTTPS	Todos los nodos de la red de origen para la replicación entre redes	Nodos de administración y nodos de pasarela en la grid de destino para la replicación entre grids	Este rango de puertos está reservado para las conexiones de federación de grids. Ambos grids en una conexión usan el mismo puerto.

Guía de inicio rápido de StorageGRID

Sigue estos pasos a grandes rasgos para configurar y utilizar cualquier sistema StorageGRID.

1

Aprender, planificar y recopilar datos

Colabora con tu representante comercial de NetApp para conocer las opciones y planificar tu nuevo sistema StorageGRID. Plantéate este tipo de preguntas:

- ¿Cuántos datos de objetos esperas almacenar inicialmente y con el tiempo?
- ¿Cuántos sitios necesitas?
- ¿Cuántos nodos y de qué tipos necesitas en cada sitio?
- ¿Qué redes StorageGRID vas a utilizar?
- ¿Quién usará tu grid para almacenar objetos? ¿Qué aplicaciones usarán?
- ¿Tienes algún requisito especial en materia de seguridad o de almacenamiento?
- ¿Tienes que cumplir algún requisito legal o normativo?

Opcionalmente, trabaja con tu consultor de Servicios Profesionales de NetApp para acceder a la herramienta NetApp ConfigBuilder y completar un libro de configuración para usar al instalar y desplegar tu nuevo sistema. También puedes usar esta herramienta para ayudar a automatizar la configuración de cualquier dispositivo StorageGRID. Consulta ["Automatiza la instalación y configuración de los dispositivos"](#).

Revisa ["Conoce StorageGRID"](#) y la ["Directrices de redes"](#).

2

Instalar nodos

Un sistema StorageGRID está formado por nodos individuales, tanto de hardware como de software. Primero instalas el hardware de cada nodo de dispositivo y configuras cada host Linux o VMware.

Para completar la instalación, instalas el software StorageGRID en cada dispositivo o host de software y conectas los nodos en una grid. Durante este paso, proporcionas los nombres del sitio y de los nodos, los detalles de la subred y las direcciones IP de tus servidores NTP y DNS.

Descubre cómo:

- ["Instala el hardware del dispositivo"](#)
- ["Instalar StorageGRID en nodos basados en software"](#)

3

Inicia sesión y revisa el estado del sistema

Cuando la instalación de Grid esté completa, puedes iniciar sesión en Grid Manager. Desde allí, puedes revisar el estado general de tu nuevo sistema, activar AutoSupport y los correos electrónicos de alerta, y configurar los nombres de dominio de los endpoints S3.

Descubre cómo:

- ["Inicia sesión en Grid Manager"](#)
- ["Supervisa el estado del sistema"](#)
- ["Configura AutoSupport"](#)
- ["Configura notificaciones por correo electrónico para las alertas"](#)
- ["Configura los nombres de dominio de los endpoints S3"](#)

4

Configurar y gestionar

Las tareas de configuración que necesitas realizar para un nuevo sistema StorageGRID dependen de cómo vayas a usar tu grid. Como mínimo, configuras el acceso al sistema; usas los asistentes de FabricPool y S3; y gestionas varios ajustes de almacenamiento y seguridad.

Descubre cómo:

- ["Controlar el acceso a StorageGRID"](#)
- ["Usa el asistente de configuración de S3"](#)
- ["Utiliza el asistente de configuración de FabricPool"](#)
- ["Gestiona la seguridad"](#)
- ["Fortalecimiento del sistema"](#)

5

Configura ILM

Puedes controlar la ubicación y la duración de cada objeto en tu sistema StorageGRID configurando una política de gestión del ciclo de vida de la información (ILM) que consta de una o varias reglas ILM. Las reglas ILM le indican a StorageGRID cómo crear y distribuir copias de los datos de los objetos y cómo gestionar esas

copias a lo largo del tiempo.

Descubre cómo: ["Gestiona objetos con ILM"](#)

6

Usa StorageGRID

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

Descubre cómo:

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

7

Supervisar y solucionar problemas

Una vez que tu sistema esté en funcionamiento, debes supervisar sus actividades de forma periódica y solucionar cualquier alerta. Quizás también quieras configurar un servidor syslog externo, usar la supervisión SNMP o recopilar datos adicionales.

Descubre cómo:

- ["Supervisar StorageGRID"](#)
- ["Soluciona problemas de StorageGRID"](#)

8

Ampliar, mantener y recuperar

Puedes añadir nodos o sitios para ampliar la capacidad o la funcionalidad de tu sistema. También puedes realizar varios procedimientos de mantenimiento para recuperarte de fallos o para mantener tu sistema StorageGRID actualizado y funcionando de manera eficiente.

Descubre cómo:

- ["Ampliar una cuadrícula"](#)
- ["Mantén tu grid"](#)
- ["Recuperar nodos"](#)

Instalar, actualizar y aplicar corrección urgente a StorageGRID

Instala nodos StorageGRID

Conoce el hardware de los dispositivos StorageGRID

Ve a "[Documentación de StorageGRID Appliance](#)" para aprender a instalar, configurar y mantener los dispositivos de almacenamiento y servicios de StorageGRID.

Instala nodos basados en software

Guía de inicio rápido para instalar StorageGRID en un nodo basado en software

Sigue estos pasos a grandes rasgos para instalar un nodo de Linux o VMware StorageGRID.



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita "[Herramienta de matriz de interoperabilidad \(IMT\) de NetApp](#)".

1

Preparación

- Conoce más sobre "[Arquitectura de StorageGRID y topología de red](#)".
- Infórmate sobre los detalles de "[Redes StorageGRID](#)".
- Reúne y prepara el "[Información y materiales necesarios](#)".
- (Solo VMware) Instala y configura "[VMware vSphere Hypervisor, vCenter y los hosts ESX](#)".
- Prepara el "[CPU y RAM](#)" necesario.
- Proporciona "[requisitos de almacenamiento y rendimiento](#)".
- (Solo para Linux) "[Prepara los servidores Linux](#)" que alojará tus nodos de StorageGRID.

2

Implementación

Implementa nodos de grid. Cuando implementas nodos de grid, se crean como parte del sistema StorageGRID y se conectan a una o más redes.

- (Solo Linux) Para implementar nodos de grid basados en software en los hosts que preparaste en el paso 1, usa la línea de comandos de Linux y "[archivos de configuración de los nodos](#)".
- (Solo VMware) Utiliza el cliente web de VMware vSphere, un archivo .vmdk y un conjunto de plantillas de archivos .ovf para "[implementa los nodos basados en software como máquinas virtuales \(VM\)](#)" en los servidores que preparaste en el paso 1.
- Para implementar nodos de dispositivos StorageGRID, sigue la "[Guía de inicio rápido para la instalación del hardware](#)".

Configuración

Cuando todos los nodos hayan sido desplegados, usa el Grid Manager para ["configura la grid y completa la instalación"](#).

Automatiza la instalación



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Linux

Para ahorrar tiempo y garantizar la coherencia, puedes automatizar la instalación del servicio de host de StorageGRID y la configuración de los nodos de grid.

- Utiliza un marco de orquestación estándar, como Ansible, Puppet o Chef, para automatizar:
 - Instalación de Linux
 - Configuración de redes y almacenamiento
 - Instalación del motor de contenedores y del servicio de host de StorageGRID
 - Implementación de nodos de grid virtual

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

- Después de implementar los nodos de la grid, ["automatizar la configuración del sistema StorageGRID"](#) usando el script de configuración de Python proporcionado en el archivo de instalación.
- ["Automatiza la instalación y configuración de los nodos de grid de appliance"](#)
- Si eres un desarrollador avanzado de implementaciones de StorageGRID, automatiza la instalación de los nodos de grid usando la ["API de REST de instalación"](#).

VMware

Para ahorrar tiempo y garantizar la coherencia, puedes automatizar la implementación y la configuración de los nodos de la red y la configuración del sistema StorageGRID.

- ["Automatiza la implementación de nodos de red usando VMware vSphere"](#).
- Después de implementar los nodos de la grid, ["automatizar la configuración del sistema StorageGRID"](#) usando el script de configuración de Python proporcionado en el archivo de instalación.
- ["Automatiza la instalación y configuración de los nodos de grid de appliance"](#)
- Si eres un desarrollador avanzado de implementaciones de StorageGRID, automatiza la instalación de los nodos de grid usando la ["API de REST de instalación"](#).

Planifica y prepárate para la instalación en nodos basados en software

Información y materiales necesarios para StorageGRID

Antes de instalar StorageGRID, recopila y prepara la información y los materiales

necesarios.

Información obligatoria

Plan de red

A qué redes piensas conectar cada nodo de StorageGRID. StorageGRID admite varias redes para la separación del tráfico, la seguridad y la comodidad administrativa.

Consulta la guía de referencia de StorageGRID "[Directrices de redes](#)".

Información de red

Direcciones IP que se deben asignar a cada nodo de grid y las direcciones IP de los servidores DNS y NTP.

Servidores para nodos de grid

Identifica un conjunto de servidores (físicos, virtuales o ambos) que, en conjunto, proporcionen recursos suficientes para dar soporte al número y tipo de nodos de StorageGRID que tienes previsto implementar.



Si tu instalación de StorageGRID no va a utilizar nodos de almacenamiento StorageGRID appliance (hardware), debes usar almacenamiento RAID de hardware con caché de escritura respaldada por batería (BBWC). StorageGRID no admite el uso de redes de área de almacenamiento virtual (vSAN), RAID de software ni la ausencia de protección RAID.

Migración de nodos (solo Ubuntu y Debian, si es necesario)

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

Información relacionada

["Herramienta NetApp Interoperability Matrix Tool"](#)

Materiales necesarios

NetApp licencia de StorageGRID

Debes tener una licencia válida y firmada digitalmente de NetApp.



Se incluye una licencia no destinada a producción, que puedes usar para grids de pruebas y de prueba de concepto, en el archivo de instalación de StorageGRID.

Archivo de instalación de StorageGRID

["Descarga el archivo de instalación de StorageGRID y extrae los archivos"](#).

Portátil de servicio

El sistema StorageGRID se instala mediante un ordenador portátil de servicio.

El portátil de servicio debe tener:

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

Documentación de StorageGRID

- ["Notas de publicación"](#). Debes iniciar sesión con tu cuenta de NetApp o crear una cuenta para acceder a las notas de la versión.
- ["Instrucciones para la administración de StorageGRID"](#)

Descarga y descomprime los archivos de instalación de StorageGRID

Debes descargar el archivo de instalación de StorageGRID y extraer los archivos necesarios. Si lo deseas, puedes verificar manualmente los archivos del paquete de instalación.

Pasos

1. Ve a ["NetApp Página de descargas de StorageGRID"](#).
2. Selecciona el botón para descargar la última versión, o selecciona otra versión del menú desplegable y selecciona **Go**.
3. Inicia sesión con el nombre de usuario y la contraseña de tu cuenta de NetApp.
4. Si aparece un mensaje de advertencia o de MustRead, léelo y marca la casilla de verificación.



Debes aplicar las correcciones urgentes necesarias tras instalar la versión de StorageGRID. Para obtener más información, consulta el ["procedimiento de corrección urgente en las instrucciones de recuperación y mantenimiento"](#)

5. Lee el Acuerdo de licencia de usuario final, marca la casilla de verificación y luego selecciona **Aceptar y continuar**.
6. En la columna **Instalar StorageGRID**, selecciona el archivo de instalación .tgz o .zip correspondiente a tu tipo de nodo basado en software: RHEL, Ubuntu o Debian, o VMware.



Utiliza el archivo .zip si el portátil de servicio está ejecutando Windows.

7. Guarda el archivo de instalación.
8. La verificación de la firma del código es manual en un nodo Linux. Opcionalmente, si necesitas verificar el archivo de instalación:
 - a. Descarga el paquete de verificación de la firma del código de StorageGRID. El nombre del archivo de este paquete usa el formato `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz`, donde `<version-number>` es la versión del software StorageGRID.
 - b. Sigue los pasos para ["verificar manualmente los archivos de instalación"](#).
9. Extrae los archivos del archivo de instalación.
10. Elige los archivos que necesites.

Los archivos que necesites dependen de la topología de grid que tengas prevista y de cómo vayas a implementar tu sistema StorageGRID.



Las rutas que figuran en la tabla son relativas al directorio de nivel superior instalado por el archivo de instalación extraído.

RHEL

Ruta y nombre del archivo	Descripción
	Un archivo de texto que describe todos los archivos que contiene el archivo de descarga de StorageGRID.
	Una licencia gratuita que no da derecho a ningún tipo de asistencia técnica para el producto.
	Paquete RPM para instalar las imágenes de los nodos de StorageGRID en tus hosts RHEL.
	Paquete RPM para instalar el servicio de host de StorageGRID en tus hosts RHEL.
Herramienta de creación de scripts de implementación	Descripción
	Un script de Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Un script en Python que se utiliza para automatizar la configuración de los appliances StorageGRID.
	Un archivo de configuración de ejemplo para usar con el script <code>configure-storagegrid.py</code> .
	Un script de Python de ejemplo que puedes usar para iniciar sesión en la Grid Management API cuando el inicio de sesión único está habilitado. También puedes usar este script para la integración con Ping Federate.
	Un archivo de configuración en blanco para usar con el script <code>configure-storagegrid.py</code> .
	Ejemplo de rol y playbook de Ansible para configurar hosts de RHEL para el despliegue de contenedores de StorageGRID. Puedes personalizar el rol o el playbook según sea necesario.
	Un script de ejemplo en Python que puedes utilizar para iniciar sesión en la API de gestión de la red cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.

Ruta y nombre del archivo	Descripción
	Un script auxiliar llamado por el script de Python compañero <code>storagegrid-ssoauth-azure.py</code> para realizar interacciones de inicio de sesión único con Azure.
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puedes utilizar estos esquemas para confirmar que cualquier código que hayas escrito para utilizar las API de gestión de StorageGRID será compatible con la nueva versión de StorageGRID si no tienes un entorno de StorageGRID que no sea de producción para pruebas de compatibilidad con la actualización.

Ubuntu o Debian

Ruta y nombre del archivo	Descripción
	Un archivo de texto que describe todos los archivos que contiene el archivo de descarga de StorageGRID.
	Un archivo de licencia de NetApp que no es de producción y que puedes utilizar para pruebas e implementaciones de prueba de concepto.
	Paquete DEB para instalar las imágenes de los nodos de StorageGRID en hosts Ubuntu o Debian.
	Suma de comprobación MD5 del archivo <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .
	Paquete DEB para instalar el servicio de host de StorageGRID en hosts con Ubuntu o Debian.
Herramienta de creación de scripts de implementación	Descripción
	Un script de Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Un script en Python que se utiliza para automatizar la configuración de los appliances StorageGRID.

Ruta y nombre del archivo	Descripción
	Un script de Python de ejemplo que puedes usar para iniciar sesión en la Grid Management API cuando el inicio de sesión único está habilitado. También puedes usar este script para la integración con Ping Federate.
	Un archivo de configuración de ejemplo para usar con el script <code>configure-storagegrid.py</code> .
	Un archivo de configuración en blanco para usar con el script <code>configure-storagegrid.py</code> .
	Ejemplo de rol y playbook de Ansible para configurar hosts de Ubuntu o Debian para el despliegue de contenedores de StorageGRID. Puedes personalizar el rol o el playbook según sea necesario.
	Un script de ejemplo en Python que puedes utilizar para iniciar sesión en la API de gestión de la red cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script auxiliar llamado por el script de Python compañero <code>storagegrid-ssoauth-azure.py</code> para realizar interacciones de inicio de sesión único con Azure.
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puedes utilizar estos esquemas para confirmar que cualquier código que hayas escrito para utilizar las API de gestión de StorageGRID será compatible con la nueva versión de StorageGRID si no tienes un entorno de StorageGRID que no sea de producción para pruebas de compatibilidad con la actualización.

VMware

Ruta y nombre del archivo	Descripción
	Un archivo de texto que describe todos los archivos que contiene el archivo de descarga de StorageGRID.

Ruta y nombre del archivo	Descripción
	Una licencia gratuita que no da derecho a ningún tipo de asistencia técnica para el producto.
	El archivo de disco de la máquina virtual que se utiliza como plantilla para crear máquinas virtuales de nodos de grid.
	El archivo de plantilla de Open Virtualization Format (.ovf) y el archivo de manifiesto (.mf) para implementar el nodo de administración primario.
	El archivo de plantilla (.ovf) y el archivo de manifiesto (.mf) para implementar nodos de administración no principales.
	El archivo de plantilla (.ovf) y el archivo de manifiesto (.mf) para implementar Gateway Nodes.
	El archivo de plantilla (.ovf) y el archivo de manifiesto (.mf) para desplegar nodos de almacenamiento basados en máquinas virtuales.
Herramienta de creación de scripts de implementación	Descripción
	Un script de Bash que se usa para automatizar el despliegue de nodos de grid virtuales.
	Un archivo de configuración de ejemplo para usarlo con el script <code>deploy-vmware-ovftool.sh</code> .
	Un script de Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Un script en Python que se utiliza para automatizar la configuración de los appliances StorageGRID.
	Un script de ejemplo en Python que puedes utilizar para iniciar sesión en la API de gestión de la red cuando está habilitado el inicio de sesión único (SSO). También puedes utilizar este script para la integración con Ping Federate.

Ruta y nombre del archivo	Descripción
	Un archivo de configuración de ejemplo para usar con el script <code>configure-storagegrid.py</code> .
	Un archivo de configuración en blanco para usar con el script <code>configure-storagegrid.py</code> .
	Un script de ejemplo en Python que puedes utilizar para iniciar sesión en la API de gestión de la red cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script auxiliar llamado por el script de Python compañero <code>storagegrid-ssoauth-azure.py</code> para realizar interacciones de inicio de sesión único con Azure.
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puedes utilizar estos esquemas para confirmar que cualquier código que hayas escrito para utilizar las API de gestión de StorageGRID será compatible con la nueva versión de StorageGRID si no tienes un entorno de StorageGRID que no sea de producción para pruebas de compatibilidad con la actualización.

Verifica los archivos de instalación de StorageGRID

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

Antes de empezar

Tienes ["descargaste el paquete de verificación"](#) de la ["NetApp Página de descargas de StorageGRID"](#).

Pasos

1. Extrae los artefactos del paquete de verificación:

```
tar -xf StorageGRID_12.0.0_Code_Signature_Verification_Package.tar.gz
```

2. Asegúrate de que se hayan extraído estos artefactos:

- Certificado Leaf: `Leaf-Cert.pem`
- Cadena de certificados: `CA-Int-Cert.pem`
- Cadena de respuestas con 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. Utiliza la cadena para comprobar que el certificado de hoja es válido.

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

Resultado esperado: Leaf-Cert.pem: OK

4. Si el paso 2 falló porque el certificado de hoja ha caducado, usa el archivo `tsr` para 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. Crea un archivo de clave pública a partir del certificado leaf.

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

Resultado esperado: *ninguno*

6. Usa la clave pública para verificar el archivo sha256sum con sha256sum.sig.

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

Resultado esperado: Verified OK

7. Verifica el contenido del archivo sha256sum comparándolo con las sumas de comprobación recién creadas.

Ejemplo: `sha256sum -c sha256sum`

Resultado esperado: `<filename>: OK`

`<filename>` es el nombre del archivo comprimido que has descargado.

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

Requisitos de software para StorageGRID

Puedes utilizar una máquina virtual para alojar cualquier tipo de nodo de StorageGRID. Necesitas una máquina virtual para cada nodo de la red.

RHEL

Para instalar StorageGRID en RHEL, tienes que instalar algunos paquetes de software de terceros. Algunas distribuciones de Linux compatibles no incluyen estos paquetes por defecto. Las versiones de los paquetes de software con las que se han probado las instalaciones de StorageGRID incluyen las que aparecen en esta página.

Si seleccionas una distribución de Linux y una opción de instalación del entorno de ejecución de contenedores que requiera alguno de estos paquetes, y la distribución de Linux no los instala automáticamente, instala una de las versiones que se indican aquí si están disponibles a través de tu proveedor o del proveedor de soporte técnico de tu distribución de Linux. De lo contrario, utiliza las versiones predeterminadas de los paquetes disponibles de tu proveedor.

Todas las opciones de instalación requieren Podman o Docker. No instales ambos paquetes. Instala únicamente el paquete que requiera tu opción de instalación.



El soporte para Docker como motor de contenedores para implementaciones exclusivamente de software ha quedado obsoleto. Docker será sustituido por otro motor de contenedores en una futura versión.

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 futura versión.

- 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

Ubuntu y Debian

Para instalar StorageGRID en Ubuntu o Debian, debes instalar algunos paquetes de software de terceros. Algunas distribuciones de Linux compatibles no incluyen estos paquetes de forma predeterminada. Las versiones de los paquetes de software con las que se han probado las instalaciones de StorageGRID son las que figuran en esta página.

Si seleccionas una distribución de Linux y una opción de instalación del entorno de ejecución de contenedores que requiera alguno de estos paquetes, y la distribución de Linux no los instala automáticamente, instala una de las versiones que se indican aquí si están disponibles a través de tu proveedor o del proveedor de soporte técnico de tu distribución de Linux. De lo contrario, utiliza las versiones predeterminadas de los paquetes disponibles de tu proveedor.

Todas las opciones de instalación requieren Podman o Docker. No instales ambos paquetes. Instala únicamente el paquete que requiera tu opción de instalación.



El soporte para Docker como motor de contenedores para implementaciones exclusivamente de software ha quedado obsoleto. Docker será sustituido por otro motor de contenedores en una futura versión.

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 futura versión.

- 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

VMware

VMware vSphere Hypervisor

Debes instalar VMware vSphere Hypervisor en un servidor físico preparado. El hardware debe estar configurado correctamente (incluidas las versiones de firmware y los ajustes de la BIOS) antes de instalar el software VMware.

- Configura la red en el hipervisor según sea necesario para dar soporte a la red del sistema StorageGRID que estás instalando.

"Directrices de redes"

- Asegúrate de que el almacén de datos tenga capacidad suficiente para las máquinas virtuales y los discos virtuales necesarios para alojar los nodos de la grid.
- Si creas más de un almacén de datos, asigna un nombre a cada almacén para que puedas identificar fácilmente qué almacén de datos debes usar para cada nodo de grid cuando crees máquinas virtuales.

Requisitos de configuración del host ESX



Debes configurar correctamente el protocolo de sincronización de tiempo de red (NTP) en cada host ESX. Si la hora del host es incorrecta, podrían producirse efectos negativos, incluida la pérdida de datos.

Requisitos de configuración de VMware

Debes instalar y configurar VMware vSphere y vCenter antes de implementar los nodos de StorageGRID.

Para conocer las versiones compatibles del hipervisor VMware vSphere y del servidor VMware vCenter Server, consulta la página "[Herramienta NetApp Interoperability Matrix Tool](#)".

Para conocer los pasos necesarios para instalar estos productos de VMware, consulta la documentación de VMware.

Requisitos de CPU y RAM para StorageGRID

Antes de instalar el software StorageGRID, verifica y configura 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 ajeno a StorageGRID que se esté ejecutando en el sistema
 - Por lo general, al menos 24 GB por nodo y entre 2 y 16 GB menos que la memoria RAM total del sistema
 - Un mínimo de 64 GB para cada inquilino que tendrá aproximadamente 5,000 buckets

Los recursos de nodos basados en software que contienen únicamente metadatos deben coincidir con los recursos de los Storage Nodes existentes. Por ejemplo:

- Si el sitio de StorageGRID existente utiliza dispositivos SG6000 o SG6100, los nodos basados en software y dedicados exclusivamente a los metadatos 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 utiliza nodos de almacenamiento virtuales con 24 GB de RAM, 8 núcleos de CPU y 3 TB o 4 TB de almacenamiento de metadatos, los nodos basados en software dedicados exclusivamente a metadatos deberían utilizar recursos similares (24 GB de RAM, 8 núcleos de CPU y 4 TB de almacenamiento de metadatos (rangedb/0)).

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



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita "[Herramienta de matriz de interoperabilidad \(IMT\) de NetApp](#)".

Linux

Asegúrate de que el número de nodos de StorageGRID que tengas previsto ejecutar en cada host físico o virtual no supere el número de núcleos de CPU ni la memoria RAM física disponible. Si los hosts no están dedicados a ejecutar StorageGRID (no se recomienda), asegúrate de considerar los requisitos de recursos de las otras aplicaciones.

VMware

VMware admite un nodo por máquina virtual. Asegúrate de que el nodo de StorageGRID no supere la memoria RAM física disponible. Cada máquina virtual debe estar dedicada a ejecutar StorageGRID.



Supervisa periódicamente el uso de la CPU y la memoria para asegurarte de que estos recursos sigan siendo suficientes para tu carga de trabajo. Por ejemplo, duplicar la asignación de RAM y CPU para los nodos de almacenamiento virtual proporcionaría recursos similares a los que se proporcionan para los nodos de los dispositivos StorageGRID. Además, si la cantidad de metadatos por nodo supera los 500 GB, considera aumentar la RAM por nodo a 48 GB o más. Para obtener información sobre la gestión del almacenamiento de metadatos de objetos, el aumento del ajuste Espacio reservado para metadatos y la supervisión del uso de la CPU y la memoria, consulta las instrucciones para ["administrar"](#), ["monitorización"](#) y ["actualización"](#) StorageGRID.

Si hyperthreading está habilitado en los hosts físicos subyacentes, puedes proporcionar 8 núcleos virtuales (4 núcleos físicos) por nodo. Si hyperthreading no está habilitado en los hosts físicos subyacentes, debes proporcionar 8 núcleos físicos por nodo.

Si utilizas máquinas virtuales como hosts y tienes control sobre el tamaño y el número de máquinas virtuales, debes utilizar una única máquina virtual para cada nodo de StorageGRID y ajustar el tamaño de la máquina virtual en consecuencia.

(Solo RHEL, Debian y Ubuntu) Para implementaciones de producción, no deberías 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 debería estar en su propio dominio de fallos aislado. Puedes maximizar la durabilidad y la disponibilidad de los datos de objetos si te aseguras de que un único fallo de hardware solo pueda afectar a un único nodo de almacenamiento.

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

Requisitos de almacenamiento y rendimiento para StorageGRID

Debes conocer los requisitos de almacenamiento de los nodos de StorageGRID, así podrás disponer de espacio suficiente para la configuración inicial y la futura ampliación del almacenamiento.

Los requisitos de almacenamiento y rendimiento varían según tu implementación de nodos basados en software.



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Categorías de almacenamiento

Los nodos de StorageGRID requieren tres categorías lógicas de almacenamiento:

- **Pool de contenedores** — almacenamiento de alto rendimiento (10K SAS o SSD) para los contenedores de los nodos, que se asignará al controlador de almacenamiento del motor de contenedores cuando instales y configures el motor de contenedores en los hosts que van a soportar tus nodos de StorageGRID.
- **Datos del sistema** — almacenamiento de alto rendimiento (SAS de 10 000 rpm o SSD) para el almacenamiento persistente por nodo de los datos del sistema y los registros de transacciones, que los servicios del host de StorageGRID consumirán y asignarán a los nodos individuales.
- **Datos de objetos** — almacenamiento de alto rendimiento (SAS de 10K o SSD) y almacenamiento masivo de gran capacidad (NL-SAS/SATA) para el almacenamiento persistente de datos de objetos y metadatos de objetos.

Debes usar dispositivos de bloques respaldados por RAID para todas las categorías de almacenamiento. No se admiten discos sin redundancia, SSD ni JBOD. Puedes usar almacenamiento RAID local o compartido para cualquiera de las categorías de almacenamiento; sin embargo, si quieres usar la capacidad de migración de nodos en StorageGRID, debes almacenar tanto los datos del sistema como los datos de objetos en un almacenamiento compartido. Para obtener más información, consulta ["Requisitos para la migración de contenedores de nodo"](#).

Requisitos de rendimiento

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

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

Requisitos para los hosts que utilizan almacenamiento de NetApp ONTAP

Si el nodo de StorageGRID utiliza almacenamiento asignado desde un sistema NetApp ONTAP, comprueba que el volumen no tenga una política de nivelación de FabricPool habilitada. Desactivar la nivelación de FabricPool para los volúmenes usados con nodos de StorageGRID simplifica la solución de problemas y las operaciones de almacenamiento.



Nunca uses FabricPool para transferir ningún dato relacionado con StorageGRID de vuelta al propio StorageGRID. Transferir datos de StorageGRID de vuelta a StorageGRID aumenta la complejidad de la resolución de problemas y de las operaciones.

Número de hosts necesarios

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



En una implementación de producción, no ejecutes más de un Storage Node en un solo host físico o virtual. Usar un host dedicado para cada Storage Node proporciona un dominio de fallo aislado.

Otros tipos de nodos, como los Admin Nodes o los Gateway Nodes, pueden implementarse en los mismos hosts o en sus propios hosts dedicados, según sea necesario.



Las instantáneas de disco no se pueden usar para restaurar nodos de grid. En su lugar, consulta los procedimientos "[recuperación de nodo de grid](#)" para cada tipo de nodo.

Número de volúmenes de almacenamiento por cada nodo

La siguiente tabla muestra el número de volúmenes de almacenamiento (LUN) necesarios para cada host y el tamaño mínimo requerido para cada LUN, en función de los nodos que se vayan a implementar en dicho host.

El tamaño máximo de LUN probado es de 39 TB.



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

Finalidad de LUN	Categoría de almacenamiento	Número de LUNs	Tamaño mínimo/LUN
Grupo de almacenamiento del motor de contenedores	Pool de contenedores	1	Número total de nodos × 100 GB
/var/local volumen	Datos del sistema	1 por cada nodo en este host	100 GB
Nodo de almacenamiento	Datos del objeto	3 para cada nodo de almacenamiento en este host Nota: un nodo de almacenamiento basado en software de Linux puede tener de 1 a 48 volúmenes de almacenamiento. Un nodo de almacenamiento basado en software de VMware puede tener de 1 a 16 volúmenes de almacenamiento. Se recomiendan al menos 3 volúmenes de almacenamiento.	12 TB (4 TB por LUN, mínimo) Tamaño máximo de LUN probado: 39 TB. Consulta Requisitos de almacenamiento para los nodos de almacenamiento para más información.

Finalidad de LUN	Categoría de almacenamiento	Número de LUNs	Tamaño mínimo/LUN
Nodo de almacenamiento (solo metadatos)	Metadatos del objeto	1	4 TB/LUN, como mínimo Tamaño máximo de LUN probado: 39 TB. Consulta Requisitos de almacenamiento para los nodos de almacenamiento para más información. Nota: Solo se requiere un rangedb para los nodos de almacenamiento que contienen únicamente metadatos.
Registros de auditoría del nodo de administración	Datos del sistema	1 por cada Admin Node en este host	200 GB
Tablas de nodo de administración	Datos del sistema	1 por cada Admin Node en este host	200 GB



Dependiendo del nivel de auditoría configurado, del tamaño de las entradas de usuario como el nombre de clave de objeto de S3 y de cuántos datos del registro de auditoría necesites conservar, es posible que debas aumentar el tamaño de la LUN del registro de auditoría en cada Admin Node. Por lo general, un grid genera aproximadamente 1 KB de datos de auditoría por operación de S3, lo que significaría que una LUN de 200 GB admitiría 70 millones de operaciones al día u 800 operaciones por segundo durante dos o tres días.

Espacio de almacenamiento mínimo para un host

La siguiente tabla muestra el espacio de almacenamiento mínimo requerido para cada tipo de nodo. Puedes usar esta tabla para determinar la cantidad mínima de almacenamiento que debes proporcionar al host en cada categoría de almacenamiento, según qué nodos se vayan a implementar en ese host.



Las instantáneas de disco no se pueden usar para restaurar nodos de grid. En su lugar, consulta los procedimientos ["recuperación de nodo de grid"](#) para cada tipo de nodo.

Cada servidor de nodo necesita un LUN de 100 GB para el sistema operativo.

Tipo de nodo	Pool de contenedores	Datos del sistema	Datos del objeto
Nodo de almacenamiento	100 GB	100 GB	4.000 GB
Nodo de administración	100 GB	500 GB (3 LUNs)	<i>no aplicable</i>

Tipo de nodo	Pool de contenedores	Datos del sistema	Datos del objeto
Nodo de puerta de enlace	100 GB	100 GB	<i>no aplicable</i>

Ejemplo: cálculo de los requisitos de almacenamiento para un host o una máquina virtual

Supongamos que planeas implementar tres nodos en el mismo host o máquina virtual: un Storage Node, un Admin Node y un Gateway Node. Deberías proporcionar un mínimo de nueve volúmenes de almacenamiento al host. Vas a necesitar un mínimo de 300 GB de almacenamiento de nivel de rendimiento para los contenedores de los nodos, 700 GB de almacenamiento de nivel de rendimiento para los datos del sistema y los registros de transacciones, y 12 TB de almacenamiento de nivel de capacidad para los datos de objetos.

Ejemplo de host Linux

Tipo de nodo	Finalidad de LUN	Número de LUNs	Tamaño de LUN
Nodo de almacenamiento	Grupo de almacenamiento del motor de contenedores	1	300 GB (100 GB por nodo)
Nodo de almacenamiento	/var/local volumen	1	100 GB
Nodo de almacenamiento	Datos del objeto	3	12 TB (4 TB por LUN)
Nodo de administración	/var/local volumen	1	100 GB
Nodo de administración	Registros de auditoría del nodo de administración	1	200 GB
Nodo de administración	Tablas de nodo de administración	1	200 GB
Nodo de puerta de enlace	/var/local volumen	1	100 GB
Total		9	Pool de contenedores: 300 GB Datos del sistema: 700 GB Datos de objeto: 12,000 GB

Ejemplo de máquina virtual de VMware

Tipo de nodo	Finalidad de LUN	Número de LUNs	Tamaño de LUN
Nodo de almacenamiento	Volumen del sistema operativo	1	100 GB
Nodo de almacenamiento	Datos del objeto	3	12 TB (4 TB por LUN)
Nodo de administración	Volumen del sistema operativo	1	100 GB
Nodo de administración	Registros de auditoría del nodo de administración	1	200 GB

Tipo de nodo	Finalidad de LUN	Número de LUNs	Tamaño de LUN
Nodo de administración	Tablas de nodo de administración	1	200 GB
Nodo de puerta de enlace	Volumen del sistema operativo	1	100 GB
Total		8	Datos del sistema: 700 GB Datos de objeto: 12,000 GB

Requisitos específicos de almacenamiento para los nodos de almacenamiento

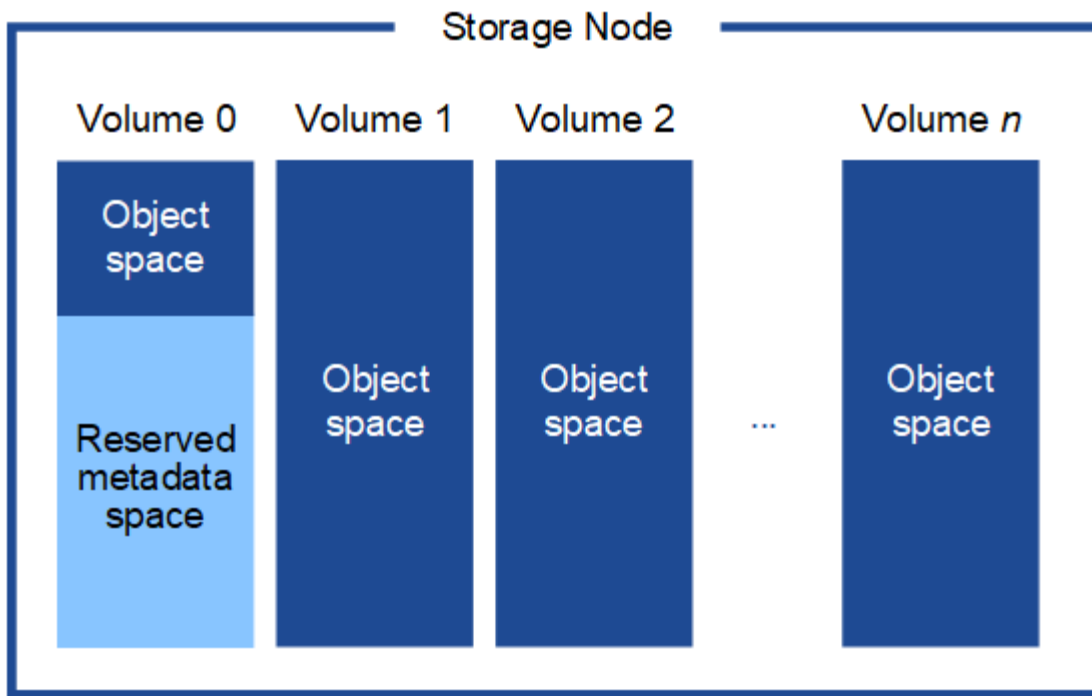
Linux y VMware tienen requisitos de almacenamiento diferentes para los nodos de almacenamiento:

- Un nodo de almacenamiento basado en software de Linux puede tener entre 1 y 48 volúmenes de almacenamiento
- Un nodo de almacenamiento basado en software de VMware puede tener de 1 a 16 volúmenes de almacenamiento
- Se recomienda disponer de tres o más volúmenes de almacenamiento.
- Cada volumen de almacenamiento debe ser de 4 TB o más.



Un nodo de almacenamiento de appliance 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. El espacio restante en el volumen de almacenamiento 0 y en cualquier otro volumen de almacenamiento del nodo de almacenamiento se utiliza exclusivamente para los datos de objetos.



Para garantizar la redundancia y proteger los metadatos de los objetos frente a posibles pérdidas, StorageGRID almacena tres copias de los metadatos de todos los objetos del sistema en cada sitio. Las tres copias de los metadatos de los objetos se distribuyen de manera uniforme entre todos los Storage Nodes de cada sitio.

Al instalar un grid con nodos de almacenamiento de solo metadatos, el grid también debe contener un número mínimo de nodos para el almacenamiento de objetos. Consulta ["Tipos de nodos de almacenamiento"](#) para obtener más información sobre los nodos de almacenamiento de solo metadatos.

- En una red de un solo sitio, se configuran al menos dos nodos de almacenamiento para objetos y metadatos.
- En una red con varios emplazamientos, se configura al menos un nodo de almacenamiento por emplazamiento para los objetos y metadatos.

Al asignar espacio al volumen 0 de un nuevo nodo de almacenamiento, debes asegurarte de que haya espacio suficiente para la parte que le corresponde a ese nodo de todos los metadatos de los objetos.

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



Si utilizas un único volumen de almacenamiento para un nodo de almacenamiento y le asignas 4 TB o menos al volumen, el nodo de almacenamiento podría entrar en estado de solo lectura al arrancar y almacenar únicamente los metadatos de los objetos.



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

- Los recursos de nodos basados en software que contienen únicamente metadatos deben coincidir con los recursos de los Storage Nodes existentes. Por ejemplo:
 - Si el sitio de StorageGRID existente utiliza dispositivos SG6000 o SG6100, los nodos basados en software y dedicados exclusivamente a los metadatos 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 utiliza nodos de almacenamiento virtuales con 24 GB de RAM, 8 núcleos de CPU y 3 TB o 4 TB de almacenamiento de metadatos, los nodos basados en software dedicados exclusivamente a metadatos deberían utilizar recursos similares (24 GB de RAM, 8 núcleos de CPU y 4 TB de almacenamiento de metadatos (rangedb/0)).

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

- Si estás instalando un nuevo sistema (StorageGRID 11.6 o superior) y cada nodo de almacenamiento tiene 128 GB o más de RAM, asigna 8 TB o más al volumen 0. Usar 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, utiliza la misma configuración para el volumen 0 siempre que sea posible. Si un sitio contiene nodos de almacenamiento de diferentes tamaños, el nodo de almacenamiento con el volumen 0 más pequeño determinará la capacidad de metadatos de ese sitio.

Para más información, visita ["Gestiona el almacenamiento de metadatos de objetos"](#).

Requisitos de migración de contenedores de nodo StorageGRID para Linux

La función de migración de nodos te permite trasladar manualmente un nodo de un host a otro. Normalmente, ambos hosts se encuentran en el mismo centro de datos físico.



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

La migración de nodos te permite realizar tareas de mantenimiento en el host físico sin interrumpir el funcionamiento del grid. Mueves todos los nodos de StorageGRID, uno por uno, a otro host antes de desconectar el host físico. Migrar nodos solo requiere un breve tiempo de inactividad para cada nodo y no debería afectar el funcionamiento ni la disponibilidad de los servicios del grid.

Si deseas utilizar la función de migración de nodos de StorageGRID, tu implementación debe cumplir requisitos adicionales:

- Nombres de interfaces de red uniformes en todos los hosts de un mismo centro de datos físico
- Almacenamiento compartido para los metadatos de StorageGRID y los volúmenes del repositorio de objetos, al que pueden acceder todos los hosts de un mismo centro de datos físico. Por ejemplo, podrías usar matrices de almacenamiento E-Series de NetApp.

Si utilizas hosts virtuales y la capa de hipervisor subyacente admite la migración de máquinas virtuales, quizá te interese utilizar esta funcionalidad en lugar de la función de migración de nodos de StorageGRID. En este caso, puedes ignorar estos requisitos adicionales.

Antes de realizar una migración o tareas de mantenimiento del hipervisor, apaga los nodos de forma controlada. Consulta las instrucciones para ["apagar un nodo de la red"](#).

La migración en vivo de VMware no es compatible

Al realizar una instalación bare-metal en máquinas virtuales de VMware, la migración en vivo de OpenStack y la migración en vivo de VMware vMotion provocan que la hora del reloj de la máquina virtual salte y no son compatibles con nodos de grid de ningún tipo. Aunque es poco frecuente, una hora incorrecta en el reloj puede provocar la pérdida de datos o de actualizaciones de configuración.

Se admite la migración en frío. En la migración en frío, apagas los nodos de StorageGRID antes de migrarlos entre hosts. Consulta las instrucciones para ["apagar un nodo de la red"](#).

Nomenclatura coherente para las interfaces de red

Para trasladar un nodo de un host a otro, el servicio de host de StorageGRID necesita tener cierta seguridad de que la conectividad de red externa de la que dispone el nodo en su ubicación actual se puede replicar en la nueva ubicación. Esta seguridad se consigue mediante el uso de nombres de interfaz de red coherentes en los hosts.

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

eth0 → bond0.1001

eth1 → bond0.1002

eth2 → bond0.1003

El lado izquierdo de las flechas corresponde a las interfaces tradicionales tal y como se ven desde el interior de un contenedor de StorageGRID (es decir, las interfaces Grid, Admin y Client Network, respectivamente). El lado derecho de las flechas corresponde a las interfaces reales del host que proporcionan estas redes, que son tres interfaces VLAN subordinadas al mismo enlace de interfaces físicas.

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

Hay muchas formas de conseguir una nomenclatura coherente para las interfaces de red en varios hosts; consulta ["Configura la red del host"](#) para ver algunos ejemplos.

Almacenamiento compartido

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

- Durante la operación de «exportación de nodo», se extrae una pequeña cantidad de datos de estado persistente del contenedor del 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 del nodo en HostA.
- Durante la operación de «importación de nodo», se instancia el contenedor del nodo en HostB que utiliza las mismas asignaciones de interfaz de red y 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 funcionamiento, 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 la migración se permita y funcione. Además, deben haberse asignado al nodo utilizando nombres que garanticen que hacen referencia a los mismos LUN en HostA y HostB.

El siguiente ejemplo muestra una solución para la asignación de dispositivos de bloques en un nodo de almacenamiento de StorageGRID, donde se utiliza la multivía de DM en los hosts y se ha usado el campo `alias` en `/etc/multipath.conf` para proporcionar nombres de dispositivos de bloques coherentes y fáciles de recordar 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
```

Prepara los hosts (Linux)

Cómo StorageGRID realiza cambios en la configuración de todo el host

En los sistemas bare metal, StorageGRID realiza algunos cambios en la configuración a nivel de host `sysctl`.



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Se han realizado 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 RAM
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
```

Instala StorageGRID en hosts grid de Linux

Debes instalar StorageGRID en todos los hosts de grid Linux. Para ver una lista de las versiones compatibles, usa la Herramienta de matriz de interoperabilidad de NetApp.

Antes de empezar

Asegúrate de que tu sistema operativo cumple los requisitos mínimos de versión del núcleo de StorageGRID, tal y como se indican a continuación. Utiliza el comando `uname -r` para conocer la versión del núcleo de tu sistema operativo, o consulta con tu proveedor de sistema operativo.



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

RHEL

Versión de RHEL	Versión mínima del kernel	Nombre del paquete del núcleo
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	kernel-4.18.0-553.el8_10.x86_64
9.0 (en desuso)	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

Ubuntu

Nota: La compatibilidad con las versiones 18.04 y 20.04 de Ubuntu ha quedado obsoleta y se eliminará en una futura versión.

Versión de Ubuntu	Versión mínima del kernel	Nombre del paquete del núcleo
22.04.1	5.15.0-47-generic	linux-image-5.15.0-47-generic/jammy-updates,jammy-security,ahora 5.15.0-47.51
24,04	6.8.0-31-generic	linux-image-6.8.0-31-generic/noble,ahora 6.8.0-31.31

Debian

Nota: La compatibilidad con la versión 11 de Debian ha quedado obsoleta y se eliminará en una futura versión.

Versión de Debian	Versión mínima del kernel	Nombre del paquete del núcleo
11 (obsoleto)	5.10.0-18-amd64	linux-image-5.10.0-18-amd64/stable,now 5.10.150-1
12	6.1.0-9-amd64	linux-image-6.1.0-9-amd64/stable,now 6.1.27-1

Pasos

1. Instala Linux en todos los servidores físicos o virtuales de la red según las instrucciones del distribuidor o tu procedimiento habitual.



No instales ningún entorno de escritorio gráfico.

- Si utilizas el instalador estándar de Linux para instalar RHEL, selecciona la configuración de software «nodo de cálculo», si está disponible, o el entorno básico «instalación mínima».
 - Al instalar Ubuntu, debes seleccionar **utilidades estándar del sistema**. Se recomienda seleccionar **OpenSSH server** para habilitar el acceso ssh a tus hosts de Ubuntu. Todas las demás opciones pueden dejarse desmarcadas.
2. Asegúrate de que todos los hosts tengan acceso a los repositorios de paquetes, incluido el canal Extras de RHEL.
 3. Si el swap está activado:
 - a. Ejecuta el siguiente comando: `$ sudo swapoff --all`
 - b. Elimina todas las entradas de intercambio de `/etc/fstab` para que la configuración se mantenga.



No desactivar por completo el espacio de intercambio puede reducir gravemente el rendimiento.

Conoce los perfiles de AppArmor para StorageGRID en Ubuntu y Debian

Si estás operando en un entorno Ubuntu que hayas desplegado tú mismo y utilizas el sistema de control de acceso obligatorio AppArmor, es posible que los perfiles de AppArmor asociados con los paquetes que instales en el sistema base se vean bloqueados por los paquetes correspondientes instalados con StorageGRID.

De forma predeterminada, se instalan perfiles de AppArmor para los paquetes que instalas en el sistema operativo base. Cuando ejecutas 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.

Tienes dos opciones para gestionar los perfiles de AppArmor:

- Deshabilita los perfiles individuales de los paquetes instalados en el sistema base que se solapan con los paquetes del contenedor del sistema StorageGRID. Cuando deshabilitas los perfiles individuales, aparece una entrada en los archivos de registro de StorageGRID que indica que AppArmor está habilitado.

Utiliza 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
```

- Desactiva por completo AppArmor. Para Ubuntu 9.10 o versiones posteriores, sigue las instrucciones de la comunidad en línea de Ubuntu: ["Deshabilita AppArmor"](#). Es posible que no se pueda desactivar por completo AppArmor en las versiones más recientes de Ubuntu.

Después de que desactives AppArmor, no aparecerá ninguna entrada que indique que AppArmor está activado en los archivos de registro de StorageGRID.

Configura la red de host de StorageGRID para implementaciones en Linux

Una vez completada la instalación de Linux en tus hosts, es posible que tengas que realizar alguna configuración adicional para preparar un conjunto de interfaces de red en cada host que sean adecuadas para asignarlas a los nodos de StorageGRID que implementarás más adelante.



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Antes de empezar

- Has revisado la ["Directrices de red de StorageGRID"](#).
- Has consultado la información sobre ["Requisitos para la migración de contenedores de nodo"](#).
- Si utilizas hosts virtuales, debes haber leído la [Consideraciones y recomendaciones para la clonación de direcciones MAC](#) antes de configurar la red del host.



Si utilizas máquinas virtuales como hosts, debes seleccionar VMXNET 3 como adaptador de red virtual. El adaptador de red VMware E1000 ha provocado problemas de conectividad con los contenedores de StorageGRID implementados en determinadas distribuciones de Linux.

Acerca de esta tarea

Los nodos de la red Grid deben poder acceder a la Grid Network y, opcionalmente, a las Admin y Client Networks. Proporcionas este acceso creando asignaciones que asocian la interfaz física del host a las interfaces virtuales de cada grid node. Al crear interfaces del host, usa nombres amigables para facilitar la implementación en todos los hosts y permitir la migración.

La misma interfaz puede compartirse entre el host y uno o más nodos. Por ejemplo, puedes usar la misma interfaz para el acceso al host y el acceso a la red de administración de los nodos, para facilitar el mantenimiento tanto del host como de los nodos. Aunque la misma interfaz puede compartirse entre el host y nodos individuales, todos deben tener direcciones IP diferentes. Las direcciones IP no pueden compartirse entre nodos ni entre el host y ningún nodo.

Puedes utilizar la misma interfaz de red del host para proporcionar la interfaz de red Grid a todos los nodos de StorageGRID del host; puedes utilizar una interfaz de red del host diferente para cada nodo; o puedes hacer algo intermedio. Sin embargo, normalmente no proporcionarías la misma interfaz de red del host como interfaz de red Grid y de red de administración para un solo nodo, ni como interfaz de red Grid para un nodo y como interfaz de red de cliente para otro.

Puedes realizar esta tarea de varias formas. Por ejemplo, si tus hosts son máquinas virtuales y vas a implementar uno o dos nodos de StorageGRID por cada host, puedes crear el número adecuado de interfaces de red en el hipervisor y utilizar una asignación 1 a 1. Si estás implementando varios nodos en hosts bare metal para uso en producción, puedes aprovechar la compatibilidad de la pila de red de Linux con VLAN y LACP para lograr tolerancia a fallos y compartir ancho de banda. Las siguientes secciones ofrecen enfoques detallados para ambos ejemplos. No necesitas usar ninguno de estos ejemplos; puedes emplear cualquier enfoque que se adapte a tus necesidades.



No utilices dispositivos «bond» o «bridge» directamente como interfaz de red del contenedor. Si lo haces, podrías impedir el arranque del nodo debido a un problema del núcleo relacionado con el uso de MACVLAN con dispositivos «bond» y «bridge» en el espacio de nombres del contenedor. En su lugar, utiliza un dispositivo que no sea «bond», como una VLAN o un par de Ethernet virtuales (veth). Especifica este dispositivo como la interfaz de red en el archivo de configuración del nodo.

Consideraciones y recomendaciones para la clonación de direcciones MAC

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

Habilitar la clonación de direcciones MAC

En determinados entornos, es posible mejorar la seguridad mediante la clonación de direcciones MAC, ya que permite utilizar una NIC virtual dedicada para la Admin Network, Grid Network y Client Network. Al hacer que el contenedor utilice la dirección MAC de la NIC dedicada del host, puedes evitar usar configuraciones de red en modo promiscuo.



La clonación de direcciones MAC está pensada para utilizarse con instalaciones de servidores virtuales y podría no funcionar correctamente con todas las configuraciones de dispositivos físicos.



Si un nodo no se inicia porque la interfaz en la que se va a clonar la dirección MAC está ocupada, es posible que tengas que establecer el enlace en "inactivo" antes de iniciar el nodo. Además, es posible que el entorno virtual impida la clonación de la dirección MAC en una interfaz de red mientras el enlace esté activo. Si un nodo no consigue establecer la dirección MAC ni iniciarse debido a que una interfaz está ocupada, establecer el enlace en "inactivo" antes de iniciar el nodo podría solucionar el problema.

La clonación de direcciones MAC está desactivada por defecto y debe configurarse mediante claves de configuración del nodo. Debes activarla al instalar StorageGRID.

Hay una clave para cada red:

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

Si se establece la clave en «true», el contenedor utilizará la dirección MAC de la NIC del host. Además, el host utilizará entonces la dirección MAC de la red del contenedor especificada. Por defecto, la dirección del contenedor es una dirección generada aleatoriamente, pero si has establecido una mediante la clave de configuración del nodo `_NETWORK_MAC`, se utilizará esa dirección en su lugar. El host y el contenedor siempre tendrán direcciones MAC diferentes.



Activar la clonación de direcciones MAC en un host virtual sin activar también el modo promiscuo en el hipervisor podría provocar que la red del host Linux que usa la interfaz del host deje de funcionar.

Casos de uso de la clonación de MAC

Hay dos casos de uso que hay que tener en cuenta en relación con la clonación de direcciones MAC:

- Clonación de MAC desactivada: cuando la `_CLONE_MAC` clave en el archivo de configuración del nodo no está definida o está establecida en "false", 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 la `_NETWORK_MAC` clave. Si se establece una dirección en la `_NETWORK_MAC` clave, el contenedor tendrá la dirección especificada en la `_NETWORK_MAC` clave. Esta configuración de claves requiere el uso de modo promiscuo.
- Clonación de MAC habilitada: cuando la `_CLONE_MAC` clave en el archivo de configuración del nodo se establece en "true", el contenedor usa la MAC de la NIC del host y el host usa una MAC generada por StorageGRID, a menos que se especifique una MAC en la `_NETWORK_MAC` clave. Si se establece una dirección en la `_NETWORK_MAC` clave, el host usa la dirección especificada en lugar de una generada. En esta configuración de claves, no deberías usar el modo promiscuo.



Si no deseas utilizar la clonación de direcciones MAC y prefieres permitir que todas las interfaces reciban y transmitan datos para direcciones MAC distintas de las asignadas por el hipervisor, asegúrate de que las propiedades de seguridad a nivel de conmutador virtual y de grupo de puertos estén configuradas en **Aceptar** para el modo promiscuo, los cambios de dirección MAC y las transmisiones falsificadas. Los valores configurados en el conmutador virtual pueden ser anulados por los valores a nivel de grupo de puertos, así que asegúrate de que la configuración sea la misma en ambos lugares.

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

Ejemplo de clonación de MAC

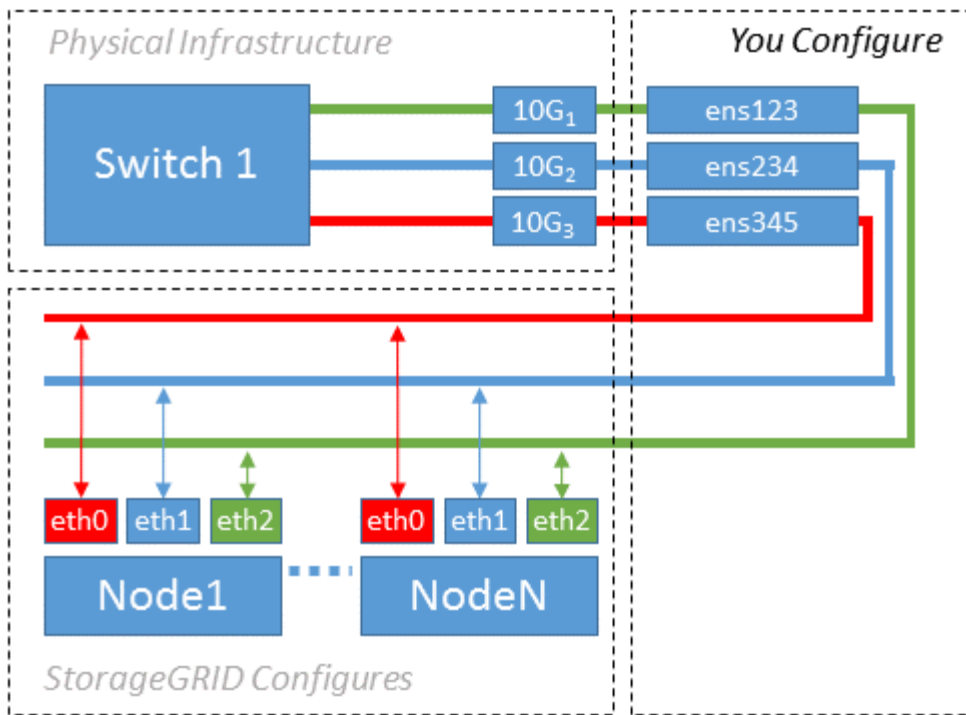
Ejemplo de clonación de MAC habilitada en un host con la dirección MAC 11:22:33:44:55:66 para la interfaz ens256 y las siguientes claves en el archivo de configuración del nodo:

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

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

Ejemplo 1: asignación 1 a 1 a tarjetas de red físicas o virtuales

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



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

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

Si el conmutador 1 es un conmutador físico, debes configurar los puertos conectados a las interfaces $10G_1$ a $10G_3$ en modo de acceso y colocarlos en las VLAN apropiadas.

Ejemplo 2: enlace LACP que transporta VLAN

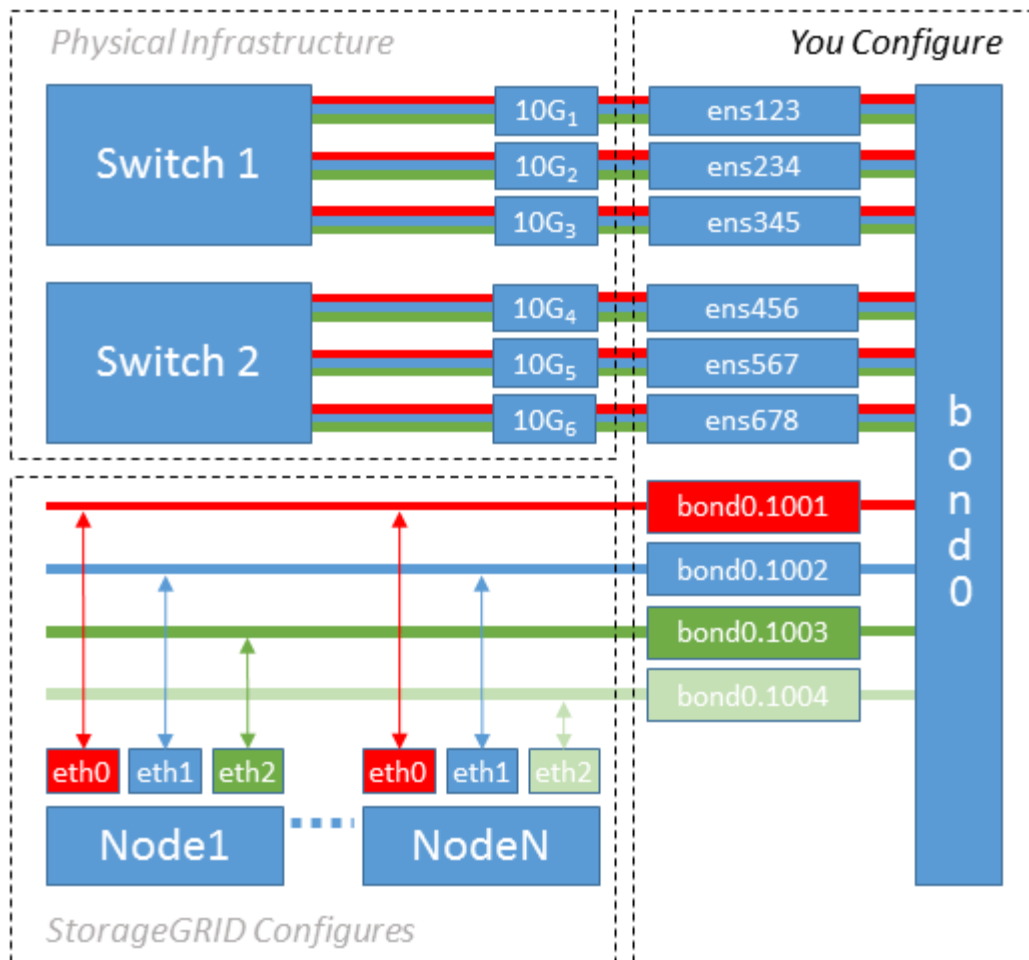
El ejemplo 2 da por hecho que estás familiarizado con la agrupación de interfaces de red y con la creación de interfaces VLAN en la distribución de Linux que utilizas.

Acerca de esta tarea

El ejemplo 2 describe un esquema genérico y flexible, basado en VLAN, que facilita el reparto de todo el ancho de banda de red disponible entre todos los nodos de un único host. Este ejemplo es especialmente aplicable a los hosts bare metal.

Para entender este ejemplo, supongamos que tienes tres subredes independientes para las redes Grid, Admin y Client en cada centro de datos. Las subredes se encuentran en VLAN independientes (1001, 1002 y 1003) y se presentan al host a través de un puerto troncal con enlace LACP (`bond0`). Configurarías tres interfaces de VLAN en el enlace: `bond0.1001`, `bond0.1002` y `bond0.1003`.

Si necesitas VLAN y subredes independientes para las redes de los nodos en un mismo host, puedes añadir interfaces de VLAN al bond y asignarlas al host (que aparece como `bond0.1004` en la ilustración).



Pasos

1. Agrupa todas las interfaces de red físicas que se vayan a utilizar para la conectividad de red de StorageGRID en un único enlace LACP.

Usa el mismo nombre para el bond en cada host, por ejemplo, bond0.

2. Crea interfaces VLAN que utilicen este enlace como su «dispositivo físico» asociado, usando la convención de nomenclatura estándar para interfaces VLAN `physdev-name.VLAN ID`.

Ten en cuenta que los pasos 1 y 2 requieren una configuración adecuada en los switches periféricos que terminan los otros extremos de los enlaces de red. Los puertos del switch periférico también se deben agregar en un canal de puertos LACP, configurar como trunk y permitir el paso de 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 de /etc/network/interfaces para Ubuntu y Debian"](#)
- ["Ejemplo de /etc/sysconfig/network-scripts para RHEL"](#)

Configura el almacenamiento de host de StorageGRID para implementaciones de Linux

Debes asignar volúmenes de almacenamiento en bloque a cada host Linux.

Antes de empezar

Has revisado los siguientes temas, que te proporcionan la información necesaria para llevar a cabo esta tarea:

- ["Requisitos de almacenamiento y rendimiento"](#)
- ["Requisitos para la migración de contenedores de nodo"](#)



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Acerca de esta tarea

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

- Número de volúmenes necesarios para cada host (en función del número y los tipos de nodos que se vayan a implementar en ese host)
- Categoría de almacenamiento de cada volumen (es decir, System Data o Object Data)
- Tamaño de cada volumen

Utilizarás esta información, así como el nombre permanente asignado por Linux a cada volumen físico cuando implementes nodos de StorageGRID en el host.



No necesitas particionar, formatear ni montar ninguno de estos volúmenes; solo tienes que asegurarte de que sean visibles para los hosts.



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

Evita usar archivos de dispositivo especiales "raw" (`/dev/sdb`, por ejemplo) a medida que creas tu lista de nombres de volúmenes. Estos archivos pueden cambiar entre reinicios del host, lo que afectará al correcto funcionamiento del sistema. Si estás utilizando LUN iSCSI y Device Mapper Multipathing, considera usar alias de multivía en el directorio `/dev/mapper`, especialmente si tu topología de SAN incluye rutas de red redundantes al almacenamiento compartido. Como alternativa, puedes usar los enlaces simbólicos creados por el sistema bajo `/dev/disk/by-path/` para tus nombres de dispositivos persistentes.

Por ejemplo:

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

Los resultados variarán en función de cada instalación.

Asigna nombres descriptivos a cada uno de estos volúmenes de almacenamiento de bloques para simplificar la instalación inicial de StorageGRID y los procedimientos de mantenimiento futuros. Si estás utilizando el controlador multivía de device mapper para el acceso redundante a los volúmenes de almacenamiento compartido, puedes usar el campo `alias` en tu archivo `/etc/multipath.conf`.

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
    }
    ...
}

```

Al utilizar el campo alias de esta forma, los alias aparecen como dispositivos de bloque en el directorio `/dev/mapper` del host, lo que te permite especificar un nombre descriptivo y fácil de validar siempre que una operación de configuración o mantenimiento requiera indicar un volumen de almacenamiento en bloque.

Si estás configurando un almacenamiento compartido para permitir la migración de nodos de StorageGRID y utilizas Device Mapper Multipathing, puedes crear e instalar un `/etc/multipath.conf` común en todos los hosts colocados. Solo asegúrate de usar un volumen de almacenamiento del motor de contenedores diferente en cada host. Usar alias e incluir el nombre de host de destino en el alias de cada LUN del volumen de almacenamiento del motor de contenedores hará que esto sea fácil de recordar y es lo recomendado.



El soporte para Docker como motor de contenedores para implementaciones exclusivamente de software ha quedado obsoleto. Docker será sustituido por otro motor de contenedores en una futura versión.

Información relacionada

- ["Configura el volumen de almacenamiento del motor de contenedores"](#)
- ["Requisitos de almacenamiento y rendimiento"](#)
- ["Requisitos para la migración de contenedores de nodo"](#)

Configura el volumen de almacenamiento del motor de contenedores para StorageGRID en Linux

Antes de instalar el motor de contenedores Docker o Podman, es posible que tengas que formatear el volumen de almacenamiento y montarlo.



El soporte para Docker como motor de contenedores para implementaciones exclusivamente de software ha quedado obsoleto. Docker será sustituido por otro motor de contenedores en una futura versión.



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Acerca de esta tarea

Puedes saltarte estos pasos si tienes pensado utilizar el volumen raíz como volumen de almacenamiento para Docker o Podman y dispones de espacio suficiente en la partición del host que contiene:

- Podman: `/var/lib/containers`
- Docker: `/var/lib/docker`

Pasos

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

RHEL

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

Ubuntu o Debian

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Monta el volumen de almacenamiento del motor de contenedores:

RHEL

- 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
```

Ubuntu o Debian

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

- Para Podman:

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

3. Agrega una entrada para el dispositivo de volumen de almacenamiento de contenedores en /etc/fstab.

- RHEL: dispositivo de volumen de almacenamiento de contenedores
- Ubuntu o Debian: docker-storage-volume-device

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

Instalar Docker

El sistema StorageGRID puede ejecutarse en Linux como un conjunto de contenedores.

- Antes de poder instalar StorageGRID para Ubuntu o Debian, debes instalar Docker.
- Si has decidido utilizar el motor de contenedores Docker, sigue estos pasos para instalar Docker. De lo contrario, [Instala Podman](#).



El soporte para Docker como motor de contenedores para implementaciones exclusivamente de software ha quedado obsoleto. Docker será sustituido por otro motor de contenedores en una futura versión.

Pasos

1. Instala Docker siguiendo las instrucciones correspondientes a tu distribución de Linux.



Si Docker no viene incluido en tu distribución de Linux, puedes descargarlo desde la página web de Docker.

2. Asegúrate de que Docker esté activado y en marcha ejecutando los dos comandos siguientes:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Comprueba que has instalado la versión prevista de Docker introduciendo lo siguiente:

```
sudo docker version
```

Las versiones del cliente y del servidor deben ser la 1.11.0 o posterior.

Instala Podman

El sistema StorageGRID funciona como un conjunto de contenedores. Si has optado por utilizar el motor de contenedores Podman, sigue estos pasos para instalar Podman. De lo contrario, [instalar Docker](#).

Pasos

1. Instala Podman y Podman-Docker siguiendo las instrucciones para tu distribución de Linux.



Además, debes instalar el paquete Podman-Docker cuando instales Podman.

2. Comprueba que has instalado la versión prevista de Podman y Podman-Docker introduciendo lo siguiente:

```
sudo docker version
```



El paquete Podman-Docker te permite utilizar los comandos de Docker.

Las versiones del cliente y del servidor deben ser la 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
```

Información relacionada

Instala los servicios de host de StorageGRID en Linux

Debes utilizar el paquete de StorageGRID correspondiente a tu tipo de sistema operativo para instalar los servicios de host de StorageGRID.



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

RHEL

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

Acerca de esta tarea

Estas instrucciones describen cómo instalar los servicios del host a partir de los paquetes RPM. Como alternativa, puedes utilizar los metadatos del repositorio DNF incluidos en el archivo de instalación para instalar los paquetes RPM de forma remota. Consulta las instrucciones del repositorio DNF correspondientes a tu sistema operativo Linux.

Pasos

1. Copia los paquetes RPM de StorageGRID en cada uno de tus hosts o ponlos a disposición en un almacenamiento compartido.

Por ejemplo, colócalos en el directorio `/tmp`, así podrás usar el comando de ejemplo en el siguiente paso.

2. Inicia sesión en cada host como root o usando una cuenta con permisos de sudo, y ejecuta 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 debes instalar el paquete Images y, a continuación, el paquete Service.



Si has colocado los paquetes en un directorio distinto de `/tmp`, modifica el comando para que refleje la ruta que hayas utilizado.

Ubuntu o Debian

El paquete DEB de StorageGRID sirve para instalar los servicios de host de StorageGRID en Ubuntu o Debian.

Acerca de esta tarea

Estas instrucciones describen cómo instalar los servicios del host a partir de los paquetes DEB. Como alternativa, puedes utilizar los metadatos del repositorio APT incluidos en el archivo de instalación para instalar los paquetes DEB de forma remota. Consulta las instrucciones del repositorio APT correspondientes a tu sistema operativo Linux.

Pasos

1. Copia los paquetes DEB de StorageGRID en cada uno de tus hosts o ponlos a disposición en un almacenamiento compartido.

Por ejemplo, colócalos en el directorio `/tmp`, así podrás usar el comando de ejemplo en el siguiente paso.

2. Inicia sesión en cada host como root o usando una cuenta con permisos de sudo, y ejecuta los siguientes comandos.

Debes instalar primero el paquete `images` y después el paquete `service`. Si pusiste los paquetes en un directorio diferente de `/tmp`, modifica el comando para reflejar la ruta que usaste.

```
sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
```

```
sudo dpkg --install /tmp/storagegrid-webscale-service-version-SHA.deb
```



Python 3 debe estar ya instalado antes de poder instalar los paquetes de StorageGRID. El comando `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` fallará hasta que lo hayas hecho.

Automatiza la instalación de nodos basados en software

Automatiza la instalación del servicio host de StorageGRID y la configuración de los nodos grid en Linux

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



Acerca de esta tarea

«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

La automatización de la implementación podría resultar útil en cualquiera de los siguientes casos:

- Ya utilizas un marco de orquestación estándar, como Ansible, Puppet o Chef, para implementar y configurar hosts físicos o virtuales.
- Tienes la intención de implementar varias instancias de StorageGRID.
- Estás implementando una instancia de StorageGRID grande y compleja.

El servicio de host StorageGRID se instala mediante un paquete y se gestiona a través de archivos de configuración. Puedes crear los archivos de configuración usando uno de estos métodos:

- ["Crea los archivos de configuración"](#) de forma interactiva durante una instalación manual.
- Prepara los archivos de configuración con antelación (o mediante código) para permitir la instalación automatizada utilizando marcos de orquestación estándar, como se describe en este artículo.

StorageGRID ofrece scripts opcionales en Python para automatizar la configuración de los dispositivos StorageGRID y de todo el sistema StorageGRID (la «red»). Puedes utilizar estos scripts directamente o consultarlos para aprender a usar el ["API de REST de instalación de StorageGRID"](#) en las herramientas de implementación y configuración de la grid que desarrolles tú mismo.

Automatiza la instalación y la configuración del servicio de host de StorageGRID

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

El servicio de host de StorageGRID se distribuye en un paquete DEB (Ubuntu o Debian) o RPM (RHEL) y se gestiona mediante archivos de configuración que puedes preparar con antelación (o mediante programación) para permitir la instalación automatizada. Si ya utilizas un marco de orquestación estándar para instalar y configurar tu entorno Linux, añadir StorageGRID a tus playbooks o recetas debería resultar sencillo.

Puedes automatizar todos los pasos para preparar los hosts e implementar los nodos de grid virtual.

Ejemplo de rol y playbook de Ansible

Se suministran un rol y un playbook de Ansible de ejemplo con el archivo de instalación en la carpeta /extras. El playbook de Ansible muestra cómo el rol `storagegrid` prepara los hosts e instala StorageGRID en los servidores de destino. Puedes personalizar el rol o el playbook según sea necesario.



El playbook de ejemplo no incluye los pasos necesarios para crear dispositivos de red antes de iniciar el servicio de host de StorageGRID. Añade estos pasos antes de finalizar y utilizar el playbook.

RHEL

En el caso de RHEL, las tareas de instalación en el ejemplo de rol proporcionado `storagegrid` utilizan el módulo `ansible.builtin.dnf` para realizar la instalación desde los archivos RPM locales o desde un repositorio Yum remoto. Si el módulo no está disponible o no es compatible, puede que tengas que editar las tareas de Ansible correspondientes en los siguientes archivos para usar el módulo `yum` o `ansible.builtin.yum`:

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

Ubuntu o Debian

Para Ubuntu o Debian, las tareas de instalación en el ejemplo de rol `storagegrid` proporcionado utilizan el módulo `ansible.builtin.apt` para realizar la instalación desde los archivos DEB locales o un repositorio apt remoto. Si el módulo no está disponible o no es compatible, es posible que tengas que editar las tareas de Ansible correspondientes en los siguientes archivos para utilizar el módulo `ansible.builtin.apt`:

- `roles/storagegrid/tasks/deb_install_from_repo.yml`
- `roles/storagegrid/tasks/deb_install_from_local.yml`

Automatiza la configuración de StorageGRID

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

Antes de empezar

- Ya conoces la ubicación de los siguientes archivos del archivo de instalación.

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

- Has creado un `configure-storagegrid.json` archivo de configuración. Para crear este archivo, puedes modificar el archivo de configuración de ejemplo (`configure-storagegrid.sample.json`) o el archivo de configuración en blanco (`configure-storagegrid.blank.json`).



Guarda la contraseña de administración y la frase de contraseña de aprovisionamiento de la sección de contraseñas del archivo de configuración `configure-storagegrid.json` modificado en un lugar seguro. Estas contraseñas son necesarias para los procedimientos de instalación, expansión y mantenimiento. También debes realizar una copia de seguridad del archivo de configuración `configure-storagegrid.json` modificado y guardarlo en un lugar seguro.

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 tu sistema StorageGRID.



También puedes configurar el sistema usando el Grid Manager o la Installation API.

Pasos

1. Inicia sesión en el equipo Linux que estás utilizando para ejecutar el script de Python.
2. Cambia al directorio donde extrajiste el archivo de instalación.

Por ejemplo:

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

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

3. Ejecuta el script de Python y utiliza el archivo de configuración que creaste.

Por ejemplo:

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

Resultado

Durante el proceso de configuración se genera un archivo de Recovery Package `.zip` y se descarga en el

directorio desde donde estás ejecutando el proceso de instalación y configuración. Debes realizar una copia de seguridad del archivo de Recovery Package para poder recuperar el sistema StorageGRID si uno o varios nodos de grid fallan. Por ejemplo, cópialo en una ubicación de red segura con copia de seguridad y en una ubicación de almacenamiento en la nube segura.



El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

Si especificaste que se generen contraseñas aleatorias, abre el `Passwords.txt` archivo y busca las contraseñas necesarias para acceder a tu 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.      #####  
#####
```

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

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

Automatiza el despliegue de nodos grid en StorageGRID con VMware vSphere

Puedes usar la herramienta VMware OVF Tool para automatizar el despliegue de los nodos de grid. También puedes automatizar la configuración de StorageGRID.

Automatiza la implementación de nodos de grid

Utiliza la herramienta VMware OVF para automatizar la implementación de los nodos de la grid.

Antes de empezar

- Tienes acceso a un sistema Linux/Unix con Bash 3.2 o una versión posterior.
- Tienes VMware vSphere con vCenter
- Tienes VMware OVF Tool instalada y correctamente configurada.
- Conoces el nombre de usuario y la contraseña para acceder a VMware vSphere mediante la OVF Tool
- Dispones de los permisos necesarios para implementar máquinas virtuales a partir de archivos OVF y encenderlas, así como de los permisos para crear volúmenes adicionales que se puedan conectar a las máquinas virtuales. Consulta la `ovftool` documentación para más detalles.
- Conoces la URL de la infraestructura virtual (VI) para la ubicación en vSphere donde quieres implementar las máquinas virtuales de StorageGRID. Esta URL normalmente será un vApp o un Resource Pool. Por ejemplo: `vi://vcenter.example.com/vi/sgws`



Puedes usar la utilidad de VMware `ovftool` para determinar este valor (consulta la documentación de `ovftool` para más detalles).



Si realizas el despliegue en una vApp, las máquinas virtuales no se iniciarán automáticamente la primera vez y tendrás que encenderlas manualmente.

- Has recopilado toda la información necesaria para el archivo de configuración de despliegue. Consulta ["Recopila información sobre tu entorno de implementación"](#) para obtener información.
- Tienes acceso a los siguientes archivos del archivo de instalación de VMware para StorageGRID:

Nombre del archivo	Descripción
NetApp-SG-version-SHA.vmdk	El archivo de disco de la máquina virtual que se utiliza como plantilla para crear máquinas virtuales de nodos de grid. Nota: Este archivo debe estar en la misma carpeta que los archivos <code>.ovf</code> y <code>.mf</code> .
vsphere-primary-admin.ovf vsphere-primary-admin.mf	El archivo de plantilla de Open Virtualization Format (<code>.ovf</code>) y el archivo de manifiesto (<code>.mf</code>) para implementar el nodo de administración primario.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	El archivo de plantilla (<code>.ovf</code>) y el archivo de manifiesto (<code>.mf</code>) para implementar nodos de administración no principales.
vsphere-gateway.ovf vsphere-gateway.mf	El archivo de plantilla (<code>.ovf</code>) y el archivo de manifiesto (<code>.mf</code>) para implementar Gateway Nodes.
vsphere-storage.ovf vsphere-storage.mf	El archivo de plantilla (<code>.ovf</code>) y el archivo de manifiesto (<code>.mf</code>) para desplegar nodos de almacenamiento basados en máquinas virtuales.
deploy-vsphere-ovftool.sh	El script de Bash que se utiliza para automatizar la implementación de nodos de grid virtuales.
deploy-vsphere-ovftool-sample.ini	El archivo de configuración de ejemplo para usar con el script <code>deploy-vsphere-ovftool.sh</code> .

Define el archivo de configuración para tu implementación

Especificas la información necesaria para implementar nodos de grid virtuales para StorageGRID en un archivo de configuración, que utiliza el script de Bash `deploy-vsphere-ovftool.sh`. Puedes modificar un archivo de configuración de ejemplo para no tener que crear el archivo desde cero.

Pasos

1. Crea una copia del archivo de configuración de ejemplo (`deploy-vsphere-ovftool.sample.ini`). Guarda el nuevo archivo como `deploy-vsphere-ovftool.ini` en el mismo directorio que `deploy-vsphere-ovftool.sh`.
2. Abre `deploy-vsphere-ovftool.ini`.

3. Introduce toda la información necesaria para implementar los nodos de grid virtual de VMware.

Consulta [Ajustes del archivo de configuración](#) para obtener información.

4. Cuando hayas introducido y comprobado toda la información necesaria, guarda y cierra el archivo.

Ajustes del archivo de configuración

El archivo de configuración `deploy-vmware-ovftool.ini` contiene los ajustes necesarios para implementar nodos de grid virtual.

El archivo de configuración enumera primero los parámetros globales y, a continuación, los parámetros específicos de cada nodo en secciones definidas por el nombre de nodo. Cuando se utiliza el archivo:

- Los *parámetros globales* se aplican a todos los nodos de la grid.
- Los *parámetros específicos de cada nodo* tienen prioridad sobre los parámetros globales.

Parámetros globales

Los parámetros globales se aplican a todos los nodos de la grid, a menos que se anulen mediante la configuración en secciones individuales. Coloca los parámetros que se aplican a varios nodos en la sección de parámetros globales y luego anula estos ajustes según sea necesario en las secciones para nodos individuales.

- **OVFTOOL_ARGUMENTS:** puedes especificar OVFTOOL_ARGUMENTS como configuración global o puedes aplicar argumentos de forma individual a nodos específicos. Por ejemplo:

```
OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick  
--datastore='datastore_name'
```

Puedes utilizar las opciones `--powerOffTarget` y `--overwrite` para apagar y sustituir máquinas virtuales existentes.



Deberías implementar los nodos en diferentes almacenes de datos y especificar OVFTOOL_ARGUMENTS para cada nodo, en lugar de hacerlo de forma global.

- **SOURCE:** la ruta al archivo de la plantilla de máquina virtual de StorageGRID (`.vmdk`) y a los archivos `.ovf` y `.mf` para los nodos de grid individuales. Por defecto, es el directorio actual.

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- **DESTINO:** la URL de la infraestructura virtual (vi) de VMware vSphere para la ubicación donde se implementará StorageGRID. Por ejemplo:

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- **GRID_NETWORK_CONFIG:** El método utilizado para obtener direcciones IP, ya sea STATIC o DHCP. El valor predeterminado es STATIC. Si todos o la mayoría de los nodos utilizan el mismo método para

obtener direcciones IP, puedes especificar ese método aquí. Luego puedes anular la configuración global especificando ajustes diferentes para uno o más nodos individuales. Por ejemplo:

```
GRID_NETWORK_CONFIG = STATIC
```

- **GRID_NETWORK_TARGET:** El nombre de una red de VMware ya existente que se usará para la Grid Network. Si todos o la mayoría de los nodos usan el mismo nombre de red, puedes especificarlo aquí. Luego puedes anular la configuración global especificando ajustes diferentes para uno o más nodos individuales. Por ejemplo:

```
GRID_NETWORK_TARGET = SG Admin Network
```

- **GRID_NETWORK_MASK:** la máscara de red para la Grid Network. Si todos o la mayoría de los nodos usan la misma máscara de red, puedes especificarla aquí. Después, puedes sobrescribir la configuración global especificando configuraciones diferentes para uno o varios 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 usan la misma puerta de enlace de red, puedes especificarla aquí. A continuación, puedes invalidar la configuración global especificando configuraciones diferentes para uno o varios nodos individuales. Por ejemplo:

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- **GRID_NETWORK_MTU:** opcional. La unidad máxima de transmisión (MTU) en la red Grid. Si se especifica, el valor debe estar entre 1280 y 9216. Por ejemplo:

```
GRID_NETWORK_MTU = 9000
```

Si lo omites, se usa 1400.

Si deseas utilizar tramas gigantes, configura el MTU con un valor adecuado para las tramas gigantes, como 9000. De lo contrario, mantén el valor predeterminado.



El valor de MTU de la red debe coincidir con el valor configurado en el puerto del switch 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 **Desajuste de MTU de la red Grid** se activa si existe una diferencia significativa en la configuración de MTU de la red Grid en los distintos nodos. No es necesario que los valores de MTU sean iguales para todos los tipos de red.

- **ADMIN_NETWORK_CONFIG:** el método utilizado para adquirir direcciones IP, ya sea DISABLED, STATIC o DHCP. El valor predeterminado es DISABLED. Si todos o la mayoría de los nodos usan el mismo método para adquirir direcciones IP, puedes especificar ese método aquí. Luego puedes anular la configuración global especificando configuraciones diferentes para uno o varios nodos individuales. Por ejemplo:

```
ADMIN_NETWORK_CONFIG = STATIC
```

- **ADMIN_NETWORK_TARGET:** el nombre de una red de VMware existente que se usará para la red de administración. Este ajuste es obligatorio a menos que la red de administración esté desactivada. 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. Después, puedes anular el ajuste global especificando diferentes ajustes para uno o varios nodos individuales. Por ejemplo:

```
ADMIN_NETWORK_TARGET = SG Admin Network
```

- **ADMIN_NETWORK_MASK:** la máscara de red para la red de administración. Este ajuste es necesario si estás usando direccionamiento IP estático. Si todos o la mayoría de los nodos usan la misma máscara de red, puedes especificarla aquí. Después, puedes anular el ajuste global especificando ajustes diferentes para uno o varios nodos individuales. Por ejemplo:

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- **ADMIN_NETWORK_GATEWAY:** la puerta de enlace de red para la Admin Network. Este ajuste es necesario si estás usando direccionamiento IP estático y especificas subredes externas en el ajuste ADMIN_NETWORK_ESL. (Es decir, no es necesario si ADMIN_NETWORK_ESL está vacío). Si todos o la mayoría de los nodos usan la misma puerta de enlace de red, puedes especificarla aquí. Después, puedes anular el ajuste global especificando ajustes diferentes para uno o varios nodos individuales. Por ejemplo:

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- **ADMIN_NETWORK_ESL:** la lista de subredes externas (rutas) para la red de administración (Admin Network), especificada como una lista separada por comas de destinos de ruta CIDR. Si todos o la mayoría de los nodos usan la misma lista de subredes externas, puedes especificarla aquí. Luego puedes invalidar la configuración global especificando configuraciones diferentes para uno o varios nodos individuales. Por ejemplo:

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- **ADMIN_NETWORK_MTU:** opcional. La unidad máxima de transmisión (MTU) en la red de administración. No lo especifiques si ADMIN_NETWORK_CONFIG = DHCP. Si se especifica, el valor debe estar entre 1280 y 9216. Si se omite, se usa 1400. Si quieres usar tramas jumbo, establece la MTU en un valor adecuado para tramas jumbo, como 9000. De lo contrario, mantén el valor predeterminado. Si todos o la mayoría de los nodos usan la misma MTU para la red de administración, puedes especificarla aquí. Después, puedes invalidar la configuración global especificando configuraciones diferentes para uno o

varios nodos individuales. Por ejemplo:

```
ADMIN_NETWORK_MTU = 8192
```

- **CLIENT_NETWORK_CONFIG:** el método utilizado para obtener direcciones IP, ya sea DISABLED, STATIC o DHCP. El valor predeterminado es DISABLED. Si todos o la mayoría de los nodos utilizan el mismo método para obtener direcciones IP, puedes especificar ese método aquí. Luego, puedes 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 de VMware existente que quieras usar para la red de clientes. Este ajuste es obligatorio a menos que la red de clientes esté desactivada. Si todos o la mayoría de los nodos usan el mismo nombre de red, puedes especificarlo aquí. A diferencia de la red de grid, no es necesario que todos los nodos estén conectados a la misma red de clientes. Después, puedes anular el ajuste global especificando diferentes ajustes para uno o varios nodos individuales. Por ejemplo:

```
CLIENT_NETWORK_TARGET = SG Client Network
```

- **CLIENT_NETWORK_MASK:** la máscara de red para la Client Network. Este ajuste es necesario si estás utilizando direccionamiento IP estático. Si todos o la mayoría de los nodos usan la misma máscara de red, puedes especificarla aquí. Después, puedes invalidar el ajuste global especificando ajustes diferentes para uno o varios nodos individuales. Por ejemplo:

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- **CLIENT_NETWORK_GATEWAY:** la puerta de enlace de red para la red de clientes. Este ajuste es necesario si utilizas direccionamiento IP estático. Si todos o la mayoría de los nodos usan la misma puerta de enlace de red, puedes especificarla aquí. A continuación, puedes invalidar el ajuste global especificando ajustes diferentes para uno o varios nodos individuales. Por ejemplo:

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- **CLIENT_NETWORK_MTU:** opcional. La unidad de transmisión máxima (MTU) en la red de clientes. No lo especifiques si CLIENT_NETWORK_CONFIG = DHCP. Si se especifica, el valor debe estar entre 1280 y 9216. Si se omite, se usa 1400. Si quieres usar tramas jumbo, establece la MTU en un valor adecuado para tramas jumbo, como 9000. De lo contrario, mantén el valor predeterminado. Si todos o la mayoría de los nodos usan la misma MTU para la red de clientes, puedes especificarla aquí. Después, puedes invalidar la configuración global especificando configuraciones diferentes para uno o varios nodos individuales. Por ejemplo:

```
CLIENT_NETWORK_MTU = 8192
```

- **PORT_REMAP:** Reasigna cualquier puerto utilizado por un nodo para comunicaciones internas entre nodos de la cuadrícula o para comunicaciones externas. La reasignación de puertos es necesaria si las políticas de red empresarial restringen uno o más puertos utilizados por StorageGRID. Para ver la lista de puertos utilizados por StorageGRID, consulta las comunicaciones internas entre nodos de la cuadrícula y las comunicaciones externas en ["Directrices de redes"](#).



No reasignes los puertos que planeas usar para configurar los endpoints del balanceador de carga.



Si solo se configura PORT_REMAP, el mapeo que especifiques se usará 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 client, y el protocolo es tcp o udp.

Por ejemplo:

```
PORT_REMAP = client/tcp/18082/443
```

Si la usas sola, esta configuración de ejemplo mapea simétricamente tanto las comunicaciones entrantes como las salientes para el nodo de grid del puerto 18082 al puerto 443. Si la usas en combinación con PORT_REMAP_INBOUND, esta configuración de ejemplo mapea las comunicaciones salientes del puerto 18082 al puerto 443.

También puedes reasignar varios puertos utilizando 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 especificas PORT_REMAP_INBOUND pero no especificas un valor para PORT_REMAP, las comunicaciones salientes para el puerto no cambian.



No reasignes los puertos que planeas usar para configurar los endpoints 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 client, y el protocolo es tcp o udp.

Por ejemplo:

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

En este ejemplo, el tráfico enviado al puerto 443 atraviesa un cortafuegos interno y se redirige al puerto 18082, donde el nodo de la red está a la espera de solicitudes S3.

También puedes reasignar varios puertos de entrada usando 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 temporal de instalación que se utilizará para acceder a la consola de la máquina virtual o a la API de instalación de StorageGRID, o usando SSH, antes de que el nodo se una a la grid.



Si todos o la mayoría de los nodos utilizan el mismo tipo de contraseña de instalación temporal, especifica el tipo en la sección de parámetros globales. Luego, opcionalmente usa una configuración diferente para un nodo individual. Por ejemplo, si seleccionas **Use Custom Password** globalmente, puedes usar **CUSTOM_TEMPORARY_PASSWORD=<password>** para establecer la contraseña de cada nodo.

TEMPORARY_PASSWORD_TYPE puede ser uno de los siguientes:

- **Utilizar el nombre de nodo**: El nombre de nodo se utiliza como contraseña temporal de instalación y permite acceder a la consola de la VM, a la API de instalación de StorageGRID y a SSH.
- **Desactivar contraseña**: no se utilizará ninguna contraseña de instalación temporal. Si necesitas acceder a la VM para depurar problemas de instalación, consulta ["Soluciona problemas de instalación"](#).
- **Utilizar contraseña personalizada**: El valor proporcionado con **CUSTOM_TEMPORARY_PASSWORD=<password>** se utiliza como contraseña temporal de instalación y permite acceder a la consola de la máquina virtual, a la API de instalación de StorageGRID y a SSH.



Si lo prefieres, puedes omitir el parámetro **TEMPORARY_PASSWORD_TYPE** y especificar únicamente **CUSTOM_TEMPORARY_PASSWORD=<password>**.

- **CUSTOM_TEMPORARY_PASSWORD=<password>** Opcional. La contraseña temporal que se utiliza durante la instalación al acceder a la consola de la VM, la API de instalación de StorageGRID y SSH. Se ignora si **TEMPORARY_PASSWORD_TYPE** está configurado en **Use node name** o **Disable password**.

Parámetros específicos de nodo

Cada nodo está en su propia sección del archivo de configuración. Cada nodo requiere los siguientes ajustes:

- El encabezado de la sección define el nombre de nodo que se mostrará en el Grid Manager. Puedes sobrescribir ese valor especificando el parámetro opcional **NODE_NAME** para el nodo.
- **NODE_TYPE**: VM_Admin_Node, VM_Storage_Node o VM_API_Gateway_Node
- **STORAGE_TYPE**: combinado, datos o metadatos. Este parámetro opcional para los nodos de almacenamiento toma por defecto el valor combinado (datos y metadatos) si no se especifica. Para obtener más información, consulta ["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. Solo es obligatorio 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 Client Network. Solo es obligatorio si el nodo está conectado a la Client Network y CLIENT_NETWORK_CONFIG para este nodo está configurado como STATIC.
- **ADMIN_IP:** La dirección IP del nodo de administración principal de la red Grid. Utiliza el valor que especifiques como GRID_NETWORK_IP para el nodo de administración principal. Si omites este parámetro, el nodo intenta descubrir la dirección IP del nodo de administración principal usando mDNS. Para más información, consulta ["Cómo detectan los nodos de la grid el nodo de administración principal"](#).



El parámetro ADMIN_IP se ignora para el nodo de administración principal.

- Cualquier parámetro que no se haya establecido de forma global. Por ejemplo, si un nodo está conectado a la Admin Network y no especificaste los parámetros de ADMIN_NETWORK de forma global, debes especificarlos para el nodo.

Nodo de administración principal

Se requieren los siguientes ajustes adicionales para el nodo de administración principal:

- **NODE_TYPE:** VM_Admin_Node
- **ADMIN_ROLE:** Principal

Esta entrada de ejemplo corresponde a un nodo de administración principal que se encuentra 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:

- **DISK:** De forma predeterminada, a los nodos de administración se les asignan dos discos duros adicionales de 200 GB para auditoría y bases de datos. Puedes ampliar estos valores mediante el parámetro DISK. Por ejemplo:

```
DISK = INSTANCES=2, CAPACITY=300
```



Para los nodos de administración, INSTANCES siempre debe ser igual a 2.

Nodo de almacenamiento

La siguiente configuración adicional es necesaria para los nodos de almacenamiento:

- **NODE_TYPE:** VM_Storage_Node

Esta entrada de ejemplo es para un nodo de almacenamiento que está en las redes Grid y de administración, pero no en la red de cliente. Este nodo usa el ajuste 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 corresponde a 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 usando el puerto 80 o 443. El archivo de configuración de ejemplo usa 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
```

Los siguientes ajustes adicionales son opcionales para los nodos de almacenamiento:

- **DISK:** por defecto, a los nodos de almacenamiento se les asignan tres discos de 4 TB para el uso de RangeDB. Puedes aumentar estos ajustes con el parámetro DISK. Por ejemplo:

```
DISK = INSTANCES=16, CAPACITY=4096
```

- **STORAGE_TYPE:** de forma predeterminada, todos los nuevos Storage Nodes están configurados para almacenar tanto datos de objetos como metadatos, lo que se conoce como un Storage Node *combinado*. Puedes cambiar el tipo de Storage Node para almacenar solo datos o metadatos con el parámetro STORAGE_TYPE. Por ejemplo:

```
STORAGE_TYPE = data
```

Nodo de puerta de enlace

Para los nodos de pasarela es necesario realizar la siguiente configuración adicional:

- **NODE_TYPE:** VM_API_Gateway

Esta entrada de ejemplo es para un nodo de puerta de enlace de ejemplo en las tres redes. En este ejemplo, no se especificaron parámetros de la red de clientes en la sección global del archivo de configuración, por lo que debes especificarlos 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

Se requieren las siguientes configuraciones adicionales para los nodos de administración que no son primarios:

- **NODE_TYPE:** VM_Admin_Node
- **ADMIN_ROLE:** No principal

Esta entrada de ejemplo corresponde a un nodo de administración no principal que no se encuentra 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 que no sean primarios:

- **DISK:** De forma predeterminada, a los nodos de administración se les asignan dos discos duros adicionales de 200 GB para auditoría y bases de datos. Puedes ampliar estos valores mediante el parámetro DISK. Por ejemplo:

```
DISK = INSTANCES=2, CAPACITY=300
```



Para los nodos de administración, INSTANCES siempre debe ser igual a 2.

Ejecuta el script de Bash

Puedes usar el `deploy-vmware-ovftool.sh` script de Bash y el archivo de configuración `deploy-vmware-ovftool.ini` que modificaste para automatizar el despliegue de nodos de StorageGRID en VMware vSphere.

Antes de empezar

Has creado un archivo de configuración `deploy-vmware-ovftool.ini` para tu entorno.

Puedes consultar la ayuda disponible para el script de Bash introduciendo los comandos de ayuda (`-h/ --help`). Por ejemplo:

```
./deploy-vmware-ovftool.sh -h
```

o

```
./deploy-vmware-ovftool.sh --help
```

Pasos

1. Inicia sesión en el equipo Linux que estás utilizando para ejecutar el script de Bash.
2. Cambia al directorio donde extrajiste el archivo de instalación.

Por ejemplo:

```
cd StorageGRID-Webscale-version/vsphere
```

3. Para implementar todos los nodos de la red, ejecuta el script de Bash con las opciones adecuadas para tu 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 por un error, soluciona el error y vuelve a ejecutar el script de 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

Automatiza la configuración de StorageGRID

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

Antes de empezar

- Ya conoces la ubicación de los siguientes archivos del archivo de instalación.

Nombre del archivo	Descripción
configure-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
configure-storagegrid.blank.json	Archivo de configuración en blanco para utilizarlo con el script

- Has creado un `configure-storagegrid.json` archivo de configuración. Para crear este archivo, puedes modificar el archivo de configuración de ejemplo (`configure-storagegrid.sample.json`) o el archivo de configuración en blanco (`configure-storagegrid.blank.json`).



Guarda la contraseña de administración y la frase de contraseña de aprovisionamiento de la sección de contraseñas del archivo de configuración `configure-storagegrid.json` modificado en un lugar seguro. Estas contraseñas son necesarias para los procedimientos de instalación, expansión y mantenimiento. También debes realizar una copia de seguridad del archivo de configuración `configure-storagegrid.json` modificado y guardarlo en un lugar seguro.

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 tu sistema StorageGRID.



También puedes configurar el sistema usando el Grid Manager o la Installation API.

Pasos

1. Inicia sesión en el equipo Linux que estás utilizando para ejecutar el script de Python.
2. Cambia al directorio donde extrajiste el archivo de instalación.

Por ejemplo:

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

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

3. Ejecuta el script de Python y utiliza el archivo de configuración que creaste.

Por ejemplo:

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

Resultado

Durante el proceso de configuración se genera un archivo de Recovery Package `.zip` y se descarga en el directorio desde donde estás ejecutando el proceso de instalación y configuración. Debes realizar una copia de seguridad del archivo de Recovery Package para poder recuperar el sistema StorageGRID si uno o varios nodos de grid fallan. Por ejemplo, cópialo en una ubicación de red segura con copia de seguridad y en una ubicación de almacenamiento en la nube segura.



El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

Si especificaste que se generen contraseñas aleatorias, abre el `Passwords.txt` archivo y busca las contraseñas necesarias para acceder a tu 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. #####  
#####
```

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

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

Información relacionada

- ["Accede al Grid Manager"](#)
- ["API de REST de instalación"](#)

Implementar nodos de grid virtual

Recopila información sobre tu entorno VMware para StorageGRID

Antes de implementar los nodos de grid, debes recopilar información sobre la configuración de tu red y tu entorno VMware.



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

Información sobre VMware

Debes 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 volúmenes de almacenamiento que planeas usar para los Storage Nodes.

Debes recopilar información sobre tu entorno VMware, incluyendo lo siguiente:

- El nombre de usuario y la contraseña de una cuenta de VMware vSphere que cuente con los permisos adecuados para completar la implementación.
- Información sobre la configuración del host, el datastore y la red de cada máquina virtual de nodo de StorageGRID.



VMware live vMotion hace que la hora del reloj de la máquina virtual salte y no es compatible con los nodos de grid de ningún tipo. Aunque es poco frecuente, los horarios incorrectos pueden provocar la pérdida de datos o de actualizaciones de configuración.

Información de la red Grid

Debes recopilar información sobre la red de VMware creada para la red Grid de StorageGRID (obligatorio), incluyendo:

- El nombre de la red.
- El método utilizado para asignar direcciones IP, ya sea estáticas o mediante DHCP.
 - Si utilizas direcciones IP estáticas, los datos de red necesarios para cada nodo de grid (dirección IP, puerta de enlace, máscara de red).
 - Si utilizas DHCP, la dirección IP del nodo de administración principal de la red Grid. Consulta ["Cómo detectan los nodos de la grid el nodo de administración principal"](#) para obtener más información.

Información de la red de administración

Para los nodos que se conectarán a la red de administración opcional de StorageGRID, debes recopilar información sobre la red de VMware creada para esta red, incluyendo:

- El nombre de la red.
- El método utilizado para asignar direcciones IP, ya sea estáticas o mediante DHCP.
 - Si utilizas direcciones IP estáticas, los datos de red necesarios para cada nodo de grid (dirección IP, puerta de enlace, máscara de red).
 - Si utilizas DHCP, la dirección IP del nodo de administración principal de la red Grid. Consulta ["Cómo detectan los nodos de la grid el nodo de administración principal"](#) para obtener más información.
- La lista de subredes externas (ESL) de la red de administración.

Información de la red del cliente

En el caso de los nodos que se conectarán a la red opcional StorageGRID Client Network, debes recopilar información sobre la red de VMware creada para esta red, incluyendo:

- El nombre de la red.
- El método utilizado para asignar direcciones IP, ya sea estáticas o mediante DHCP.
- Si utilizas direcciones IP estáticas, los datos de red necesarios para cada nodo de grid (dirección IP, puerta de enlace, máscara de red).

Información sobre interfaces adicionales

Si lo deseas, puedes añadir interfaces de tronco o de acceso a la máquina virtual en vCenter después de instalar el nodo. Por ejemplo, podrías querer añadir una interfaz de tronco a un Admin Node o Gateway Node, así puedes usar interfaces VLAN para segregar el tráfico que pertenece a diferentes aplicaciones o tenants. O podrías querer añadir una interfaz de acceso para usarla en un grupo de alta disponibilidad (HA).

Las interfaces que añadas se muestran en la página de interfaces VLAN y en la página de grupos de alta disponibilidad en Grid Manager.

- Si añades una interfaz trunk, configura una o varias interfaces VLAN para cada nueva interfaz principal. Consulta ["configurar interfaces VLAN"](#).
- Si añades una interfaz de acceso, debes añadirla directamente a los grupos de alta disponibilidad. Consulta ["configurar grupos de alta disponibilidad"](#).

Volúmenes de almacenamiento para nodos de almacenamiento virtuales

Debes recopilar la siguiente información para los nodos de almacenamiento basados en máquinas virtuales:

- El número y el tamaño de los volúmenes de almacenamiento (LUN de almacenamiento) que planeas añadir. Consulta "[Requisitos de almacenamiento y rendimiento](#)".

Información de configuración de grid

Debes recopilar información para configurar tu grid:

- Licencia de grid
- Direcciones IP de los servidores Network Time Protocol (NTP)
- Direcciones IP del servidor DNS

Crea archivos de configuración de nodos StorageGRID para implementaciones en Linux

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



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita "[Herramienta de matriz de interoperabilidad \(IMT\) de NetApp](#)".

Ubicación de los archivos de configuración de los nodos

Coloca el archivo de configuración de cada nodo de StorageGRID en el directorio `/etc/storagegrid/nodes` del host donde se ejecutará el nodo. Por ejemplo, si planeas ejecutar un Admin Node, un Gateway Node y un Storage Node en HostA, debes colocar tres archivos de configuración de nodo en `/etc/storagegrid/nodes` en HostA.

Puedes crear los archivos de configuración directamente en cada host utilizando un editor de texto, como vim o nano, o puedes crearlos en otro lugar y moverlos a cada host.

Nomenclatura de los archivos de configuración de nodo

Los nombres de los archivos de configuración son importantes. El formato es `node-name.conf`, donde `node-name` es un nombre que tú le asignas al nodo. Este nombre aparece en el StorageGRID Installer y se usa para operaciones de mantenimiento del nodo, como la migración del nodo.

Los nombres de los nodos deben cumplir las siguientes normas:

- Debe ser único
- Debe empezar por una letra
- Puede contener los caracteres de la A a la Z y de la a a la z
- Puede contener los números del 0 al 9
- Puede contener uno o más guiones (-)

- No debe tener más de 32 caracteres, sin contar la `.conf` extensión

Cualquier archivo en `/etc/storagegrid/nodes` que no siga estas convenciones de nomenclatura no será procesado por el servicio de alojamiento.

Si tienes prevista una topología con varios emplazamientos para tu grid, un esquema típico de nomenclatura de nodos podría ser:

`site-nodetype-nodenum.conf`

Por ejemplo, podrías utilizar `dc1-adm1.conf` para el primer nodo de administración en Data Center 1, y `dc2-sn3.conf` para el tercer nodo de almacenamiento en Data Center 2. Sin embargo, puedes usar cualquier esquema que quieras, siempre y cuando todos los nombres de los 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, sigue 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.
- Se ignoran los espacios en blanco al principio o al final.

En la siguiente tabla se definen los valores de todas las claves admitidas. Cada clave tiene una de las siguientes denominaciones:

- **Obligatorio:** obligatorio para todos los nodos o para los tipos de nodos especificados
- **Práctica recomendada:** opcional, aunque se recomienda
- **Opcional:** opcional para todos los nodos

Claves de la red de administración

ADMIN_IP

Valor	Denominación
Dirección IPv4 de la red Grid del nodo de administración que deseas utilizar para instalar el nodo basado en Linux. Para la recuperación, utiliza la dirección IP del nodo de administración principal si está disponible; de lo contrario, utiliza la dirección IP de un nodo de administración no principal. Si omites este parámetro, el nodo intenta descubrir un nodo de administración principal usando mDNS. "Cómo detectan los nodos de la grid el nodo de administración principal" Nota: Este valor se ignora y puede que esté prohibido en el nodo de administración principal.	Mejor práctica

ADMIN_NETWORK_CONFIG

Valor	Denominación
DHCP, ESTÁTICO o DESACTIVADO	Opcional

ADMIN_NETWORK_ESL

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

ADMIN_NETWORK_GATEWAY

Valor	Denominación
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 mediante DHCP. Ejemplos: 1.1.1.1 10.224.4.81	Obligatorio si se especifica ADMIN_NETWORK_ESL. Opcional en caso contrario.

ADMIN_NETWORK_IP

Valor	Denominación
Dirección IPv4 de este nodo en la red de administración. Esta clave solo es necesaria cuando ADMIN_NETWORK_CONFIG = STATIC; no la especifiques para otros valores. Ejemplos: 1.1.1.1 10.224.4.81	Es obligatorio cuando ADMIN_NETWORK_CONFIG = STATIC. Opcional de lo contrario.

ADMIN_NETWORK_MAC

Valor	Denominación
La dirección MAC de la interfaz de red Admin en el contenedor. Este campo es opcional. Si no se indica, 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

ADMIN_NETWORK_MASK

Valor	Denominación
Máscara de red IPv4 para este nodo, en la Admin Network. Especifica esta clave cuando ADMIN_NETWORK_CONFIG = STATIC; no la especifiques para otros valores. Ejemplos: 255.255.255.0 255.255.248.0	Es obligatorio si se especifica ADMIN_NETWORK_IP y ADMIN_NETWORK_CONFIG = STATIC. Opcional de lo contrario.

ADMIN_NETWORK_MTU

Valor	Denominación
La unidad máxima de transmisión (MTU) para este nodo en la Admin Network. No lo especifiques si ADMIN_NETWORK_CONFIG = DHCP. Si lo especificas, el valor debe estar entre 1280 y 9216. Si lo omites, se usa 1500. Si deseas utilizar tramas gigantes, configura el MTU con un valor adecuado para las tramas gigantes, como 9000. De lo contrario, mantén el valor predeterminado. IMPORTANTE: el valor de MTU de la red debe coincidir con el valor configurado en el puerto del switch al que está conectado el nodo. De lo contrario, podrían producirse problemas de rendimiento de la red o pérdida de paquetes. Ejemplos: 1500 8192	Opcional

ADMIN_NETWORK_TARGET

Valor	Denominación
Nombre del dispositivo host que vas a usar para el acceso a la red de administración por parte del nodo de StorageGRID. Solo se admiten nombres de interfaz de red. Normalmente, usas un nombre de interfaz diferente al que se especificó para GRID_NETWORK_TARGET o CLIENT_NETWORK_TARGET. Nota: No utilices dispositivos bond o bridge como destino de red. Configura una VLAN (u otra interfaz virtual) sobre el dispositivo bond, o utiliza un bridge y un par de Ethernet virtual (veth). Práctica recomendada: especifica un valor incluso si este nodo no va a tener inicialmente una dirección IP de la red de administración. Así podrás añadir una dirección IP de la red de administración más adelante, sin tener que volver a configurar el nodo en el host. Ejemplos: bond0.1002 ens256	Mejor práctica

ADMIN_NETWORK_TARGET_TYPE

Valor	Denominación
Interfaz (Este es el único valor admitido.)	Opcional

ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valor	Denominación
Verdadero o falso Establece la clave en «true» para que el contenedor de StorageGRID use la dirección MAC de la interfaz de red del host de destino en la Admin Network. Práctica recomendada: En redes donde se requiera el modo promiscuo, usa en su lugar la clave ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Para obtener más detalles sobre la clonación de MAC para Linux, consulta "Consideraciones y recomendaciones para la clonación de direcciones MAC".	Mejor práctica

ADMIN_ROLE

Valor	Denominación
Primario o no primario	Obligatorio cuando NODE_TYPE = VM_Admin_Node
Esta clave solo es necesaria cuando NODE_TYPE = VM_Admin_Node; no la especifique para otros tipos de nodo.	Opcional de lo contrario.

Claves de dispositivos de bloque

BLOCK_DEVICE_AUDIT_LOGS

Valor	Denominación
Ruta y nombre del archivo especial de dispositivo de bloques que utilizará este nodo para almacenamiento persistente de los registros de auditoría. Ejemplos: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> Greenfield deployment of StorageGRID with StorageGRID-mapped drives is supported. However, you cannot use StorageGRID-mapped drives if you are upgrading from StorageGRID 11.4 or earlier. To use StorageGRID-mapped drives, you must configure the StorageGRID appliance to use StorageGRID-mapped drives during the initial installation. You cannot change this configuration after installation. If you are upgrading from StorageGRID 11.4 or earlier, you must use the standard drive mapping. For more information about StorageGRID-mapped drives, see the StorageGRID-mapped drives page. StorageGRID-mapped drives StorageGRID-mapped drives are drives that are mapped to a specific StorageGRID node. This mapping is persistent and does not change even if the drive is moved to a different slot in the appliance or if the appliance is rebooted. Using StorageGRID-mapped drives provides the following benefits: • Simplified drive replacement: When you replace a failed drive, the new drive is automatically mapped to the same StorageGRID node as the failed drive. You do not need to manually configure the mapping. • Improved reliability: StorageGRID-mapped drives help prevent data loss by ensuring that data is always written to the correct drive, even if the drive is moved to a different slot. • Easier troubleshooting: If a drive fails, you can easily identify which StorageGRID node is affected by looking at the drive mapping. Standard drive mapping With standard drive mapping, drives are mapped to StorageGRID nodes based on their physical slot location in the appliance. If you move a drive to a different slot, the mapping changes, and the data on the drive might no longer be accessible to the StorageGRID node. If you are upgrading from StorageGRID 11.4 or earlier, you must continue to use standard drive mapping. You cannot migrate to StorageGRID-mapped drives. How to determine which drive mapping is in use You can determine which drive mapping is in use by looking at the Drive Mapping field on the Nodes page in the StorageGRID Grid Manager.	Es necesario para los nodos con <code>NODE_TYPE = VM_Admin_Node</code>. No lo especifique para otros tipos de nodo.

BLOCK_DEVICE_RANGEDB_nnn

- If the field displays **StorageGRID-mapped**, the appliance is using StorageGRID-mapped drives.
- If the field displays **Standard**, the appliance is using standard drive mapping.

You can also use the StorageGRID API to determine which drive mapping is in use. For more information, see the .

Configuring StorageGRID-mapped drives

You configure StorageGRID-mapped drives during the initial installation of the StorageGRID appliance.

For instructions on how to configure StorageGRID-mapped drives, see the installation guide for your appliance:

*
*
*

Replacing drives

The procedure for replacing a drive depends on whether the appliance is using StorageGRID-mapped drives or standard drive mapping.

- **StorageGRID-mapped drives:** When you replace a failed drive, the new drive is automatically mapped to the correct StorageGRID node. You do not need to perform any manual configuration steps. For instructions, see .
- **Standard drive mapping:** When you replace a failed drive, you must ensure that the new drive is installed in the same physical slot as the failed drive. If you install the drive in a different slot, the data on the drive might not be accessible. For instructions, see .

Moving drives

You should not move drives between slots in the appliance unless you are instructed to do so by NetApp Support.

- **StorageGRID-mapped drives:** If you move a StorageGRID-mapped drive to a different slot, the mapping remains intact, and the data on the drive remains accessible to the StorageGRID node. However, moving drives is still not recommended.
- **Standard drive mapping:** If you move a drive to a different slot, the mapping changes, and the data on the drive might no longer be accessible to the StorageGRID node. This can result in data loss. Do not move drives if the appliance is using standard drive mapping. Se admite la implementación desde cero de StorageGRID con unidades asignadas a StorageGRID. Sin embargo, no puedes usar unidades asignadas a StorageGRID si vas a realizar una actualización desde StorageGRID 11.4 o versiones anteriores.

Para usar unidades asignadas a StorageGRID, debes configurar el dispositivo de StorageGRID para que use unidades asignadas a StorageGRID durante la instalación inicial. No puedes cambiar esta

configuración después de la instalación.

Si vas a realizar una actualización desde StorageGRID 11.4 o versiones anteriores, debes usar la asignación de unidades estándar.

Para obtener más información sobre las unidades asignadas a StorageGRID, consulta la `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`.

Unidades asignadas a StorageGRID

Las unidades asignadas a StorageGRID son unidades que se asignan a un nodo de StorageGRID específico. Esta asignación es persistente y no cambia incluso si la unidad se mueve a una ranura diferente en el dispositivo o si este se reinicia.

El uso de unidades asignadas a StorageGRID proporciona las siguientes ventajas:

- **Sustitución de unidades simplificada:** cuando sustituyes una unidad que ha fallado, la nueva unidad se asigna automáticamente al mismo nodo de StorageGRID que la unidad que falló. No necesitas configurar la asignación de forma manual.
- **Fiabilidad mejorada:** las unidades asignadas a StorageGRID ayudan a evitar la pérdida de datos al garantizar que los datos siempre se escriban en la unidad correcta, incluso si la unidad se mueve a una ranura diferente.
- **Resolución de problemas más sencilla:** si una unidad falla, puedes identificar fácilmente qué nodo de StorageGRID se ve afectado al observar la asignación de unidades.

Asignación de unidades estándar

Con la asignación de unidades estándar, las unidades se asignan a los nodos de StorageGRID según su ubicación física en la ranura del dispositivo. Si mueves una unidad a una ranura diferente, la asignación cambia y es posible que el nodo de StorageGRID ya no pueda acceder a los datos de la unidad.

Si vas a realizar una actualización desde StorageGRID 11.4 o versiones anteriores, debes seguir usando la asignación de unidades estándar. No puedes migrar a unidades asignadas a StorageGRID.

Cómo determinar qué asignación de unidades se está utilizando

Puedes determinar qué asignación de unidades se está utilizando observando el campo **Asignación de unidades** en la página **Nodos** en el Gestor de grid de StorageGRID.

- Si el campo muestra **Asignada a StorageGRID**, el dispositivo está utilizando unidades asignadas a StorageGRID.
- Si el campo muestra **Estándar**, el dispositivo está utilizando la asignación de unidades estándar.

Valor	Denominación
Ruta y nombre del archivo especial de dispositivo de bloques que este nodo usará para el almacenamiento persistente de objetos. Esta clave solo es necesaria para nodos con <code>NODE_TYPE = VM_Storage_Node</code>; no la especifiques para otros tipos de nodo. Solo se requiere <code>BLOCK_DEVICE_RANGEDB_000</code>; los demás son opcionales. El dispositivo de bloques especificado para <code>BLOCK_DEVICE_RANGEDB_000</code> debe tener al menos 4 TB; los otros pueden ser más pequeños. No dejes huecos. Si especificas <code>BLOCK_DEVICE_RANGEDB_005</code>, también debes especificar <code>BLOCK_DEVICE_RANGEDB_004</code>. Nota: Para compatibilidad con las 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> Greenfield deployment of StorageGRID with StorageGRID-mapped drives is supported. However, you cannot use StorageGRID-mapped drives if you are upgrading from StorageGRID 11.4 or earlier. To use StorageGRID-mapped drives, you must configure the StorageGRID appliance to use StorageGRID-mapped drives during the initial installation. You cannot change this configuration after installation. If you are upgrading from StorageGRID 11.4 or earlier, you must use the standard drive mapping. For more information about StorageGRID-mapped drives, see the <code>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</code>. StorageGRID-mapped drives StorageGRID-mapped drives are drives that are mapped to a specific StorageGRID node. This mapping is persistent and does not change even if the drive is moved to a different slot in the appliance or if the appliance is rebooted. Using StorageGRID-mapped drives provides the following benefits: • Simplified drive replacement: When you replace a failed drive, the new drive is automatically mapped to the same StorageGRID node as the failed drive. You do not need to manually configure the mapping. • Improved reliability: StorageGRID-mapped drives help prevent data loss by ensuring that data is always written to the correct drive, even if the drive is moved to a different slot. • Easier troubleshooting: If a drive fails, you can easily identify which StorageGRID node is affected by looking at the drive mapping.	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>

BLOCK_DEVICE_TABLES

Standard drive mapping

With standard drive mapping, drives are mapped to StorageGRID nodes based on their physical slot location in the appliance. If you move a drive to a different slot, the mapping changes, and the data on the drive might no longer be accessible to the StorageGRID node.

If you are upgrading from StorageGRID 11.4 or earlier, you must continue to use standard drive mapping. You cannot migrate to StorageGRID-mapped drives.

How to determine which drive mapping is in use

You can determine which drive mapping is in use by looking at the **Drive Mapping** field on the **Nodes** page in the StorageGRID Grid Manager.

- If the field displays **StorageGRID-mapped**, the appliance is using StorageGRID-mapped drives.
- If the field displays **Standard**, the appliance is using standard drive mapping.

You can also use the StorageGRID API to determine which drive mapping is in use. For more information, see the .

Configuring StorageGRID-mapped drives

You configure StorageGRID-mapped drives during the initial installation of the StorageGRID appliance.

For instructions on how to configure StorageGRID-mapped drives, see the installation guide for your appliance:

*
*
*

Replacing drives

The procedure for replacing a drive depends on whether the appliance is using StorageGRID-mapped drives or standard drive mapping.

- **StorageGRID-mapped drives:** When you replace a failed drive, the new drive is automatically mapped to the correct StorageGRID node. You do not need to perform any manual configuration steps. For instructions, see .
- **Standard drive mapping:** When you replace a failed drive, you must ensure that the new drive is installed in the same physical slot as the failed drive. If you install the drive in a different slot, the data on the drive might not be accessible. For instructions, see .

Moving drives

You should not move drives between slots in the appliance unless you are instructed to do so by NetApp Support.

- **StorageGRID-mapped drives:** If you move a StorageGRID-mapped drive to a different slot, the mapping remains intact, and the data on the drive remains accessible to the StorageGRID node. However, moving drives is still not recommended.
- **Standard drive mapping:** If you move a drive to a different slot, the mapping changes, and the data on the drive might no longer be accessible to the StorageGRID node. This can result in data loss. Do not move drives if the appliance is using standard drive mapping. Se admite la implementación desde cero de StorageGRID con unidades asignadas a StorageGRID. Sin embargo, no puedes usar unidades asignadas a StorageGRID si vas a realizar una actualización desde StorageGRID 11.4 o versiones anteriores.

Para usar unidades asignadas a StorageGRID, debes configurar el dispositivo de StorageGRID para que use unidades asignadas a StorageGRID durante la instalación inicial. No puedes cambiar esta configuración después de la instalación.

Si vas a realizar una actualización desde StorageGRID 11.4 o versiones anteriores, debes usar la asignación de unidades estándar.

Para obtener más información sobre las unidades asignadas a StorageGRID, consulta la `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`.

Unidades asignadas a StorageGRID

Las unidades asignadas a StorageGRID son unidades que se asignan a un nodo de StorageGRID específico. Esta asignación es persistente y no cambia incluso si la unidad se mueve a una ranura diferente en el dispositivo o si este se reinicia.

El uso de unidades asignadas a StorageGRID proporciona las siguientes ventajas:

- **Sustitución de unidades simplificada:** cuando sustituyes una unidad que ha fallado, la nueva unidad se asigna automáticamente al mismo nodo de StorageGRID que la unidad que falló. No necesitas configurar la asignación de forma manual.
- **Fiabilidad mejorada:** las unidades asignadas a StorageGRID ayudan a evitar la pérdida de datos al garantizar que los datos siempre se escriban en la unidad correcta, incluso si la unidad se mueve a una ranura diferente.
- **Resolución de problemas más sencilla:** si una unidad falla, puedes identificar fácilmente qué nodo de StorageGRID se ve afectado al observar la asignación de unidades.

Asignación de unidades estándar

Con la asignación de unidades estándar, las unidades se asignan a los nodos de StorageGRID según su ubicación física en la ranura del dispositivo. Si mueves una unidad a una ranura diferente, la asignación cambia y es posible que el nodo de StorageGRID ya no pueda acceder a los datos de la unidad.

Valor	Denominación
Ruta y nombre del archivo especial de 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> Greenfield deployment of StorageGRID with StorageGRID-mapped drives is supported. However, you cannot use StorageGRID-mapped drives if you are upgrading from StorageGRID 11.4 or earlier. To use StorageGRID-mapped drives, you must configure the StorageGRID appliance to use StorageGRID-mapped drives during the initial installation. You cannot change this configuration after installation. If you are upgrading from StorageGRID 11.4 or earlier, you must use the standard drive mapping. For more information about StorageGRID-mapped drives, see the StorageGRID-mapped drives page. StorageGRID-mapped drives StorageGRID-mapped drives are drives that are mapped to a specific StorageGRID node. This mapping is persistent and does not change even if the drive is moved to a different slot in the appliance or if the appliance is rebooted. Using StorageGRID-mapped drives provides the following benefits: • Simplified drive replacement: When you replace a failed drive, the new drive is automatically mapped to the same StorageGRID node as the failed drive. You do not need to manually configure the mapping. • Improved reliability: StorageGRID-mapped drives help prevent data loss by ensuring that data is always written to the correct drive, even if the drive is moved to a different slot. • Easier troubleshooting: If a drive fails, you can easily identify which StorageGRID node is affected by looking at the drive mapping. Standard drive mapping With standard drive mapping, drives are mapped to StorageGRID nodes based on their physical slot location in the appliance. If you move a drive to a different slot, the mapping changes, and the data on the drive might no longer be accessible to the StorageGRID node. If you are upgrading from StorageGRID 11.4 or earlier, you must continue to use standard drive mapping. You cannot migrate to StorageGRID-mapped drives.	Requerido

BLOCK_DEVICE_VAR_LOCAL

How to determine which drive mapping is in use

You can determine which drive mapping is in use by looking at the **Drive Mapping** field on the **Nodes** page in the StorageGRID Grid Manager.

- If the field displays **StorageGRID-mapped**, the appliance is using StorageGRID-mapped drives.
- If the field displays **Standard**, the appliance is using standard drive mapping.

You can also use the StorageGRID API to determine which drive mapping is in use. For more information, see the .

Configuring StorageGRID-mapped drives

You configure StorageGRID-mapped drives during the initial installation of the StorageGRID appliance.

For instructions on how to configure StorageGRID-mapped drives, see the installation guide for your appliance:

*
*
*

Replacing drives

The procedure for replacing a drive depends on whether the appliance is using StorageGRID-mapped drives or standard drive mapping.

- **StorageGRID-mapped drives:** When you replace a failed drive, the new drive is automatically mapped to the correct StorageGRID node. You do not need to perform any manual configuration steps. For instructions, see .
- **Standard drive mapping:** When you replace a failed drive, you must ensure that the new drive is installed in the same physical slot as the failed drive. If you install the drive in a different slot, the data on the drive might not be accessible. For instructions, see .

Moving drives

You should not move drives between slots in the appliance unless you are instructed to do so by NetApp Support.

- **StorageGRID-mapped drives:** If you move a StorageGRID-mapped drive to a different slot, the mapping remains intact, and the data on the drive remains accessible to the StorageGRID node. However, moving drives is still not recommended.
- **Standard drive mapping:** If you move a drive to a different slot, the mapping changes, and the data on the drive might no longer be accessible to the StorageGRID node. This can result in data loss. Do not move drives if the appliance is using standard drive mapping. Se admite la implementación desde cero de StorageGRID con unidades asignadas a StorageGRID. Sin embargo, no puedes usar unidades asignadas a StorageGRID si vas a realizar una

Valor	Denominación
Ruta y nombre del archivo especial de dispositivo de bloques 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> Greenfield deployment of StorageGRID with StorageGRID-mapped drives is supported. However, you cannot use StorageGRID-mapped drives if you are upgrading from StorageGRID 11.4 or earlier. To use StorageGRID-mapped drives, you must configure the StorageGRID appliance to use StorageGRID-mapped drives during the initial installation. You cannot change this configuration after installation. If you are upgrading from StorageGRID 11.4 or earlier, you must use the standard drive mapping. For more information about StorageGRID-mapped drives, see the <code>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</code>. StorageGRID-mapped drives StorageGRID-mapped drives are drives that are mapped to a specific StorageGRID node. This mapping is persistent and does not change even if the drive is moved to a different slot in the appliance or if the appliance is rebooted. Using StorageGRID-mapped drives provides the following benefits: • Simplified drive replacement: When you replace a failed drive, the new drive is automatically mapped to the same StorageGRID node as the failed drive. You do not need to manually configure the mapping. • Improved reliability: StorageGRID-mapped drives help prevent data loss by ensuring that data is always written to the correct drive, even if the drive is moved to a different slot. • Easier troubleshooting: If a drive fails, you can easily identify which StorageGRID node is affected by looking at the drive mapping. Standard drive mapping With standard drive mapping, drives are mapped to StorageGRID nodes based on their physical slot location in the appliance. If you move a drive to a different slot, the mapping changes, and the data on the drive might no longer be accessible to the StorageGRID node. If you are upgrading from StorageGRID 11.4 or earlier, you must continue to use standard drive mapping. You cannot migrate to StorageGRID-mapped drives. How to determine which drive mapping is in use You can determine which drive mapping is in use by looking at the Drive Mapping field on the Nodes page in the StorageGRID Grid Manager.	Requerido

Claves de red del cliente

/o, if the field has the value **StorageGRID-mapped**, the appliance is using StorageGRID-mapped drives.

Valor	Denominación
DHCP, ESTÁTICO o DESACTIVADO	Opcional

You can also use the StorageGRID API to determine which drive mapping is in use. For more information, see the .

CLIENT_NETWORK_GATEWAY

Valor	Denominación
Dirección IPv4 de la puerta de enlace de la red local del cliente 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

The procedure for replacing a drive depends on whether the appliance is using StorageGRID-mapped drives or standard drive mapping.

CLIENT_NETWORK_IP

- **StorageGRID-mapped drives:** When you replace a failed drive, the

Valor	Denominación
Dirección IPv4 de este nodo en la red del cliente. Esta clave solo es necesaria cuando CLIENT_NETWORK_CONFIG = STATIC; no la especifiques para otros valores. Ejemplos: 1.1.1.1 10.224.4.81	Obligatorio cuando CLIENT_NETWORK_CONFIG = STATIC Opcional de lo contrario.

- **StorageGRID-mapped drives:** If you move a StorageGRID-mapped drive to a different slot, the mapping remains intact, and the data on

Valor	Denominación
La dirección MAC de la interfaz de red del cliente en el contenedor. Este campo es opcional. Si no se indica, 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

Para usar unidades asignadas a StorageGRID, debes configurar el dispositivo de StorageGRID para que use unidades asignadas a StorageGRID durante la instalación inicial. No puedes cambiar esta

CLIENT_NETWORK_MASK

Valor	Denominación
Máscara de red IPv4 para este nodo en la red del cliente. Especifica esta clave cuando CLIENT_NETWORK_CONFIG = STATIC; no la especifiques 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 de lo contrario.

no cambia incluso si la unidad se mueve a una ranura diferente en el dispositivo o si este se reinicia.

CLIENT_NETWORK_MTU

Valor	Denominación
La unidad máxima de transmisión (MTU) para este nodo en la red del cliente. No especifiques si CLIENT_NETWORK_CONFIG = DHCP. Si se especifica, el valor debe estar entre 1280 y 9216. Si se omite, se usa 1500. Si deseas utilizar tramas gigantes, configura el MTU con un valor adecuado para las tramas gigantes, como 9000. De lo contrario, mantén el valor predeterminado. IMPORTANTE: el valor de MTU de la red debe coincidir con el valor configurado en el puerto del switch al que está conectado el nodo. De lo contrario, podrían producirse problemas de rendimiento de la red o pérdida de paquetes. Ejemplos: 1500 8192	Opcional

a los datos de la unidad.

CLIENT_NETWORK_TARGET

Si vas a realizar una actualización desde StorageGRID 11.4 o versiones anteriores, debes seguir usando la asignación de unidades estándar. No puedes migrar a unidades asignadas a StorageGRID.

Cómo determinar qué asignación de unidades se está utilizando

Puedes determinar qué asignación de unidades se está utilizando observando el campo **Asignación de unidades** en la página **Nodos** en el Gestor de grid de StorageGRID.

- Si el campo muestra **Asignada a StorageGRID**, el dispositivo está utilizando unidades asignadas a StorageGRID.
- Si el campo muestra **Estándar**, el dispositivo está utilizando la asignación de unidades estándar.

También puedes usar la API de StorageGRID para determinar qué

Valor	Denominación
Nombre del dispositivo host que usarás para el acceso a la red de clientes por parte del nodo de StorageGRID. Solo se admiten nombres de interfaz de red. Por lo general, usarás un nombre de interfaz diferente al que especificaste para GRID_NETWORK_TARGET o ADMIN_NETWORK_TARGET. Nota: No utilices dispositivos bond o bridge como destino de red. Configura una VLAN (u otra interfaz virtual) sobre el dispositivo bond, o utiliza un bridge y un par de Ethernet virtual (veth). Práctica recomendada: especifica un valor incluso si este nodo no tendrá inicialmente una dirección IP de red de cliente. Así podrás añadir una dirección IP de red de cliente más adelante, sin tener que volver a configurar el nodo en el host. Ejemplos: <pre>bond0.1003</pre> <pre>ens423</pre>	Mejor práctica

• **Unidades asignadas a StorageGRID:** cuando sustituyes una unidad que ha fallado, la nueva unidad se asigna automáticamente al nodo de StorageGRID correcto. No necesitas realizar ningún paso adicional.

Valor	Denominación
Interfaz (Este es el único valor admitido.)	Opcional

en la misma ranura física que la unidad que falló. Si instalas la unidad en un cliente diferente, asegúrate de poder acceder a los datos de la unidad. Para obtener instrucciones, consulta [Consideraciones y recomendaciones para la clonación de direcciones MAC](#).

Valor	Denominación
Verdadero o falso Establece la clave en «true» para que el contenedor de StorageGRID utilice la dirección MAC de la interfaz de destino del host en la red del cliente. Práctica recomendada: En redes donde se requiera el modo promiscuo, usa la clave CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC en su lugar. Para obtener más detalles sobre la clonación de MAC para Linux, consulta "Consideraciones y recomendaciones para la clonación de direcciones MAC"	Mejor práctica

Claves de la red Grid

```
/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd
```

```
/dev/mapper/sgws-sn1-var-local
```

GRID_NETWORK_CONFIG

Valor	Denominación
ESTÁTICA o DHCP El valor predeterminado es STATIC si no se especifica.	Mejor práctica

GRID_NETWORK_GATEWAY

Valor	Denominación
Dirección IPv4 de la puerta de enlace de la red Grid 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 Grid Network es una única subred sin puerta de enlace, utiliza la dirección de puerta de enlace estándar de la subred (X.Y.Z.1) o el valor GRID_NETWORK_IP de este nodo; cualquiera de estos valores simplificará posibles futuras ampliaciones de la Grid Network.	Requerido

GRID_NETWORK_IP

Valor	Denominación
Dirección IPv4 de este nodo en la Grid Network. Esta clave solo es necesaria cuando GRID_NETWORK_CONFIG = STATIC; no la especifiques para otros valores. Ejemplos: 1.1.1.1 10.224.4.81	Obligatorio cuando GRID_NETWORK_CONFIG = STATIC Opcional de lo contrario.

GRID_NETWORK_MAC

Valor	Denominación
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 no se indica, se generará automáticamente una dirección MAC.

GRID_NETWORK_MASK

Valor	Denominación
Máscara de red IPv4 para este nodo en la Grid Network. Especifica esta clave cuando GRID_NETWORK_CONFIG = STATIC; no la especifiques para otros valores. Ejemplos: 255.255.255.0 255.255.248.0	Es obligatorio cuando se especifica GRID_NETWORK_IP y GRID_NETWORK_CONFIG = STATIC. Opcional de lo contrario.

GRID_NETWORK_MTU

Valor	Denominación
La unidad máxima de transmisión (MTU) para este nodo en la red Grid. No lo especifiques si GRID_NETWORK_CONFIG = DHCP. Si lo especificas, el valor debe estar entre 1280 y 9216. Si lo omites, se usa 1500. Si deseas utilizar tramas gigantes, configura el MTU con un valor adecuado para las tramas gigantes, como 9000. De lo contrario, mantén el valor predeterminado. IMPORTANTE: el valor de MTU de la red debe coincidir con el valor configurado en el puerto del switch al que está conectado el nodo. De lo contrario, podrían producirse 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 de Grid Network. La alerta Discrepancia en el MTU de la red Grid se activa si existe una diferencia significativa en la configuración del MTU de la red Grid en los distintos nodos. No es necesario que los valores de MTU sean iguales para todos los tipos de red. Ejemplos: 1500 8192	Opcional

GRID_NETWORK_TARGET

Valor	Denominación
Nombre del dispositivo host que usarás para el acceso a la Grid Network por parte del nodo de StorageGRID. Solo se admiten nombres de interfaz de red. Normalmente, usas un nombre de interfaz diferente al especificado para ADMIN_NETWORK_TARGET o CLIENT_NETWORK_TARGET. Nota: No utilices dispositivos bond o bridge como destino de red. Configura una VLAN (u otra interfaz virtual) sobre el dispositivo bond, o utiliza un bridge y un par de Ethernet virtual (veth). Ejemplos: <pre>bond0.1001</pre> <pre>ens192</pre>	Requerido

GRID_NETWORK_TARGET_TYPE

Valor	Denominación
Interfaz (Este es el único valor admitido.)	Opcional

GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valor	Denominación
Verdadero o falso Establece el valor de la clave en "true" para que el contenedor de StorageGRID utilice la dirección MAC de la interfaz de destino del host en la red Grid. Práctica recomendada: En redes en las que sea necesario utilizar el modo promiscuo, usa en su lugar la clave GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Para obtener más detalles sobre la clonación de MAC para Linux, consulta "Consideraciones y recomendaciones para la clonación de direcciones MAC"	Mejor práctica

Clave de contraseña de instalación (temporal)

CUSTOM_TEMPORARY_PASSWORD_HASH

Valor	Denominación
Para el nodo de administración principal, establece una contraseña temporal predeterminada para la API de instalación de StorageGRID durante la instalación. Nota: Establece una contraseña de instalación únicamente en el nodo de administración principal. Si intentas 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, por defecto no se establece ninguna contraseña temporal. Como alternativa, puedes establecer una contraseña temporal usando la StorageGRID Installation API. 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. Puedes generar este hash con herramientas de CLI, como el comando <code>openssl passwd</code> en modo SHA-512.	Mejor práctica

Clave de interfaces

INTERFACE_TARGET_nnnn

Valor	Denominación
Nombre y descripción opcional de una interfaz adicional que desees añadir a este nodo. Puedes añadir varias interfaces adicionales a cada nodo. Para <i>nnnn</i>, especifica un número único para cada entrada <code>INTERFACE_TARGET</code> que añadas. Como valor, especifica el nombre de la interfaz física en el host bare-metal. Luego, si quieres, añade una coma y proporciona una descripción de la interfaz, que se muestra en la página de interfaces VLAN y en la página de grupos HA. Ejemplo: <code>INTERFACE_TARGET_0001=ens256, Trunk</code> Si añades una interfaz troncal, debes configurar una interfaz de VLAN en StorageGRID. Si añades una interfaz de acceso, puedes añadir la interfaz directamente a un grupo de HA; no necesitas configurar una interfaz de VLAN.	Opcional

Clave de RAM máxima

RAM_MÁXIMA

Valor	Denominación
La cantidad máxima de RAM que puede consumir este nodo. Si se omite esta clave, el nodo no tiene restricciones de memoria. Al configurar este campo para un nodo de producción, especifica un valor de al menos 24 GB y de 16 a 32 GB menos que la RAM total del sistema. Nota: El valor de la RAM afecta al espacio reservado para los metadatos de un nodo. Consulta "Descripción de qué es el espacio reservado para metadatos". El formato de este campo es <i>numberunit</i>, donde <i>unit</i> puede ser b, k, m o g. Ejemplos: 24g 38654705664b Nota: Si quieres utilizar esta opción, debes habilitar la compatibilidad del kernel con los cgroups de memoria.	Opcional

Claves de tipo de nodo

TIPO_DE_NODO

Valor	Denominación
Tipo de nodo: • VM_Admin_Node • VM_Storage_Node • VM_Archive_Node • VM_API_Gateway	Requerido

TIPO_DE_ALMACENAMIENTO

Valor	Denominación
Define el tipo de objetos que contiene un nodo de almacenamiento. Para obtener más información, consulta "Tipos de nodos de almacenamiento". Esta clave solo es necesaria para nodos con NODE_TYPE = VM_Storage_Node; no la especifiques para otros tipos de nodo. Tipos de almacenamiento: • combinado • data • metadatos Nota: Si no se especifica el STORAGE_TYPE, el tipo de nodo de almacenamiento se establece por defecto en combinado (datos y metadatos).	Opcional

Teclas de reasignación de puerto



La compatibilidad con la reasignación de puertos está en desuso y se eliminará en una futura versión. Para eliminar los puertos reasignados, consulta ["Eliminar las reasignaciones de puertos en los hosts bare metal"](#).

PORT_REMAP

Valor	Denominación
Reasigna cualquier puerto utilizado por un nodo para las comunicaciones internas entre nodos de la red o para las comunicaciones externas. La reasignación de puertos es necesaria si las políticas de red empresarial restringen uno o varios puertos utilizados por StorageGRID, como se describe en "Comunicaciones internas entre nodos de grid" o "Comunicaciones externas". IMPORTANTE: No reasignes los puertos que tengas previsto utilizar para configurar los endpoints del balanceador de carga. Nota: Si solo se configura PORT_REMAP, la asignación que especifiques se usará tanto para las comunicaciones entrantes como para las salientes. Si también se especifica PORT_REMAP_INBOUND, PORT_REMAP solo se aplicará 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 <i>grid</i>, <i>admin</i> o <i>client</i>, y <i>protocol</i> es <i>tcp</i> o <i>udp</i>. Ejemplo: <code>PORT_REMAP = client/tcp/18082/443</code> También puedes reasignar varios puertos utilizando una lista separada por comas. Ejemplo: <code>PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80</code>	Opcional

PORT_REMAP_INBOUND

Valor	Denominación
Reasigna las comunicaciones entrantes al puerto especificado. Si especificas PORT_REMAP_INBOUND pero no especificas un valor para PORT_REMAP, las comunicaciones salientes del puerto no cambian. IMPORTANTE: No reasignes los puertos que tengas previsto utilizar para configurar los endpoints 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 <i>grid</i>, <i>admin</i> o <i>client</i>, y <i>protocol</i> es <i>tcp</i> o <i>udp</i>. Ejemplo: <code>PORT_REMAP_INBOUND = grid/tcp/3022/22</code> También puedes reasignar varios puertos de entrada usando una lista separada por comas. Ejemplo: <code>PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22</code>	Opcional

Cómo los nodos grid descubren el nodo Admin primario en StorageGRID

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

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

- Puedes utilizar el parámetro ADMIN_IP para introducir manualmente la dirección IP del nodo de administración principal.
- Puedes omitir el parámetro ADMIN_IP para que el nodo de grid detecte el valor automáticamente. La detección automática es especialmente útil cuando la Red de grid utiliza DHCP para asignar la dirección IP al nodo de administración principal.

El descubrimiento automático del nodo de administración principal se realiza 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 consultar la dirección IP y obtenerla automáticamente. Sin embargo, como el tráfico IP de multidifusión no suele ser enrutable entre subredes, los nodos de otras subredes no pueden obtener directamente la dirección IP del nodo de administración principal.

Si utilizas la detección automática:



- Debes 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. De este modo, dicho nodo de la red publicará la dirección IP del nodo de administración principal para que los demás nodos de la subred puedan detectarlo mediante mDNS.
- Asegúrate de que tu infraestructura de red permita el paso del tráfico IP multicast dentro de una subred.

Implementa nodos grid como máquinas virtuales para StorageGRID con VMware vSphere

Tú usas el cliente web de VMware vSphere para implementar cada nodo de grid como una máquina virtual. Durante la implementación, se crea cada nodo de grid y se conecta a una o varias redes StorageGRID.

Si necesitas implementar cualquier nodo de almacenamiento de dispositivo StorageGRID, consulta ["Implementar el nodo de almacenamiento de appliance"](#).

Si lo deseas, puedes reasignar los puertos del nodo o aumentar la configuración de CPU o memoria del nodo antes de encenderlo.

Antes de empezar

- Has revisado cómo ["planificar y preparar la instalación"](#) y entiendes los requisitos de software, CPU y RAM, y almacenamiento y rendimiento.
- Conoces VMware vSphere Hypervisor y tienes experiencia en la implementación de máquinas virtuales en este entorno.



El paquete `open-vm-tools`, una implementación de código abierto similar a VMware Tools, se incluye con la máquina virtual de StorageGRID. No necesitas instalar VMware Tools manualmente.

- Has descargado y descomprimido la versión correcta del archivo de instalación de StorageGRID para VMware.



Si vas a implementar el nuevo nodo como parte de una operación de ampliación o recuperación, debes utilizar la versión de StorageGRID que se está ejecutando actualmente en la grid.

- Tienes el archivo StorageGRID Virtual Machine Disk (`.vmdk`):

```
NetApp-SG-version-SHA.vmdk
```

- Tienes los archivos `.ovf` y `.mf` para cada tipo de nodo de grid que estás implementando:

Nombre del archivo	Descripción
<code>vsphere-primary-admin.ovf</code> <code>vsphere-primary-admin.mf</code>	El archivo de plantilla y el archivo de manifiesto para el nodo de administración principal.
<code>vsphere-non-primary-admin.ovf</code> <code>vsphere-non-primary-admin.mf</code>	El archivo de plantilla y el archivo de manifiesto para un nodo de administración no principal.
<code>vsphere-storage.ovf</code> <code>vsphere-storage.mf</code>	El archivo de plantilla y el archivo de manifiesto de un nodo de almacenamiento.
<code>vsphere-gateway.ovf</code> <code>vsphere-gateway.mf</code>	El archivo de plantilla y el archivo de manifiesto de un Gateway Node.

- Los archivos `.vmdk`, `.ovf` y `.mf` están todos en el mismo directorio.
- Tienes un plan para minimizar los dominios de fallo. Por ejemplo, no debes implementar todos los nodos de puerta de enlace en un único vSphere ESXi host.



En un entorno de producción, no ejecutes más de un Storage Node en una misma máquina virtual. No ejecutes varias máquinas virtuales en el mismo host ESXi si eso pudiera provocar un problema inaceptable de dominio de fallo.

- Si estás implementando un nodo como parte de una operación de ampliación o recuperación, tienes la ["Instrucciones para ampliar un sistema StorageGRID"](#) o la ["instrucciones de recuperación y mantenimiento"](#).
- Si estás desplegando un nodo de StorageGRID como una máquina virtual con almacenamiento asignado desde un sistema NetApp ONTAP, has confirmado que el volumen no tiene habilitada una política de organización en niveles de FabricPool. Por ejemplo, si un nodo de StorageGRID se está ejecutando como una máquina virtual en un host de VMware, asegúrate de que el volumen que respalda el almacén de datos del nodo no tenga habilitada una política de organización en niveles de FabricPool. Deshabilitar la organización en niveles de FabricPool para los volúmenes usados con nodos de StorageGRID simplifica la

resolución de problemas y las operaciones de almacenamiento.



Nunca uses FabricPool para transferir ningún dato relacionado con StorageGRID de vuelta al propio StorageGRID. Transferir datos de StorageGRID de vuelta a StorageGRID aumenta la complejidad de la resolución de problemas y de las operaciones.

Acerca de esta tarea

Sigue estas instrucciones para implementar inicialmente nodos de VMware, añadir un nuevo nodo de VMware en una ampliación o sustituir un nodo de VMware como parte de una operación de recuperación. Excepto por lo que se indica en los pasos, el procedimiento de implementación de nodos es el mismo para todos los tipos de nodos, incluidos los Admin Nodes, Storage Nodes y Gateway Nodes.

Si vas a instalar un nuevo sistema StorageGRID:

- Puedes implementar los nodos en cualquier orden.
- Debes asegurarte de que cada máquina virtual pueda conectarse al nodo de administración principal a través de la red de grid.
- Debes implementar todos los nodos de la red antes de configurar la red.

Si estás llevando a cabo una operación de ampliación o recuperación:

- Debes asegurarte de que la nueva máquina virtual pueda conectarse a todos los demás nodos a través de la Grid Network.

Si necesitas reasignar alguno de los puertos del nodo, no enciendas el nuevo nodo hasta que hayas completado la configuración de la reasignación de puertos.



La compatibilidad con la reasignación de puertos está en desuso y se eliminará en una futura versión. Para eliminar los puertos reasignados, consulta ["Eliminar las reasignaciones de puertos en los hosts bare metal"](#).

Pasos

1. Utilizando VCenter, implementa una plantilla OVF.

Si especificas una URL, apunta a una carpeta que contenga los siguientes archivos. De lo contrario, selecciona 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 vas a implementar, utiliza estos archivos para implementar el nodo de administración principal de tu sistema StorageGRID:

```
NetApp-SG-version-SHA.vmdk  
vsphere-primary-admin.ovf  
vsphere-primary-admin.mf
```

2. Introduce un nombre para la máquina virtual.

Lo habitual es utilizar el mismo nombre tanto para la máquina virtual como para el nodo de grid.

3. Coloca la máquina virtual en la vApp o pool de recursos adecuado.

4. Si vas a implementar el nodo de administración principal, lee y acepta el Acuerdo de licencia de usuario final.

Dependiendo de tu 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 datastore.

5. Selecciona el almacenamiento para la máquina virtual.

Si estás desplegando un nodo como parte de una operación de recuperación, sigue las instrucciones de [paso de recuperación del almacenamiento](#) para añadir nuevos discos virtuales, volver a conectar los discos duros virtuales del nodo de grid con fallos, o ambos.

Al implementar un nodo de almacenamiento, utiliza tres o más volúmenes de almacenamiento, y cada volumen debe ser de 4 TB o más. Debes 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 tus requisitos de almacenamiento, deberías eliminarlos y asignar los VMDK o RDM adecuados para el almacenamiento antes de encender el nodo. Los VMDK se utilizan más comúnmente en entornos VMware y son más fáciles de gestionar, mientras que los RDM podrían ofrecer un mejor rendimiento para cargas de trabajo que utilizan tamaños de objeto más grandes (por ejemplo, de más de 100 MB).



Algunas instalaciones de StorageGRID pueden utilizar volúmenes de almacenamiento más grandes y con mayor actividad que las cargas de trabajo virtualizadas habituales. Es posible que tengas que ajustar algunos parámetros del hipervisor, como `MaxAddressableSpaceTB`, para lograr un rendimiento óptimo. Si observas un rendimiento deficiente, ponte en contacto con tu servicio de asistencia de virtualización para determinar si tu entorno podría beneficiarse de un ajuste de la configuración específico para la carga de trabajo.

6. Selecciona redes.

Determina qué redes StorageGRID utilizará el nodo seleccionando una red de destino para cada red de origen.

- Es necesaria la red Grid. Debes seleccionar una red de destino en el entorno 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 Grid deben poder comunicarse con el resto de nodos.
- Si utilizas la red de administración, selecciona una red de destino diferente en el entorno vSphere. Si no utilizas la red de administración, selecciona el mismo destino que seleccionaste para la red Grid.
- Si utilizas la red de cliente, selecciona una red de destino diferente en el entorno vSphere. Si no utilizas la red de cliente, selecciona el mismo destino que has seleccionado para la red de Grid.
- Si utilizas una red de administración o de clientes, los nodos no tienen que estar en la misma red de administración o de clientes.

7. Para **Personalizar plantilla**, configura las propiedades necesarias del nodo de StorageGRID.

a. Introduce el **nombre de nodo**.



Si vas a recuperar un nodo de la red, debes introducir el nombre del nodo que vas a recuperar.

b. Utiliza el menú desplegable **Contraseña temporal de instalación** para especificar una contraseña temporal de instalación, de modo que puedas acceder a la consola de la máquina virtual o a la API de instalación de StorageGRID, o usar SSH, antes de que el nuevo nodo se una al grid.



La contraseña de instalación temporal solo se utiliza durante la instalación del nodo. Después de añadir un nodo a la grid, puedes acceder a él usando la ["contraseña de la consola del nodo"](#), que aparece en el archivo `Passwords.txt` del Recovery Package.

- **Usar nombre de nodo:** El valor que has introducido en el campo **Nombre de nodo** se utiliza como contraseña temporal de instalación.
- **Utilizar contraseña personalizada:** Se utiliza una contraseña personalizada como contraseña temporal de instalación.
- **Desactivar contraseña:** no se utilizará ninguna contraseña de instalación temporal. Si necesitas acceder a la VM para depurar problemas de instalación, consulta ["Soluciona problemas de instalación"](#).

c. Si has seleccionado **Usar contraseña personalizada**, especifica la contraseña temporal de instalación que quieras usar en el campo **Contraseña personalizada**.

d. En la sección **Red Grid (eth0)**, selecciona ESTÁTICA o DHCP para la **configuración de la dirección IP de la red Grid**.

- Si seleccionas STATIC, introduce la **dirección IP de la red Grid**, la **máscara de red de la red Grid**, la **puerta de enlace de la red Grid** y el **MTU de la red Grid**.
- Si seleccionas DHCP, la **dirección IP de la red Grid**, la **máscara de red Grid** y la **puerta de enlace de la red Grid** se asignan automáticamente.

e. En el campo **IP de administración principal**, introduce la dirección IP del nodo de administración principal de la Grid Network.



Este paso no aplica si el nodo que estás implementando es el nodo de administración principal.

Si omites la dirección IP del nodo de administración principal, la dirección IP se detectará automáticamente si el nodo de administración principal, o al menos otro nodo de grid con ADMIN_IP configurado, está presente en la misma subred. Sin embargo, se recomienda establecer aquí la dirección IP del nodo de administración principal.

a. En la sección **Red de administración (eth1)**, selecciona ESTÁTICA, DHCP o DESACTIVADA para la **configuración de la dirección IP de la red de administración**.

- Si no quieres utilizar la red de administración, selecciona DESACTIVADA e introduce **0.0.0.0** como dirección IP de la red de administración. Puedes dejar los demás campos en blanco.
- Si seleccionas STATIC, introduce la **IP de la red de administración**, la **máscara de la red de administración**, la **puerta de enlace de la red de administración** y el **MTU de la red de administración**.

- Si seleccionas **STATIC**, introduce la **lista de subredes externas de la red de administración**. También debes configurar una puerta de enlace.
 - Si seleccionas **DHCP**, la **IP de la red de administración**, la **máscara de red de administración** y la **puerta de enlace de la red de administración** se asignan automáticamente.
- b. En la sección **Red del cliente (eth2)**, selecciona **ESTÁTICA**, **DHCP** o **DESACTIVADA** para la **configuración de la dirección IP de la red del cliente**.
- Si no quieres utilizar la red de cliente, selecciona **DESACTIVADA** e introduce **0.0.0.0** como dirección IP de la red de cliente. Puedes dejar los demás campos en blanco.
 - Si seleccionas **STATIC**, introduce la **IP de la red del cliente**, la **máscara de red del cliente**, la **puerta de enlace de la red del cliente** y el **MTU de la red del cliente**.
 - Si seleccionas **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. Revisa la configuración de la máquina virtual y realiza los cambios que sean necesarios.
9. Cuando estés listo para finalizar, selecciona **Finalizar** para iniciar la carga de la máquina virtual.
10. Si implementaste este nodo como parte de una operación de recuperación y no es una recuperación de nodo completo, haz lo siguiente después de que termine la implementación:
- a. Haz clic con el botón derecho del ratón en la máquina virtual y selecciona **Editar configuración**.
 - b. Selecciona cada disco duro virtual predeterminado que se haya designado para almacenamiento y selecciona **Eliminar**.
 - c. En función de las circunstancias de la recuperación de datos, añade nuevos discos virtuales según tus requisitos de almacenamiento, vuelve a conectar cualquier disco duro virtual que se haya conservado del nodo de grid averiado y retirado anteriormente, o ambas cosas.

Ten en cuenta las siguientes directrices importantes:

- Si vas a añadir nuevos discos, debes utilizar el mismo tipo de dispositivo de almacenamiento que se utilizaba 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 tus requisitos de almacenamiento, deberías eliminarlos y asignar los VMDK o RDM adecuados para el almacenamiento antes de encender el nodo. Los VMDK se utilizan más comúnmente en entornos VMware y son más fáciles de gestionar, mientras que los RDM podrían ofrecer un mejor rendimiento para cargas de trabajo que utilizan tamaños de objeto más grandes (por ejemplo, de más de 100 MB).
11. Si necesitas reasignar los puertos que utiliza este nodo, sigue estos pasos.

Es posible que tengas que reasignar un puerto si las políticas de red empresarial restringen el acceso a uno o más puertos que utiliza StorageGRID. Consulta la ["directrices de redes"](#) para ver los puertos que utiliza StorageGRID.



No reasignes los puertos utilizados en los endpoints del balanceador de carga.

- a. Selecciona la nueva máquina virtual.
- b. En la pestaña **Configurar**, selecciona **Settings > vApp Options**. La ubicación de **vApp Options** depende de la versión de vCenter.
- c. En la tabla **Propiedades**, busca **PORT_REMAP_INBOUND** y **PORT_REMAP**.
- d. Para reasignar simétricamente tanto las comunicaciones entrantes como las salientes de un puerto, selecciona **PORT_REMAP**.



La compatibilidad con la reasignación de puertos está en desuso y se eliminará en una futura versión. Para eliminar los puertos reasignados, consulta ["Eliminar las reasignaciones de puertos en los hosts bare metal"](#).



Si solo se configura PORT_REMAP, la asignación que especifiques se aplica tanto a las comunicaciones entrantes como a las salientes. Si también se especifica PORT_REMAP_INBOUND, PORT_REMAP aplica solo a las comunicaciones salientes.

- i. Selecciona **Establecer valor**.
- ii. Introduce la asignación de puertos:

```
<network type>/<protocol>/<default port used by grid node>/<new port>
```

<network type> es grid, admin o client, y <protocol> es tcp o udp.

Por ejemplo, para redirigir el tráfico SSH del puerto 22 al puerto 3022, escribe:

```
client/tcp/22/3022
```

Puedes reasignar varios puertos usando una lista separada por comas.

Por ejemplo:

```
client/tcp/18082/443, client/tcp/18083/80
```

- i. Selecciona **Aceptar**.
- e. Para especificar el puerto utilizado para las comunicaciones entrantes al nodo, selecciona **PORT_REMAP_INBOUND**.



Si especificas PORT_REMAP_INBOUND y no indicas ningún valor para PORT_REMAP, las comunicaciones salientes para el puerto no cambian.

- i. Selecciona **Establecer valor**.
- ii. Introduce la asignación de puertos:

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port used by grid node>
```

<network type> es grid, admin o client, y <protocol> es tcp o udp.

Por ejemplo, para redirigir el tráfico SSH entrante que se envía al puerto 3022 de modo que el nodo de la red lo reciba en el puerto 22, introduce lo siguiente:

```
client/tcp/3022/22
```

Puedes reasignar varios puertos de entrada usando una lista separada por comas.

Por ejemplo:

```
grid/tcp/3022/22, admin/tcp/3022/22
```

i. Selecciona **OK**

12. Si quieres aumentar la CPU o la memoria del nodo con respecto a la configuración predeterminada:
 - a. Haz clic con el botón derecho del ratón en la máquina virtual y selecciona **Editar configuración**.
 - b. Modifica el número de CPU o la cantidad de memoria según sea necesario.

Configura la **Reserva de memoria** con el mismo tamaño que la **Memoria** asignada a la máquina virtual.

c. Selecciona **Aceptar**.

13. Enciende la máquina virtual.

Después de que termines

Si implementaste este nodo como parte de un procedimiento de ampliación o recuperación, vuelve a esas instrucciones para completar el procedimiento.

Ejemplo de archivos de configuración para nodos de StorageGRID en Linux

Puedes usar los archivos de configuración de nodos de ejemplo para ayudarte a configurar los archivos de configuración de los nodos de tu sistema StorageGRID. Los ejemplos muestran archivos de configuración de nodos para todos los tipos de nodos de la grid.



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita "[Herramienta de matriz de interoperabilidad \(IMT\) de NetApp](#)".

En la mayoría de los nodos, puedes añadir la información de direccionamiento de la red de administración y de la red de clientes (IP, máscara, puerta de enlace, etc.) cuando configuras la grid usando el Grid Manager o la API de instalación. La excepción es el nodo de administración principal. Si quieres acceder a la dirección IP de la red de administración del nodo de administración principal para completar la configuración de la grid (por ejemplo, porque la red de la grid no está enrutada), debes 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 destino Client Network se ha configurado como práctica recomendada, aunque Client Network está desactivado de forma predeterminada.

Ejemplo de nodo de administración principal

Ejemplo de nombre de archivo: `/etc/storagegrid/nodes/dcl-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

Nombre de archivo de ejemplo: /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 pasarela

Nombre de archivo de ejemplo: /etc/storagegrid/nodes/dcl-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

Nombre de archivo de ejemplo: /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
```

Valida la configuración de StorageGRID en Linux

Una vez creados los archivos de configuración en /etc/storagegrid/nodes para cada uno de tus nodos de StorageGRID, debes comprobar el contenido de dichos archivos.



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

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

```
sudo storagegrid node validate all
```

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



Cuando usas solo un LUN en nodos dedicados exclusivamente a metadatos, puede aparecer un mensaje de advertencia que puedes ignorar.

```
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, puedes suprimir esta salida usando las opciones `-q` o `--quiet` en el comando `storagegrid` (por ejemplo, `storagegrid --quiet...`). Si suprimes la salida, el comando tendrá un valor de salida distinto de cero si se detecta alguna advertencia o error 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 detecta algún error de configuración, debes corregirlo 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

```

Inicia el servicio de host de StorageGRID en Linux

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



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Pasos

1. Ejecuta los siguientes comandos en cada host:

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

2. Ejecuta el siguiente comando para asegurarte de que la implementación se está llevando a cabo:

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

3. Si algún nodo muestra el estado "Not Running" o "Stopped", ejecuta el siguiente comando:

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

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

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

Conoce la API de REST de instalación de StorageGRID

StorageGRID ofrece la API de instalación de StorageGRID para realizar tareas de instalación.

La API utiliza la plataforma de código abierto Swagger para proporcionar la documentación de la API. Swagger permite tanto a desarrolladores como a usuarios sin conocimientos de programación interactuar con la API a través de una interfaz de usuario que ilustra cómo responde la API a los parámetros y opciones. Esta documentación da por hecho que estás familiarizado con las tecnologías web estándar y con el formato de datos JSON.



Cualquier operación de la API que realices a través de la página web de la documentación de la API es una operación en tiempo real. Ten cuidado de no crear, actualizar ni eliminar por error datos de configuración u otros datos.

Cada comando de la API de REST incluye la URL de la API, una acción HTTP, cualquier parámetro de URL obligatorio u opcional y una respuesta esperada de la API.

API de instalación de StorageGRID

La API de instalación de StorageGRID solo está disponible cuando estás configurando por primera vez tu sistema StorageGRID y si necesitas realizar una recuperación del nodo de administración principal. Puedes acceder a la API de instalación a través de HTTPS desde Grid Manager.

Para acceder a la documentación de la API, ve a la página web de instalación en el nodo de administración principal y selecciona **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. Puedes

consultar la versión de lanzamiento del producto y las versiones principales de la API compatibles con dicho lanzamiento.

- **grid** — Operaciones de configuración a nivel de grid. Puedes consultar y actualizar los ajustes de grid, incluidos los detalles de grid, las subredes de Grid Network, las contraseñas de grid y las direcciones IP de los servidores NTP y DNS.
- **nodos** — Operaciones de configuración a nivel de nodo. Puedes obtener una lista de nodos de la red, eliminar un nodo de la red, configurar un nodo de la red, ver un nodo de la red y restablecer la configuración de un nodo de la red.
- **provision** — Operaciones de aprovisionamiento. Puedes iniciar la operación de aprovisionamiento y ver el estado de la operación de aprovisionamiento.
- **recuperación** — Operaciones de recuperación del nodo de administración principal. Puedes restablecer la información, cargar el paquete de recuperación, iniciar la recuperación y ver el estado de la operación de recuperación.
- **paquete-de-recuperación** — Operaciones para descargar el paquete de recuperación.
- **sitios** — Operaciones de configuración a nivel de sitio. Puedes crear, ver, eliminar y modificar un sitio.
- **contraseña-temporal** — Operaciones sobre la contraseña temporal para proteger la mgmt-api durante la instalación.

Soluciona problemas de instalación de StorageGRID

Si surge algún problema durante la instalación de tu sistema StorageGRID, puedes acceder a los archivos de registro de la instalación. El soporte técnico también podría necesitar usar los archivos de registro de la instalación para resolver problemas.



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Linux

Los siguientes archivos de registro de instalación están disponibles en el contenedor que está ejecutando cada nodo:

- `/var/local/log/install.log` (se encuentra en todos los nodos del grid)
- `/var/local/log/gdu-server.log` (se encuentra en el Admin Node primario)

Los siguientes archivos de registro de instalación están disponibles desde el host:

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/node-name.log`

Para saber cómo acceder a los archivos de registro, consulta ["Recopilar archivos de registro y datos del sistema"](#).

VMware

A continuación se indican los principales archivos de registro de la instalación, que el soporte técnico podría necesitar para resolver problemas.

- `/var/local/log/install.log` (se encuentra en todos los nodos del grid)
- `/var/local/log/gdu-server.log` (se encuentra en el Admin Node primario)

Es necesario ajustar la reserva de recursos de la máquina virtual

Los archivos OVF incluyen una reserva de recursos diseñada para garantizar que cada nodo de grid tenga suficiente RAM y CPU para funcionar de manera eficiente. Si creas máquinas virtuales al implementar estos archivos OVF en VMware y no está disponible la cantidad predefinida de recursos, las máquinas virtuales no se iniciarán.

Acerca de esta tarea

Si estás seguro de que el host de la máquina virtual tiene recursos suficientes para cada nodo de grid, ajusta manualmente los recursos asignados a cada máquina virtual y luego intenta iniciar las máquinas virtuales.

Pasos

1. En el árbol de clientes del hipervisor de VMware vSphere, selecciona la máquina virtual que no está iniciada.
2. Haz clic con el botón derecho del ratón en la máquina virtual y selecciona **Editar configuración**.
3. En la ventana Propiedades de la máquina virtual, selecciona la pestaña **Recursos**.
4. Ajusta los recursos asignados a la máquina virtual:
 - a. Selecciona **CPU** y luego usa el control deslizante de Reserva para ajustar los MHz reservados para esta máquina virtual.
 - b. Selecciona **Memoria** y luego usa el control deslizante de Reserva para ajustar los MB reservados para esta máquina virtual.
5. Haz clic en **OK**.
6. Repite este proceso tantas veces como sea necesario para las demás máquinas virtuales alojadas en el mismo host de VM.

Se ha desactivado la contraseña de instalación temporal

Al implementar un nodo de VMware, puedes especificar, si lo deseas, una contraseña de instalación temporal. Necesitas esta contraseña para acceder a la consola de la VM o usar SSH antes de que el nuevo nodo se una al grid.

Si has optado por desactivar la contraseña temporal de instalación, debes realizar pasos adicionales para depurar problemas de instalación.

Puedes hacer cualquiera de las siguientes cosas:

- Vuelve a implementar la máquina virtual, pero especifica una contraseña de instalación temporal para que puedas acceder a la consola o usar SSH para depurar problemas de instalación.
- Usa vCenter para establecer la contraseña:
 - a. Apaga la máquina virtual.
 - b. Ve a **VM**, selecciona la pestaña **Configurar** y selecciona **vApp Options**.
 - c. Especifica el tipo de contraseña de instalación temporal que deseas configurar:
 - Selecciona **CUSTOM_TEMPORARY_PASSWORD** para establecer una contraseña temporal personalizada.
 - Selecciona **TEMPORARY_PASSWORD_TYPE** para usar el nombre de nodo como contraseña temporal.
 - d. Selecciona **Establecer valor**.
 - e. Establece la contraseña temporal:
 - Cambia **CUSTOM_TEMPORARY_PASSWORD** por un valor de contraseña personalizado.
 - Actualiza **TEMPORARY_PASSWORD_TYPE** con el valor **Use node name**.
 - f. Reinicia la máquina virtual para aplicar la nueva contraseña.

Información relacionada

- Para saber cómo acceder a los archivos de registro, consulta ["Referencia de los archivos de registro"](#).
- ["Soluciona problemas en un sistema StorageGRID"](#)
- Si necesitas más ayuda, ponte en contacto con ["Soporte de NetApp"](#).

Ejemplos de scripts

Ejemplo de cómo consolidar cuatro interfaces físicas en un solo enlace para StorageGRID en RHEL

Puedes utilizar los archivos de ejemplo para agrupar cuatro interfaces físicas de Linux en un único enlace LACP y luego crear tres interfaces VLAN que abarquen dicho enlace para usarlas como interfaces de red de StorageGRID Grid, Admin y Client Network.

Interfaces físicas

Ten en cuenta que los conmutadores situados en los otros extremos de los enlaces también deben tratar los cuatro puertos como un único tronco LACP o canal de puertos, y deben transmitir al menos las tres VLAN mencionadas 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 de VLAN

/etc/sysconfig/network-scripts/ifcfg-bond0.1001

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1002

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1003

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

Ejemplo de agregación de interfaces físicas para StorageGRID en Ubuntu y Debian

El archivo `/etc/network/interfaces` incluye tres secciones que definen las interfaces físicas, la interfaz de enlace y las interfaces VLAN. Puedes combinar las tres secciones de ejemplo en un solo archivo, lo que agrupará cuatro interfaces físicas de Linux en un solo enlace LACP y luego establecerá tres interfaces VLAN que dependen del enlace para usarlas como interfaces de red de StorageGRID Grid, Admin y Client.

Interfaces físicas

Ten en cuenta que los conmutadores situados en los otros extremos de los enlaces también deben tratar los cuatro puertos como un único tronco LACP o canal de puertos, y deben transmitir al menos las tres VLAN mencionadas 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 de VLAN

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

Configura la grid y completa la instalación

Ve al Grid Manager de StorageGRID

El Grid Manager sirve para definir toda la información necesaria para configurar tu sistema StorageGRID.

Antes de empezar

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

Pasos

1. Abre tu navegador web y ve a:

`https://primary_admin_node_ip`

También puedes acceder al Grid Manager en el puerto 8443:

`https://primary_admin_node_ip:8443`

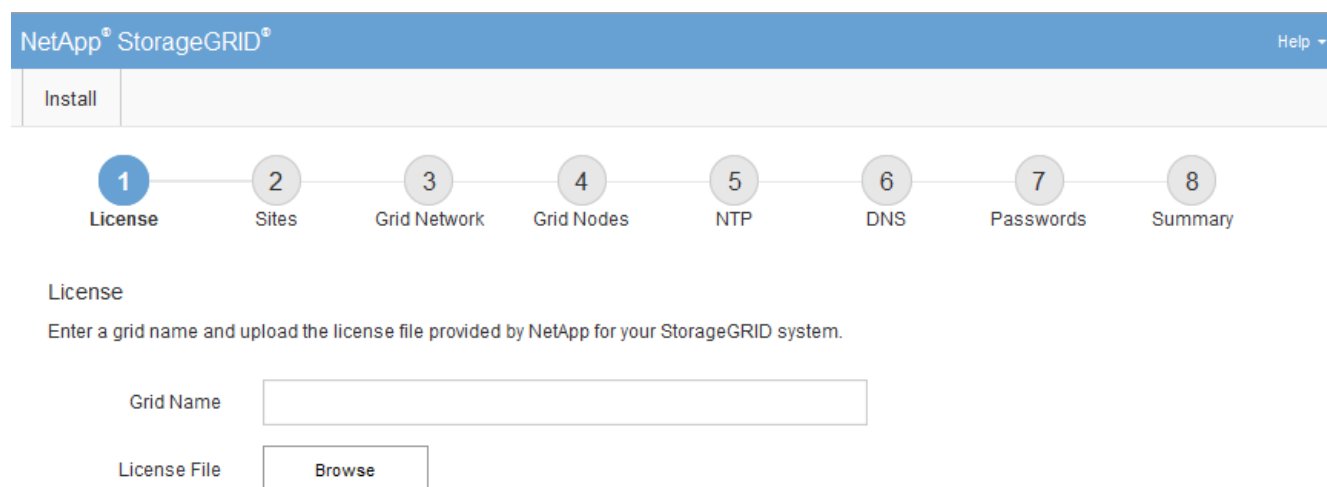
Puedes utilizar la dirección IP del nodo de administración principal en la red Grid o en la red de administración, según corresponda a tu configuración de red. Es posible que tengas que usar la opción de seguridad/avanzada en tu navegador para navegar a un certificado no confiable.

2. Gestiona una contraseña temporal de instalador según sea necesario:
 - Si ya se ha establecido una contraseña mediante uno de estos métodos, introduce la contraseña para continuar.
 - Un usuario estableció la contraseña al acceder al instalador anteriormente
 - Para Linux, la contraseña se importó automáticamente desde el archivo de configuración del nodo en `/etc/storagegrid/nodes/<node_name>.conf`
 - Para VMware, la contraseña de SSH/console se importó automáticamente desde las propiedades del OVF

- Si no se ha establecido una contraseña, opcionalmente establece una para proteger el instalador de StorageGRID.

3. Selecciona **Instalar un sistema StorageGRID**.

Aparece la página que se usa para configurar una grid de 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

Indica la información de la licencia de StorageGRID

Debes especificar el nombre de tu sistema StorageGRID y cargar el archivo de licencia facilitado por NetApp.

Pasos

1. En la página «Licencia», introduce un nombre descriptivo para tu sistema StorageGRID en el campo **Grid Name**.

Tras la instalación, el nombre aparece en la parte superior del menú Nodes.

2. Selecciona **Examinar**, busca el archivo de licencia de NetApp ((NLF-*unique-id*.txt) y selecciona **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 da derecho a ningún soporte para el producto. Puedes 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. Selecciona **Siguiente**.

Agrega sitios en StorageGRID

Debes crear al menos un sitio cuando instales StorageGRID. Puedes crear sitios adicionales para aumentar la fiabilidad y la capacidad de almacenamiento de tu sistema StorageGRID.

Pasos

1. En la página «Sitios», introduce el **Site Name**.
2. Para añadir sitios adicionales, haz clic en el signo más situado junto a la última entrada de sitio e introduce el nombre en el nuevo cuadro de texto **Nombre del sitio**.

Agrega tantos sitios adicionales como sea necesario para la topología de tu grid. Puedes agregar hasta 16 sitios.

NetApp® StorageGRID® Help ▾

Install

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

Sites

In a single-site deployment, infrastructure and operations are centralized in one site.

In a multi-site deployment, infrastructure can be distributed asymmetrically across sites, and proportional to the needs of each site. Typically, sites are located in geographically different locations. Having multiple sites also allows the use of distributed replication and erasure coding for increased availability and resiliency.

Site Name 1: **×**

Site Name 2: **+ ×**

3. Haz clic en **Next**.

Especifica las subredes de la red Grid para StorageGRID

Debes 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 de tu sistema StorageGRID, junto con cualquier subred a la que se deba poder acceder a través de la red Grid.

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

Pasos

1. Especifica la dirección de red CIDR de al menos una Grid Network en la casilla de texto **Subred 1**.
2. Haz clic en el signo más situado junto a la última entrada para añadir una entrada de red adicional. Debes especificar todas las subredes de todos los sitios en la Grid Network.
 - Si ya has implementado al menos un nodo, haz clic en **Detectar subredes de la red Grid** para que la lista de subredes de la red Grid se rellene automáticamente con las subredes comunicadas por los nodos de la red Grid que se han registrado en el Grid Manager.
 - Debes añadir manualmente cualquier subred para NTP, DNS, LDAP u otros servidores externos a los que se acceda a través de la pasarela de Grid Network.

The screenshot shows the NetApp StorageGRID installation wizard interface. 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, 3. Grid Network (current step), 4. Grid Nodes, 5. NTP, 6. DNS, 7. Passwords, and 8. Summary. Below the progress bar, the 'Grid Network' section is active. It contains a text box for 'Subnet 1' with the value '172.16.0.0/21' and a '+' icon to its right. Below this is a button labeled 'Discover Grid Network subnets'.

3. Haz clic en **Next**.

Aprueba los nodos de grid pendientes para StorageGRID

Debes aprobar cada nodo de la red antes de que pueda incorporarse al sistema StorageGRID.

Antes de empezar

Ya has implementado todos los nodos de grid virtuales y de appliance StorageGRID.



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

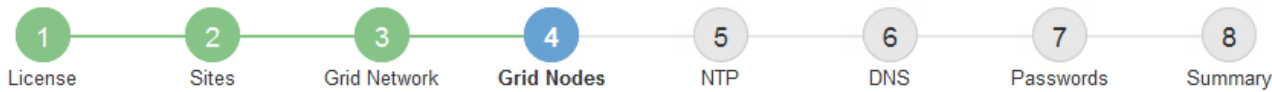
Pasos

1. Revisa la lista de nodos pendientes y comprueba que aparezcan todos los nodos de grid que has implementado.



Si falta un nodo de la red, comprueba que se haya implementado correctamente y que tenga configurada en ADMIN_IP la dirección IP de la Grid Network del nodo de administración principal.

2. Selecciona el botón de opción situado junto al nodo pendiente que quieras 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. Haz clic en **Aprobar**.
4. En «Configuración general», modifica los ajustes de las siguientes propiedades según sea necesario:
 - **Sitio:** El nombre del sistema del sitio para este nodo de la grid.
 - **Nombre:** El nombre de sistema para el nodo. El nombre predeterminado es el que especificaste al configurar el nodo.

Los nombres del sistema son necesarios para las operaciones internas de StorageGRID y no se

pueden cambiar después de que completes la instalación. Sin embargo, durante este paso del proceso de instalación, puedes cambiar los nombres del sistema según sea necesario.



En el caso de un nodo de VMware, puedes cambiar el nombre aquí, pero esta acción no modificará el nombre de la máquina virtual en vSphere.

- **Rol de NTP:** el rol de Network Time Protocol (NTP) del nodo de grid. Las opciones son **Automático**, **Primario** y **Ciente**. Seleccionar **Automático** asigna el rol Primario a los nodos de administración, los nodos de almacenamiento con servicios ADC, los nodos de puerta de enlace y cualquier nodo de grid que tenga direcciones IP no estáticas. A todos los demás nodos de grid se les asigna el rol Cliente.



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

- **Tipo de almacenamiento** (solo Storage Nodes): especifica que un nuevo Storage Node se use exclusivamente para datos, solo para metadatos o para ambos. Las opciones son **Datos y metadatos** ("combinado"), **Solo datos** y **Solo metadatos**.



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

- **Servicio ADC** (solo nodos de almacenamiento): Selecciona **Automático** para que el sistema determine si el nodo necesita el servicio de controlador de dominio administrativo (ADC). El servicio ADC realiza un seguimiento de la ubicación y la disponibilidad de los servicios de grid. Al menos tres nodos de almacenamiento en cada sitio deben incluir el servicio ADC. No puedes añadir el servicio ADC a un nodo después de que se haya implementado.

5. En Grid Network, modifica la configuración de las siguientes propiedades según sea necesario:

- **Dirección IPv4 (CIDR):** la dirección de red CIDR de 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 de grid. Por ejemplo: 192.168.0.1

La puerta de enlace es necesaria si hay varias subredes de grid.



Si has seleccionado DHCP para la configuración de la red Grid y modificas el valor aquí, el nuevo valor se configurará como una dirección estática en el nodo. Debes asegurarte de que la dirección IP configurada no se encuentre dentro de un rango de direcciones DHCP.

6. Si deseas configurar la red de administración para el nodo de grid, añade o actualiza los ajustes en la sección de red de administración según sea necesario.

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



Si seleccionaste DHCP para la configuración de la red de administración y cambias el valor aquí, el nuevo valor se configurará como una dirección estática en el nodo. Debes asegurarte de que la dirección IP configurada no esté dentro de un pool de direcciones DHCP.

Dispositivos: En el caso de un dispositivo StorageGRID, si la red de administración no se configuró durante la instalación inicial mediante el instalador de dispositivos StorageGRID, no se puede configurar en este cuadro de diálogo de Grid Manager. En su lugar, tienes que seguir estos pasos:

- a. Reinicia el appliance: en el Appliance Installer, selecciona **Advanced > Reboot**.

El reinicio puede tardar varios minutos.

- b. Selecciona **Configurar red > Configuración de enlaces** y activa las redes correspondientes.
- c. Selecciona **Configurar red > Configuración de IP** y configura las redes habilitadas.
- d. Vuelve a la página de inicio y haz clic en **Iniciar instalación**.
- e. En el Grid Manager: si el nodo aparece en la tabla de Nodos aprobados, elimina el nodo.
- f. Elimina el nodo de la tabla Nodos pendientes.
- g. Espera a que el nodo vuelva a aparecer en la lista de Nodos pendientes.
- h. Confirma que puedes configurar las redes correspondientes. Ya deberían estar completadas con la información que proporcionaste en la página IP Configuration del Appliance Installer.

Para obtener información adicional, consulta el ["Guía de inicio rápido para la instalación del hardware"](#) para localizar las instrucciones de tu dispositivo.

7. Si quieres configurar la red de clientes para el nodo de grid, añade o actualiza los ajustes en la sección de la red de clientes según sea necesario. Si la red de clientes está configurada, necesitarás la puerta de enlace, que se convertirá en la puerta de enlace predeterminada para el nodo después de la instalación.



Si seleccionaste DHCP para la configuración de Client Network y cambias el valor aquí, el nuevo valor se configurará como una dirección estática en el nodo. Debes asegurarte de que la dirección IP configurada no esté dentro de un pool de direcciones DHCP.

Dispositivos: En el caso de un dispositivo StorageGRID, si la red de clientes no se configuró durante la instalación inicial mediante el instalador de dispositivos StorageGRID, no se puede configurar en este cuadro de diálogo de Grid Manager. En su lugar, tienes que seguir estos pasos:

- a. Reinicia el appliance: en el Appliance Installer, selecciona **Advanced > Reboot**.

El reinicio puede tardar varios minutos.

- b. Selecciona **Configurar red > Configuración de enlaces** y activa las redes correspondientes.
- c. Selecciona **Configurar red > Configuración de IP** y configura las redes habilitadas.
- d. Vuelve a la página de inicio y haz clic en **Iniciar instalación**.
- e. En el Grid Manager: si el nodo aparece en la tabla de Nodos aprobados, elimina el nodo.
- f. Elimina el nodo de la tabla Nodos pendientes.
- g. Espera a que el nodo vuelva a aparecer en la lista de Nodos pendientes.
- h. Confirma que puedes configurar las redes correspondientes. Ya deberían estar completadas con la

información que proporcionaste en la página IP Configuration del Appliance Installer.

Para obtener información adicional, consulta el ["Guía de inicio rápido para la instalación del hardware"](#) para localizar las instrucciones de tu dispositivo.

8. Haz clic en **Guardar**.

La entrada del nodo de la grid pasa 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

Q

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.

✎ 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
☐	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

◀

▶

9. Repite estos pasos para cada nodo de grid pendiente que quieras aprobar.

Debes aprobar todos los nodos que quieras tener en el grid. Sin embargo, puedes volver a esta página en cualquier momento antes de hacer clic en **Instalar** en la página Resumen. Puedes modificar las propiedades de un nodo de grid aprobado seleccionando su botón de opción y haciendo clic en **Editar**.

10. Cuando hayas terminado de aprobar los nodos de la red, haz clic en **Siguiente**.

Especifica la información del servidor Network Time Protocol para StorageGRID

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

Acerca de esta tarea

Debes especificar las direcciones IPv4 de los servidores NTP.

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

Debes especificar cuatro referencias de servidor NTP de Stratum 3 o superior para evitar problemas de desviación horaria.



Al especificar la fuente NTP externa para una instalación de StorageGRID en entorno de producción, no utilices el servicio Windows Time (W32Time) en versiones de Windows anteriores a Windows Server 2016. El servicio de hora de las versiones anteriores de Windows no es lo suficientemente preciso y no es compatible por Microsoft para su uso en entornos de alta precisión, como StorageGRID.

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

Los servidores NTP externos son utilizados por los nodos a los que previamente asignaste funciones de NTP primario.



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

(Solo VMware) Realiza comprobaciones adicionales para VMware, como asegurarte de que el hipervisor utilice la misma fuente NTP que la máquina virtual y usa VMTools para desactivar la sincronización horaria entre el hipervisor y las máquinas virtuales de StorageGRID.

Pasos

1. Indica las direcciones IPv4 de al menos cuatro servidores NTP en los campos de texto **Servidor 1** a **Servidor 4**.
2. Si es necesario, selecciona el signo más situado junto a la última entrada para añadir más entradas de servidor.

NetApp® StorageGRID® Help ▾

Install

1

2

3

4

5

6

7

8

License

Sites

Grid Network

Grid Nodes

NTP

DNS

Passwords

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. Selecciona **Siguiente**.

Información relacionada

["Directrices de redes"](#)

Especifica la información del servidor DNS para StorageGRID

Debes especificar la información de DNS de tu sistema StorageGRID para poder acceder a servidores externos utilizando nombres de host en lugar de direcciones IP.

Acerca de esta tarea

Al especificar ["Información del servidor DNS"](#), podrás utilizar nombres de host con dominio completo (FQDN) en lugar de direcciones IP para las notificaciones por correo electrónico y AutoSupport.

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

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

Pasos

1. Indica la dirección IPv4 de al menos un servidor DNS en el cuadro de texto **Server 1**.
2. Si es necesario, selecciona el signo más situado junto a la última entrada para añadir más entradas de servidor.

NetApp® StorageGRID®
Help

Install

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

Domain Name Service

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.

Server 1
10.224.223.130
✖

Server 2
10.224.223.136
+ ✖

Lo más recomendable es especificar al menos dos servidores DNS. Puedes especificar hasta seis servidores DNS.

3. Selecciona **Siguiente**.

Especifica las contraseñas del sistema StorageGRID

Como parte de la instalación de tu sistema StorageGRID, debes introducir las contraseñas que usarás para proteger tu sistema y realizar tareas de mantenimiento.

Acerca de esta tarea

Utiliza la página «Instalar contraseñas» para especificar la frase de contraseña de aprovisionamiento y la contraseña del usuario raíz de gestión de grid.

- La frase de acceso de aprovisionamiento se usa como clave de cifrado y no la almacena el sistema StorageGRID.
- Debes disponer de la frase de contraseña de aprovisionamiento para los procedimientos de instalación, ampliación y mantenimiento, incluida la descarga del Recovery Package. Por lo tanto, es importante que guardes la frase de contraseña de aprovisionamiento en un lugar seguro.
- Puedes cambiar la contraseña de aprovisionamiento desde Grid Manager si tienes la actual.
- La contraseña del usuario raíz de gestión de la grid se puede cambiar usando el Grid Manager.
- Las contraseñas de la consola de línea de comandos y de SSH generadas aleatoriamente se almacenan en el archivo `Passwords.txt` del paquete de recuperación.

Pasos

1. En **Contraseña de aprovisionamiento**, introduce la contraseña de aprovisionamiento que se requerirá para realizar cambios en la topología de grid de tu sistema StorageGRID.

Guarda la frase de contraseña de aprovisionamiento en un lugar seguro.



Si, una vez finalizada la instalación, deseas cambiar la contraseña de aprovisionamiento más adelante, puedes utilizar el Grid Manager. Selecciona **Configuración > Control de acceso > Contraseñas de Grid**.

2. En **Confirmar frase de contraseña de aprovisionamiento**, vuelve a introducir la frase de contraseña de aprovisionamiento para confirmarla.
3. En **Contraseña de usuario raíz de Grid Management**, introduce la contraseña que usarás para acceder a Grid Manager como usuario "raíz".



Guarda la frase de contraseña de aprovisionamiento en un lugar seguro. Es necesaria para los procedimientos de instalación, ampliación y mantenimiento.

4. En **Confirmar contraseña del usuario raíz**, vuelve a introducir 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.

5. Si vas a instalar una grid con fines de prueba de concepto o de demostración, puedes desmarcar la casilla **Crear contraseñas aleatorias para la línea de comandos**.

En las implementaciones de producción, siempre deben utilizarse contraseñas aleatorias por motivos de seguridad. Desmarca **Crear contraseñas aleatorias en la línea de comandos** solo para grids de demostración si quieres usar contraseñas predeterminadas para acceder a los nodos del grid desde la línea de comandos usando la cuenta "root" o "admin".



Se te pedirá que descargues el archivo Recovery Package (`sgws-recovery-package-id-revision.zip`) después de hacer clic en **Instalar** en la página de resumen. Debes ["descargar este archivo"](#) para completar la instalación. Las contraseñas necesarias para acceder al sistema se almacenan en el archivo `Passwords.txt`, que está incluido en el archivo Recovery Package.

6. Haz clic en **Next**.

Revisa tu configuración de StorageGRID

Debes revisar detenidamente la información de configuración que has introducido para asegurarte de que la instalación se complete correctamente.

Pasos

1. Consulta la página **Resumen**.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

Summary

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. Comprueba que toda la información de configuración de la grid sea correcta. Utiliza los enlaces Modificar en la página Resumen para volver atrás y corregir cualquier error.

3. Haz clic en **Instalar**.



Si un nodo está configurado para utilizar la red del cliente, la puerta de enlace predeterminada de ese nodo cambia de la red de grid a la red del cliente cuando haces clic en **Instalar**. Si pierdes la conectividad, debes asegurarte de que estás accediendo al nodo de administración principal a través de una subred accesible. Consulta "[Directrices de redes](#)" para más detalles.

4. Haz clic en **Descargar paquete de recuperación**.

Cuando la instalación llega al punto en el que se define la topología de la red, se te pedirá que descargues el archivo Recovery Package (.zip) y confirmes que puedes acceder correctamente al contenido de este archivo. Debes descargar el archivo Recovery Package para que puedas recuperar el sistema StorageGRID si uno o más nodos de la grid fallan. La instalación continúa en segundo plano, pero no puedes completarla ni acceder al sistema StorageGRID hasta que descargues y verifiques este archivo.

5. Comprueba que puedes extraer el contenido del archivo .zip y luego guardarlo en dos ubicaciones seguras y separadas.



El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

6. Marca la casilla **He descargado y verificado correctamente el archivo del paquete de recuperación** y haz clic en **Siguiente**.

Si la instalación aún está en curso, aparece la página de estado. Esta página muestra el progreso de la instalación para cada nodo de la grid.

Installation Status

If necessary, you may [Download the Recovery Package file](#) again.

Name	Site	Grid Network IPv4 Address	Progress	Stage
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 fase Complete en todos los nodos de la grid, aparece la página de sign-in del Grid Manager.

7. Inicia sesión en Grid Manager con el usuario raíz y la contraseña que especificaste durante la instalación.

Requisitos de red y DHCP después de instalar StorageGRID

Una vez completada la implementación y configuración de los nodos de la red, sigue estas directrices para la asignación de direcciones DHCP y los cambios en la configuración de la red.

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

Solo puedes configurar DHCP durante la fase de implementación. No puedes configurar DHCP durante la configuración.



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

- Debes seguir los procedimientos de «Cambiar IP» si deseas modificar las direcciones IP, las máscaras de subred y las puertas de enlace predeterminadas de un nodo de la red. Consulta "[Configurar direcciones IP](#)".
- Si realizas cambios en la configuración de red, incluidos los relacionados con el enrutamiento y la puerta de enlace, es posible que se pierda la conectividad de los clientes con el nodo de administración principal y con otros nodos de la grid. Dependiendo de los cambios de red aplicados, es posible que tengas que restablecer estas conexiones.

Conoce los pasos obligatorios y opcionales después de instalar StorageGRID

Una vez finalizada la instalación, realiza las tareas de integración y configuración necesarias. Puedes realizar las tareas opcionales según sea necesario.

Tareas obligatorias

- (Solo VMware) Configura el hipervisor VMware vSphere para el reinicio automático.

Debes configurar el hipervisor para que reinicie las máquinas virtuales cuando se reinicie el servidor. Sin un reinicio automático, las máquinas virtuales y los nodos de grid permanecerán apagados después de que se reinicie el servidor. Para obtener más detalles, consulta la documentación de VMware vSphere Hypervisor.

- ["Crear una cuenta de inquilino"](#) para el protocolo de cliente S3 que se utilizará para almacenar objetos en tu sistema StorageGRID.
- ["Control del acceso al sistema"](#) configurando grupos y cuentas de usuario. Si lo deseas, puedes ["configurar una fuente de identidad federada"](#) (como Active Directory u OpenLDAP), para poder importar grupos y usuarios de administración. O bien, puedes ["crear grupos y usuarios locales"](#).
- Integra y prueba las aplicaciones cliente ["S3 API"](#) que vas a utilizar para cargar objetos en tu sistema StorageGRID.
- ["Configura las reglas de gestión del ciclo de vida de la información \(ILM\) y la política de ILM"](#) que quieras utilizar para proteger los datos de los objetos.
- Si tu instalación incluye nodos de almacenamiento appliance, utiliza SANtricity OS para realizar las siguientes tareas:
 - Conéctate a cada dispositivo StorageGRID.
 - Verifica la recepción de los datos de AutoSupport.

Consulta ["Configurar el hardware"](#).

- Revisa y sigue la ["Directrices para el refuerzo de la seguridad del sistema StorageGRID"](#) para eliminar riesgos de seguridad.
- ["Configura las notificaciones por correo electrónico para las alertas del sistema"](#).

Tareas opcionales

- ["Actualizar las direcciones IP de los nodos de grid"](#) si han cambiado desde que planificaste tu implementación y generaste el paquete de recuperación.
- ["Configura el cifrado del almacenamiento"](#), si fuera necesario.
- ["Configura la compresión del almacenamiento"](#) para reducir el tamaño de los objetos almacenados, si fuera necesario.
- ["Configurar interfaces VLAN"](#) para aislar y dividir el tráfico de red, si fuera necesario.
- ["Configurar grupos de alta disponibilidad"](#) para mejorar la disponibilidad de la conexión para Grid Manager, Tenant Manager y los clientes S3, si fuera necesario.
- ["Configura los puntos de conexión del equilibrador de carga"](#) para la conectividad del cliente S3, si es necesario.

Actualizar el software StorageGRID

Actualizar el software StorageGRID

Sigue estas instrucciones para actualizar un sistema StorageGRID a una nueva versión.

Cuando realizas la actualización, todos los nodos de tu sistema StorageGRID se actualizan.



No comiences la actualización si necesitas ampliar urgentemente tu almacenamiento para aumentar la capacidad (si tu almacenamiento está casi lleno). Completa el procedimiento de actualización a tiempo. Si se requiere una recuperación, contacta al soporte técnico.

Antes de actualizar

Revisa estos temas para conocer las nuevas funciones y mejoras de StorageGRID 12.0, determinar si alguna función ha quedado obsoleta o se ha eliminado, y enterarte de los cambios en las API de StorageGRID.

- ["Cómo se ve afectado tu sistema durante la actualización"](#)
- ["Novedades de StorageGRID 12.0"](#)
- ["Funcionalidades eliminadas u obsoletas"](#)
- ["Cambios en la API de gestión de grid"](#)
- ["Cambios en la API de gestión de inquilinos"](#)

Planifica y prepárate para la actualización

Estima el tiempo para completar una actualización de StorageGRID

Valora cuándo realizar la actualización, teniendo en cuenta el tiempo que podría llevar. Ten en cuenta qué operaciones puedes y no puedes realizar durante cada fase de la actualización.

Acerca de esta tarea

El tiempo necesario para completar una actualización de StorageGRID depende de diversos factores, como la carga de los clientes 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 ofrecen instrucciones que puedes usar para estimar el tiempo de actualización de tu sistema.

Tarea de actualización	Descripción	Tiempo aproximado necesario	Durante esta tarea
Ejecuta comprobaciones previas y actualiza el nodo de administración principal	Se ejecutan las comprobaciones previas a la actualización y el nodo de administración principal se detiene, se actualiza y se reinicia.	30 minutos a 1 hora, siendo los nodos de servicios appliance los que requieren más tiempo. Los errores de comprobación previa sin resolver aumentarán este tiempo.	No se puede acceder al nodo de administración principal. Es posible que aparezcan mensajes de error de conexión, que puedes ignorar. Realizar las comprobaciones previas a la actualización antes de iniciarla te permite resolver cualquier error antes de la ventana de mantenimiento programada para la actualización.
Iniciar el servicio de actualización	Se distribuye el archivo de software y se inicia el servicio de actualización.	3 minutos por nodo de la grid	
Actualizar otros nodos de la red	El software de todos los demás nodos de la red se actualiza en el orden en que apruebes los nodos. Un nodo de administración o de puerta de enlace se actualiza al mismo tiempo que un nodo de almacenamiento.	Entre 15 minutos y 1 hora por nodo, siendo los nodos de los dispositivos los que requieren más tiempo Nota: Para los nodos de dispositivo, el instalador de StorageGRID Appliance se actualiza automáticamente a la última versión.	• No modifiques la configuración de la cuadrícula. • No modifiques la configuración del nivel de auditoría. • No actualices la configuración de ILM. • No puedes realizar otros procedimientos de mantenimiento, como la corrección urgente, decomisionar o la ampliación. Nota: Si necesitas realizar una recuperación, ponte en contacto con soporte técnico.
Activar funciones	Las nuevas funciones de la nueva versión están activadas.	Menos de 5 minutos	• No modifiques la configuración de la cuadrícula. • No modifiques la configuración del nivel de auditoría. • No actualices la configuración de ILM. • No puedes realizar otro procedimiento de mantenimiento.

Tarea de actualización	Descripción	Tiempo aproximado necesario	Durante esta tarea
Actualizar la base de datos	El proceso de actualización comprueba cada nodo para verificar que no sea necesario actualizar la base de datos de Cassandra.	10 segundos por nodo o unos minutos para toda la grid	La actualización a StorageGRID 12.0 incluye una actualización de la base de datos Cassandra. Después de actualizar de StorageGRID 11.9 a 12.0, se realizará una actualización del formato de metadatos en segundo plano durante uno a tres días. Durante este tiempo, ciertos procedimientos de mantenimiento, como la expansión, estarán deshabilitados. En futuras versiones de StorageGRID, el paso de actualización de la base de datos Cassandra podría tardar 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 finalice la tarea Pasos finales de la actualización , podrás llevar a cabo todos los procedimientos de mantenimiento.

Estima el tiempo para la actualización

Pasos

1. Calcula el tiempo necesario para actualizar todos los nodos de la red.
 - a. Multiplica el número de nodos de tu sistema StorageGRID por 1 hora por nodo.

Por regla general, los nodos de dispositivos tardan más en actualizarse que los nodos basados en software.
 - b. Añade una hora a este tiempo para tener en cuenta el tiempo necesario para descargar el archivo `.upgrade`, ejecutar las validaciones previas y completar los pasos finales de la actualización.
2. Si tienes nodos Linux, añade 15 minutos por cada nodo para tener en cuenta el tiempo necesario para descargar e instalar el paquete RPM o DEB.
3. Calcula el tiempo total estimado para la actualización sumando los resultados de los pasos 1 y 2.

Ejemplo: tiempo estimado para actualizar a StorageGRID 12.0

Supongamos que tu sistema tiene 14 nodos de grid, de los cuales 8 son nodos Linux.

1. Multiplica 14 por 1 hora por nodo.
2. Añade una hora para tener en cuenta la descarga, la comprobación previa y los pasos finales.

El tiempo estimado para actualizar todos los nodos es de 15 horas.

3. Multiplica 8 por 15 minutos por nodo para tener en cuenta el tiempo necesario para instalar el paquete RPM o DEB en los nodos de Linux.

El tiempo estimado para este paso es de 2 horas.

4. Suma los valores.

Debes prever hasta 17 horas para completar la actualización de tu sistema a StorageGRID 12.0.0.



Si lo necesitas, puedes dividir la ventana de mantenimiento en ventanas más pequeñas aprobando subconjuntos de nodos de la grid para actualizarlos en varias sesiones. Por ejemplo, podrías preferir actualizar los nodos del sitio A en una sesión y luego actualizar los nodos del sitio B en una sesión posterior. Si eliges realizar la actualización en más de una sesión, ten en cuenta que no podrás empezar a usar las nuevas funciones hasta que todos los nodos hayan sido actualizados.

Cómo afectan las actualizaciones de StorageGRID a tu sistema

Descubre cómo se verá afectado tu sistema StorageGRID durante la actualización.

Se permite el acceso externo mediante SSH hasta que finalice la actualización

Durante la actualización se permite el acceso SSH externo. Una vez finalizada la actualización, el acceso SSH externo queda bloqueado de forma predeterminada. Tras la actualización, puedes utilizar la pestaña **Bloquear SSH**, disponible en la página **Grid Manager > Configuración de seguridad**, para ["gestionar el acceso externo mediante SSH"](#). El acceso SSH entre los nodos de la red no se ve afectado.

Las actualizaciones de StorageGRID se realizan sin interrupciones

El sistema StorageGRID puede recibir y recuperar datos de las aplicaciones cliente durante todo el proceso de actualización. Si autorizas la actualización de todos los nodos de un mismo tipo (por ejemplo, Storage Nodes), estos se desconectan de uno en uno, por lo que en ningún momento todos los nodos de la red ni todos los nodos de un tipo concreto quedan indisponibles.

Para garantizar la disponibilidad continua, asegúrate de que tu política de ILM incluya reglas que especifiquen el almacenamiento de varias copias de cada objeto. También debes asegurarte de que todos los clientes externos de S3 estén configurados para enviar solicitudes a uno de los siguientes:

- Una dirección IP virtual de un grupo de alta disponibilidad (HA)
- Un equilibrador de carga de terceros de alta disponibilidad
- Varios nodos de puerta de enlace para cada cliente
- Varios nodos de almacenamiento para cada cliente

Las aplicaciones de los clientes podrían experimentar interrupciones de corta duración

El sistema StorageGRID puede recibir y recuperar datos de las aplicaciones cliente durante todo el proceso de actualización; sin embargo, las conexiones de los clientes a nodos Gateway o nodos Storage concretos podrían verse interrumpidas temporalmente si la actualización requiere reiniciar los servicios en dichos nodos. La conectividad se restablecerá una vez que finalice el proceso de actualización y se reanuden los servicios en los nodos concretos.

Es posible que tengas que programar un tiempo de inactividad para aplicar una actualización si no es aceptable que se produzca una pérdida de conectividad durante un breve periodo de tiempo. Puedes utilizar la aprobación selectiva para programar cuándo se actualizan determinados nodos.



Puedes usar varias puertas de enlace y grupos de alta disponibilidad (HA) para proporcionar conmutación automática por error durante el proceso de actualización. Consulta las instrucciones para "[configuración de grupos de alta disponibilidad](#)".

Las reparaciones en segundo plano no se ejecutarán en grids con nodos de versiones mixtas

Las reparaciones en segundo plano no se ejecutan durante la actualización cuando la red contiene nodos de versiones mixtas. Cualquier inconsistencia que se produzca durante un fallo energético en el sitio no se reparará hasta que la actualización haya finalizado.

Se ha actualizado el firmware del appliance

Durante la actualización de StorageGRID 12.0:

- Todos los nodos del dispositivo StorageGRID se actualizan automáticamente a la versión 12.0 del firmware de StorageGRID Appliance Installer.
- Los dispositivos SG6060 y SGF6024 se actualizan automáticamente a la versión 3B08.EX del firmware de la BIOS y a la versión 4.01.07 del firmware del BMC.
- Los dispositivos SG100 y SG1000 se actualizan automáticamente a la versión 3B13.EC del firmware del BIOS y a la versión 4.75.07 del firmware del BMC.
- Los dispositivos SGF6112, SG6160, SG110 y SG1100 se actualizan automáticamente a la versión 3A14.QD del firmware BIOS y a la versión 3.19.07 del firmware BMC.

Las políticas de ILM se gestionan de forma diferente según su estado

- La política activa seguirá siendo la misma tras la actualización.
- Solo se conservan las últimas 10 políticas históricas al actualizar.
- Si hay una política propuesta, se eliminará durante la actualización.

Es posible que se activen alertas

Es posible que se activen alertas al iniciar y detener los servicios, así como cuando el sistema StorageGRID funcione en un entorno con versiones mixtas (en el que algunos nodos de la red ejecutan una versión anterior, mientras que otros se han actualizado a una versión posterior). También es posible que se activen otras alertas una vez finalizada la actualización.

Por ejemplo, es posible que veas la alerta **No se puede establecer comunicación con el nodo** cuando los servicios están detenidos, o que veas la alerta **Error de comunicación de Cassandra** cuando algunos nodos se han actualizado a StorageGRID 12.0 pero otros siguen ejecutando StorageGRID 11.9. En general, estas alertas se eliminarán cuando termine la actualización.

La alerta **ILM placement unachievable** puede activarse cuando los Storage Nodes se detienen durante la actualización a StorageGRID 12.0. Esta alerta puede persistir durante 1 día después de que se complete la actualización.

Una vez finalizada la actualización, puedes consultar cualquier alerta relacionada con la actualización seleccionando **Alertas resueltas recientemente** o **Alertas actuales** desde el panel de control de Grid Manager.

Los cambios en la configuración están restringidos



Esta lista se aplica específicamente a las actualizaciones de StorageGRID 11.9 a StorageGRID 12.0. Si vas a actualizar a otra versión de StorageGRID, consulta la lista de cambios restringidos en las instrucciones de actualización de esa versión.

Hasta que finalice la tarea **Habilitar nueva función**:

- No realices ningún cambio en la configuración de grid.
- No actives ni desactives ninguna función nueva.
- No actualices la configuración de ILM. De lo contrario, podrías encontrarte con un comportamiento inconsistente e inesperado de ILM.
- No apliques una corrección urgente ni recuperes un nodo de grid.



Ponte en contacto con el soporte técnico si necesitas recuperar un nodo durante la actualización.

- No debes gestionar grupos de alta disponibilidad, interfaces VLAN ni puntos finales del equilibrador de carga mientras actualizas a StorageGRID 12.0.
- No elimines ningún grupo de HA hasta que se complete la actualización a StorageGRID 12.0. Las direcciones IP virtuales de otros grupos de HA podrían quedar inaccesibles.

Hasta que finalice la tarea **Pasos finales de la actualización**:

- No realices un procedimiento de expansión.
- No realices un procedimiento de decomisionar.

Verifica la versión instalada de StorageGRID antes de actualizar

Antes de iniciar la actualización, verifica que la versión anterior de StorageGRID esté instalada con la última corrección urgente disponible aplicada.

Acerca de esta tarea

Antes de actualizar a StorageGRID 12.0, tu grid debe tener instalado StorageGRID 11.9.0.8 o una versión posterior. Si actualmente estás usando una versión anterior de StorageGRID, debes instalar todos los archivos de actualización anteriores junto con sus últimas correcciones urgentes (muy recomendable) hasta que la versión actual de tu grid sea al menos StorageGRID 11.9.0.8.

En la [ejemplo](#) se muestra una posible ruta de actualización.



NetApp te recomienda encarecidamente que apliques la última corrección urgente para cada versión de StorageGRID antes de actualizar a la siguiente versión, y que también apliques la última corrección urgente para cada nueva versión que instales. En algunos casos, debes aplicar una corrección urgente para evitar el riesgo de pérdida de datos. Consulta "[Descargas de NetApp: StorageGRID](#)" y las notas de la versión de cada corrección urgente para obtener más información.

Comprobar la versión instalada

Pasos

1. Inicia sesión en Grid Manager usando una "[navegador web compatible](#)" cuenta.

2. En la parte superior del Grid Manager, selecciona **Ayuda > Acerca de**.
3. Comprueba que la **versión** sea 11.9.0.8 o posterior.
4. Si **Versión** no es 11.9.0.8 o posterior, entra en "[Descargas de NetApp: StorageGRID](#)" para descargar los archivos de actualización y corrección urgente que necesites.
5. "[Sigue las instrucciones de actualización](#)" para cada versión que descargaste. "[Aplica la última corrección urgente](#)" para cada versión (altamente recomendado).

Consulta el siguiente ejemplo de actualización.

Ejemplo: actualización a StorageGRID 12.0 desde la versión 11.8

El siguiente ejemplo muestra los pasos para actualizar de StorageGRID versión 11.8 a la versión 11.9, como preparación para una actualización a StorageGRID 12.0.

Descarga e instala el software en el siguiente orden para preparar tu sistema para la actualización:

1. Actualiza a la versión principal StorageGRID 11.8.0.
2. Aplica la última corrección urgente de StorageGRID 11.8.0.y.
3. Actualiza a la versión principal StorageGRID 11.9.0.
4. Aplica la corrección urgente de StorageGRID 11.9.0.8 o posterior.

Obtén los materiales necesarios para una actualización de software de StorageGRID

Antes de iniciar la actualización del software, procura tener a mano todo el material necesario.

Artículo	Notas
Portátil de servicio	El portátil de servicio debe tener: • Puerto de red • Cliente SSH (por ejemplo, PuTTY)
"Navegador web compatible"	La compatibilidad con los navegadores suele variar en cada versión de StorageGRID. Asegúrate de que tu navegador sea compatible con la nueva versión de StorageGRID.
Contraseña de aprovisionamiento	La frase de contraseña se crea y se documenta durante la primera instalación del sistema StorageGRID. La frase de contraseña de aprovisionamiento no aparece en el <code>Passwords.txt</code> archivo.
Archivo RPM o DEB de Linux	Si hay algún nodo instalado en servidores Linux, debes "Descarga e instala el paquete RPM o DEB en todos los hosts" antes de iniciar la actualización. Asegúrate de que tu sistema operativo Linux cumpla los requisitos mínimos de versión del kernel de StorageGRID. Consulta "Instala StorageGRID en servidores Linux" .

Artículo	Notas
Documentación de StorageGRID	• "Notas de publicación". Debes iniciar sesión con tu cuenta de NetApp o crear una cuenta para acceder a las notas de la versión. Asegúrate de leerlas detenidamente antes de empezar la actualización. • "Guía de resolución para la actualización del software de StorageGRID" para la versión principal a la que vas a actualizar (es necesario iniciar sesión) • Otros "Documentación de StorageGRID", según sea necesario.

Revisa el estado de tu sistema StorageGRID antes de actualizar

Antes de actualizar un sistema StorageGRID, comprueba que el sistema esté preparado para la actualización. Asegúrate de que el sistema funcione con normalidad y de que todos los nodos de la red estén operativos.

Pasos

1. Inicia sesión en Grid Manager usando una ["navegador web compatible"](#) cuenta.
2. Comprueba si hay alertas activas y resuélvelas.
3. Consulta ["Comunicaciones internas entre nodos de grid"](#) y ["Comunicaciones externas"](#) para asegurarte de que todos los puertos necesarios para StorageGRID 12.0 estén abiertos antes de realizar la actualización.



No se necesitan puertos adicionales al actualizar a StorageGRID 12.0.

Actualizar software

Inicio rápido para las actualizaciones de StorageGRID

Antes de iniciar la actualización, revisa el flujo de trabajo general. La página de actualización de StorageGRID te guía a lo largo de cada paso de la actualización.

1

Prepara los hosts de Linux

Si hay algún nodo de StorageGRID implementado en hosts Linux, ["Instala el paquete RPM o DEB en cada host"](#) antes de iniciar la actualización.

2

Subir archivos de actualización y corrección urgente

Desde el nodo de administración principal, accede a la página de actualización de StorageGRID y sube el archivo de actualización y el archivo de corrección urgente, si es necesario.

3

Descargar el paquete de recuperación

Descarga el paquete de recuperación actual antes de iniciar la actualización.

4

Ejecuta las comprobaciones previas de la actualización

Las comprobaciones previas a la actualización te ayudan a detectar problemas, para que puedas resolverlos antes de iniciar la actualización propiamente dicha.

5

Iniciar actualización

Al iniciar la actualización, se vuelven a ejecutar las comprobaciones previas y el nodo de administración principal se actualiza automáticamente. No puedes acceder al Grid Manager mientras se actualiza el nodo de administración principal. Los registros de auditoría tampoco estarán disponibles. Esta actualización puede tardar hasta 30 minutos.

6

Descarga el paquete de recuperación

Después de que el nodo de administración principal haya sido actualizado, descarga un nuevo paquete de recuperación.

7

Aprobar nodos

Puedes aprobar nodos individuales de grid, grupos de nodos de grid o todos los nodos de grid.



No apruebes la actualización de un nodo de la red a menos que estés seguro de que dicho nodo está listo para ser detenido y reiniciado.

8

Reanudar operaciones

Una vez actualizados todos los nodos de la red, se activan las nuevas funciones y puedes reanudar las operaciones. Debes esperar a realizar un procedimiento para decomisionar o ampliar hasta que se hayan completado la tarea en segundo plano **Actualizar base de datos** y la tarea **Pasos finales de la actualización**.

Información relacionada

["Calcular el tiempo necesario para completar una actualización"](#)

Descarga e instala paquetes RPM o DEB en todos los hosts Linux para StorageGRID

Si hay algún nodo de StorageGRID implementado en hosts Linux, descarga e instala un paquete RPM o DEB adicional en cada uno de estos hosts antes de iniciar la actualización.

Descarga archivos de actualización, Linux y corrección urgente

Cuando realizas una actualización de StorageGRID desde Grid Manager, el primer paso es descargar el archivo de actualización y cualquier corrección urgente necesaria. Sin embargo, si necesitas descargar archivos para actualizar hosts Linux, puedes ahorrar tiempo descargando todos los archivos necesarios con antelación.

Pasos

1. Ve a "[Descargas de NetApp: StorageGRID](#)".
2. Selecciona el botón para descargar la última versión, o selecciona otra versión del menú desplegable y selecciona **Go**.

Las versiones del software StorageGRID tienen este formato: 11.x.y. Las correcciones urgentes de StorageGRID tienen este formato: 11.x.y.z.

3. Inicia sesión con el nombre de usuario y la contraseña de tu cuenta de NetApp.
4. Si aparece un aviso de precaución/MustRead, toma nota del número de la corrección urgente y selecciona la casilla de verificación.
5. Lee el Acuerdo de licencia de usuario final (EULA), marca la casilla de verificación y luego selecciona **Aceptar & Continuar**.

Aparece la página de descargas de la versión que seleccionaste. La página contiene tres columnas.

6. En la segunda columna (**Actualizar StorageGRID**), descarga dos archivos:
 - El archivo de actualización para la última versión (este es el archivo en la sección etiquetada como **VMware, SG1000 o SG100 Primary Admin Node**). Aunque no necesitarás este archivo hasta que realices la actualización, descargarlo ahora te ahorrará tiempo.
 - Un archivo RPM o DEB en formato .tgz o .zip. Selecciona el archivo .zip si estás ejecutando Windows en el portátil de servicio.
 - RHEL
`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 has tenido que aceptar un aviso de Caution/MustRead debido a la necesidad de instalar una corrección urgente, descarga la corrección urgente:
 - a. Vuelve a "[Descargas de NetApp: StorageGRID](#)".
 - b. Selecciona el número de corrección urgente en el menú desplegable.
 - c. Acepta de nuevo el aviso de advertencia y el EULA.
 - d. Descarga y guarda la corrección urgente y su README.

Cuando inicies la actualización, se te pedirá que subas el archivo de corrección urgente en la página de actualización de StorageGRID.
8. La verificación de la firma de código es manual en un nodo Linux. Opcionalmente, verifica el archivo de instalación:
 - a. Descarga el paquete de verificación de la firma del código de StorageGRID. El nombre del archivo de este paquete usa el formato `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz`, donde `<version-number>` es la versión del software StorageGRID.
 - b. Sigue los pasos para "[verificar manualmente los archivos de instalación](#)".

Instala el archivo en todos los servidores Linux

Sigue estos pasos antes de actualizar el software de StorageGRID.

Pasos

1. Extrae los paquetes RPM o DEB del archivo de instalación.
2. Instala los paquetes RPM o DEB en todos los hosts Linux.

Consulta los pasos para instalar los servicios de host de StorageGRID para Linux en "[Instala los servicios de host de StorageGRID](#)".

Los nuevos paquetes se instalan como paquetes adicionales.

Eliminar los archivos de instalación de las versiones anteriores

Para liberar espacio en los hosts Linux, puedes eliminar los archivos de instalación de las versiones anteriores de StorageGRID que ya no necesites.

Pasos

1. Elimina los archivos de instalación antiguos de StorageGRID.

RHEL

1. Obtén 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. Elimina los paquetes de StorageGRID anteriores: `dnf remove images-package service-package`



No elimines los archivos de instalación de la versión de StorageGRID que estás utilizando actualmente ni de las versiones de StorageGRID a las que tienes previsto actualizar.

Puedes ignorar sin problemas las advertencias que aparecen. Se refieren a archivos que se han reemplazado cuando instalas paquetes de StorageGRID más recientes.

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. Obtén 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. Elimina los paquetes anteriores de StorageGRID: `dpkg -r images-package service-package`



No elimines los archivos de instalación de la versión de StorageGRID que estás utilizando actualmente ni de las versiones de StorageGRID a las que tienes previsto 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 las imágenes de contenedores de StorageGRID.

Docker

1. Captura la lista de imágenes de contenedor 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. Elimina las imágenes de contenedor de las versiones anteriores de StorageGRID: `docker rmi image id`



No elimines las imágenes de los contenedores correspondientes a la versión de StorageGRID que estás utilizando actualmente ni a las versiones de StorageGRID a las que tienes previsto 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. Obtén la lista de imágenes de contenedores instaladas: `podman images`

Ejemplo:

```
[root@podman-example ~]# podman images
```

REPOSITORY SIZE	TAG	IMAGE ID	CREATED
localhost/storagegrid-11.8.0 ago 2.57 GB	Storage_Node	7125480de71b	7 months
localhost/storagegrid-11.8.0 ago 2.67 GB	Admin_Node	404e9f1bd173	7 months
localhost/storagegrid-11.8.0 ago 2.42 GB	Archive_Node	c3294a29697c	7 months
localhost/storagegrid-11.8.0 ago 1.77 GB	API_Gateway	1f88f24b9098	7 months
localhost/storagegrid-11.7.0 ago 2.54 GB	Storage_Node	1655350eff6f	16 months
localhost/storagegrid-11.7.0 ago 2.51 GB	Admin_Node	872258dd0dc8	16 months
localhost/storagegrid-11.7.0 ago 2.44 GB	Archive_Node	121e7c8b6d3b	16 months
localhost/storagegrid-11.7.0 ago 1.8 GB	API_Gateway	5b7a26e382de	16 months
localhost/storagegrid-11.6.0 ago 2.42 GB	Admin_Node	ee39f71a73e1	2 years
localhost/storagegrid-11.6.0 ago 2.11 GB	Storage_Node	f5ef895dcad0	2 years
localhost/storagegrid-11.6.0 ago 1.98 GB	Archive_Node	5782de552db0	2 years
localhost/storagegrid-11.6.0 ago 1.38 GB	API_Gateway	cb480ed37eea	2 years

```
[root@podman-example ~]#
```

2. Elimina las imágenes de contenedor de las versiones anteriores de StorageGRID: `podman rmi image id`



No elimines las imágenes de los contenedores correspondientes a la versión de StorageGRID que estás utilizando actualmente ni a las versiones de StorageGRID a las que tienes previsto actualizar.

Ejemplo:

```
[root@podman-example ~]# podman rmi f5ef895dcad0
Untagged: localhost/storagegrid-11.6.0:Storage_Node
Deleted:
f5ef895dcad0d78d0fd21a07dd132d7c7f65f45d80ee7205a4d615494e44cbb7
[root@podman-example ~]#
```


Realiza una actualización de StorageGRID

Puedes actualizar a StorageGRID 12.0 y aplicar la última corrección urgente para esa versión al mismo tiempo. La página de actualización de StorageGRID proporciona la ruta de actualización recomendada y ofrece enlaces directos a las páginas de descarga correctas.

Antes de empezar

Ya has revisado todos los aspectos a tener en cuenta y has completado todos los pasos de planificación y preparación.



No comiences la actualización si necesitas ampliar urgentemente tu almacenamiento para aumentar la capacidad (si tu almacenamiento está casi lleno). Completa el procedimiento de actualización a tiempo. Si se requiere una recuperación, contacta al soporte técnico.

Accede a la página de actualización de StorageGRID

Como primer paso, accede a la página de actualización de StorageGRID en Grid Manager.

Pasos

1. Inicia sesión en Grid Manager usando una ["navegador web compatible"](#) cuenta.
2. Selecciona **Mantenimiento > Sistema > Actualización de software**.
3. En el mosaico de actualización de StorageGRID, selecciona **Upgrade**.

Selecciona archivos

La ruta de actualización que aparece en la página «Actualización de StorageGRID» indica qué versiones principales (por ejemplo, 12.0.0) y correcciones urgentes (por ejemplo, 12.0.0.1) debes instalar para llegar a la última versión de StorageGRID. Debes instalar las versiones y correcciones urgentes recomendadas en el orden indicado.



Si no se muestra ninguna ruta de actualización, es posible que tu navegador no pueda acceder al sitio de soporte de NetApp, o que la casilla de verificación **Buscar actualizaciones de software** en la página de AutoSupport (**Soporte > Herramientas > AutoSupport > Configuración**) esté desactivada.

Pasos

1. En el paso **Seleccionar archivos**, revisa la ruta de actualización.
2. En la sección «Archivos de descarga», selecciona cada enlace **Descargar** para descargar los archivos necesarios desde el sitio de soporte de NetApp.

Si no se muestra ninguna ruta de actualización, ve a ["Descargas de NetApp: StorageGRID"](#) para determinar si hay disponible una nueva versión o corrección urgente y para descargar los archivos que necesitas.



Si tuvieras que descargar e instalar un paquete RPM o DEB en todos los hosts Linux, es posible que ya tengas los archivos de actualización y corrección urgente de StorageGRID que figuran en la ruta de actualización.

3. Selecciona **Examinar** para cargar el archivo de actualización de versión en StorageGRID:

NetApp_StorageGRID_12.0.0_Software_uniqueID.upgrade

Cuando se completa la subida y la verificación de la firma del código, aparece una marca de verificación verde junto al nombre del archivo.

4. Si descargaste un archivo de corrección urgente, selecciona **Examinar** para cargar ese archivo. La corrección urgente se aplicará automáticamente como parte de la actualización de versión.
5. Selecciona **Continuar**.

Ejecuta comprobaciones previas

La ejecución de comprobaciones previas te permite detectar y resolver cualquier problema de actualización antes de empezar a actualizar tu grid.

Pasos

1. En el paso **Ejecutar comprobaciones previas**, empieza introduciendo la frase de contraseña de aprovisionamiento de tu grid.
2. Selecciona **Descargar paquete de recuperación**.

Debes descargar la versión actual del archivo del paquete de recuperación antes de actualizar el nodo de administración principal. El archivo del paquete de recuperación te permite restaurar el sistema en caso de que se produzca un fallo.

3. Cuando se descargue el archivo, confirma que puedes acceder al contenido, incluido el archivo `Passwords.txt`.
4. Copia el archivo descargado (.zip) en dos ubicaciones seguras y distintas.



El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

5. Selecciona **Ejecutar comprobaciones previas** y espera a que finalicen las comprobaciones.
6. Revisa los detalles de cada comprobación previa notificada y resuelve los errores detectados. Consulta el ["Guía de resolución para la actualización del software de StorageGRID"](#) para la versión 12.0 de StorageGRID.

Debes resolver todos los *errores* de la comprobación previa antes de poder actualizar tu sistema. Sin embargo, no necesitas atender las *advertencias* de la comprobación previa antes de actualizar.



Si has abierto algún puerto personalizado del cortafuegos, se te notificará durante la validación previa. Debes ponerte en contacto con el soporte técnico antes de continuar con la actualización.

7. Si hiciste algún cambio en la configuración para resolver los problemas detectados, selecciona **Ejecutar comprobaciones previas** otra vez para obtener los resultados actualizados.

Si se han solucionado todos los errores, se te pedirá que inicies la actualización.

Inicia la actualización y actualiza el nodo de administración principal

Al iniciar la actualización, se vuelven a ejecutar las comprobaciones previas a la actualización y el nodo de administración principal se actualiza automáticamente. Esta parte de la actualización puede tardar hasta 30

minutos.



No podrás 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. Selecciona **Iniciar actualización**.

Aparece un aviso para recordarte que perderás temporalmente el acceso al Grid Manager.

2. Selecciona **OK** para confirmar la advertencia e iniciar la actualización.

3. Espera a que se realicen las comprobaciones previas a la actualización y a que se actualice el nodo de administración principal.



Si se detectan errores durante la comprobación previa, corrígelos y selecciona de nuevo **Start upgrade**.

Si la red cuenta con otro nodo de administración que esté conectado y listo, puedes utilizarlo para supervisar el estado del nodo de administración principal. En cuanto se actualice el nodo de administración principal, puedes aprobar los demás nodos de la red.

4. Como se requiere, selecciona **Continuar** para acceder al paso **Actualizar otros nodos**.

Actualizar otros nodos

Debes actualizar todos los nodos de la red, pero puedes realizar varias sesiones de actualización y personalizar el orden en que se llevan a cabo. Por ejemplo, quizá prefieras actualizar los nodos del sitio A en una sesión y luego actualizar los nodos del sitio B en una sesión posterior. Si decides realizar la actualización en más de una sesión, ten en cuenta que no podrás empezar a usar las nuevas funciones hasta que se hayan actualizado todos los nodos.

Si el orden en el que se actualizan los nodos es importante, aprueba los nodos o grupos de nodos de uno en uno y espera a que la actualización se complete en cada nodo antes de aprobar el siguiente nodo o grupo de nodos.



Cuando comienza la actualización en un nodo de grid, se detienen los servicios de ese nodo. Más tarde, el nodo de grid se reinicia. Para evitar interrupciones del servicio en las aplicaciones cliente que se comunican con el nodo, no apruebes la actualización de un nodo a menos que estés seguro de que está listo para detenerse y reiniciarse. Según sea necesario, programa una ventana de mantenimiento o notifica a los clientes.

Pasos

1. En el paso **Actualizar otros nodos**, revisa el resumen, que indica la hora de inicio de la actualización en su conjunto y el estado de cada tarea principal de la actualización.
 - **Start upgrade service** 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 finaliza la tarea **Iniciar el servicio de actualización**, se inicia la tarea **Actualizar otros nodos de la red** y se te pedirá que descargues una nueva copia del paquete de recuperación.
2. Cuando se te solicite, introduce tu contraseña de aprovisionamiento y descarga una nueva copia del paquete de recuperación.



Debes descargar una nueva copia del archivo del paquete de recuperación una vez actualizado el nodo de administración principal. El archivo del paquete de recuperación te permite restaurar el sistema en caso de que se produzca un fallo.

3. Revisa las tablas de estado de cada tipo de nodo. Hay tablas para los nodos de administración no primarios, los nodos de puerta de enlace y los nodos de almacenamiento.

Un nodo de la red puede encontrarse en una de estas fases cuando aparecen las tablas por primera vez:

- Desempaquetando la actualización
- Descargando
- A la espera de ser aprobado

4. [[paso de aprobación]] Cuando estés listo para seleccionar los nodos de grid que se van a actualizar (o si necesitas anular la aprobación de los nodos seleccionados), sigue estas instrucciones:



Para una actualización a StorageGRID 12.0, si quieres aprobar nodos individuales en lugar de todos los nodos, la mejor práctica es actualizar un sitio completo antes de pasar al siguiente sitio.

Tarea	Instrucción
Busca nodos específicos para aprobar, como todos los nodos de un sitio en particular	Introduce la cadena de búsqueda en el campo Buscar
Selecciona todos los nodos para la actualización	Selecciona Aprobar todos los nodos
Selecciona todos los nodos del mismo tipo para la actualización (por ejemplo, todos los Storage Nodes)	Selecciona el botón Aprobar todo para el tipo de nodo Si apruebas más de un nodo del mismo tipo, los nodos se actualizarán de uno en uno.
Selecciona un nodo concreto para actualizarlo	Selecciona el botón Aprobar para el nodo
Aplaza la actualización en todos los nodos seleccionados	Selecciona Desaprobar todos los nodos
Aplaza la actualización en todos los nodos seleccionados del mismo tipo	Selecciona el botón Desaprobar todo para el tipo de nodo
Aplaza la actualización en un nodo concreto	Selecciona el botón Rechazar para el nodo

5. Espera a que los nodos aprobados pasen por estas fases de actualización:
 - Aprobado y a la espera de ser actualizado
 - Detener servicios



No puedes eliminar un nodo cuando su etapa llega a **Parada de servicios**. El botón **Rechazar** está desactivado.

- Deteniendo contenedor
- Limpieza de imágenes de Docker
- Actualización de los paquetes base del sistema operativo



Cuando un nodo del dispositivo llega a esta etapa, el software StorageGRID Appliance Installer del dispositivo se actualiza. Este proceso automatizado garantiza que la versión de StorageGRID Appliance Installer se mantenga sincronizada con la versión del software StorageGRID.

- Reinicio



Es posible que algunos modelos de appliance se reinicien varias veces para actualizar el firmware y la BIOS.

- Pasos a seguir tras el reinicio
- Iniciando servicios
- Hecho

6. Repite el [fase de aprobación](#) tantas veces como sea necesario hasta que hayas actualizado todos los nodos de grid.

Actualización completa

Cuando todos los nodos de la grid hayan completado las etapas de actualización, la tarea **Upgrade other grid nodes** se muestra como Completada. Las tareas de actualización restantes se realizan automáticamente en segundo plano.

Pasos

1. En cuanto se complete la tarea **Habilitar funciones** (lo cual ocurre rápidamente), puedes empezar a usar el ["nuevas funciones"](#) en la versión actualizada de StorageGRID.
2. Comienza la actualización de la base de datos Cassandra. Esta actualización se llevará a cabo en segundo plano durante uno a tres días, y el servicio Cassandra se detendrá y se reiniciará en cada Storage Node. Durante este tiempo, se desactivarán ciertos procedimientos de mantenimiento que involucren la transmisión de metadatos, como la expansión.
3. Cuando se hayan completado los **pasos finales de la actualización**, la actualización está lista. El primer paso, **Seleccionar archivos**, vuelve a mostrarse con un banner verde de éxito.
4. Comprueba que las operaciones del grid hayan vuelto a la normalidad:
 - a. Comprueba que los servicios funcionen con normalidad y que no haya alertas inesperadas.
 - b. Comprueba que las conexiones de los clientes al sistema StorageGRID funcionan como esperas.

Información relacionada

["Cómo se ve afectado tu sistema durante la actualización"](#)

Soluciona problemas de actualización de StorageGRID

Si surge algún problema al realizar una actualización, es posible que puedas resolverlo por tu cuenta. Si no consigues resolver el problema, recopila toda la información que puedas y luego ponte en contacto con soporte técnico.

La actualización no se completa

Las siguientes secciones describen cómo recuperar situaciones en las que la actualización ha fallado parcialmente.

Errores de comprobación previa de la actualización

Para detectar y resolver problemas, puedes ejecutar manualmente las comprobaciones previas de la actualización antes de iniciar la actualización real. La mayoría de los errores de las comprobaciones previas proporcionan información sobre cómo resolver el problema.

Errores de aprovisionamiento

Si falla el proceso de aprovisionamiento automático, ponte en contacto con el soporte técnico.

El nodo de grid se bloquea o no se inicia

Si un nodo de la red se bloquea durante el proceso de actualización o no se inicia correctamente una vez finalizada la actualización, ponte en contacto con el soporte técnico para que investiguen y solucionen cualquier problema subyacente.

Se interrumpe la ingesta o la recuperación de datos

Si la importación o la recuperación de datos se interrumpe de forma inesperada cuando no estés actualizando un nodo de la grid, ponte en contacto con soporte técnico.

Errores en la actualización de la base de datos

Si la actualización de la base de datos falla y se produce un error, vuelve a intentar la actualización. Si vuelve a fallar, ponte en contacto con soporte técnico.

Información relacionada

["Comprobación del estado del sistema antes de actualizar el software"](#)

Problemas con la interfaz de usuario

Es posible que experimentes problemas con el Grid Manager o el Tenant Manager durante o después de la actualización.

Grid Manager muestra varios mensajes de error durante la actualización

Si actualizas el navegador o accedes a otra página de Grid Manager mientras se está actualizando el nodo de administración principal, es posible que veas varios mensajes del tipo "503: Service Unavailable" y "Problem connecting to the server". Puedes ignorar estos mensajes sin problema; dejarán de aparecer en cuanto se haya actualizado el nodo.

Si estos mensajes siguen apareciendo más de una hora después de haber iniciado la actualización, es posible que haya ocurrido algo que haya impedido la actualización del nodo de administración principal. Si no

consigues resolver el problema por tu cuenta, ponte en contacto con soporte técnico.

La interfaz web no responde como se esperaba

Es posible que Grid Manager o Tenant Manager no respondan como se espera después de actualizar el software de StorageGRID.

Si tienes algún problema con la interfaz web:

- Asegúrate de que estás utilizando un ["navegador web compatible"](#).



La compatibilidad con los navegadores suele variar en cada versión de StorageGRID.

- Borra la caché de tu navegador web.

Al vaciar la caché se eliminan los recursos obsoletos utilizados por la versión anterior del software StorageGRID, y permite que la interfaz de usuario vuelva a funcionar correctamente. Para obtener instrucciones, consulta la documentación de tu navegador web.

Mensajes de error de «Comprobación de disponibilidad de la imagen de Docker»

Al intentar iniciar el proceso de actualización, es posible que recibas un mensaje de error que dice: "La suite de validación de la comprobación de disponibilidad de la imagen de Docker ha detectado los siguientes problemas". Debes resolver todos los problemas antes de poder completar la actualización.

Ponte en contacto con el soporte técnico si no estás seguro de los cambios necesarios para resolver los problemas detectados.

Mensaje	Causa	Solución
No se ha podido determinar la versión de actualización. El archivo de información de la versión de actualización {file_path} no coincidía con el formato esperado.	El paquete de actualización está dañado.	Vuelve a cargar el paquete de actualización e inténtalo de nuevo. Si el problema persiste, ponte en contacto con el soporte técnico.
No se encontró el archivo de información de la versión de actualización {file_path}. No se puede determinar la versión de actualización.	El paquete de actualización está dañado.	Vuelve a cargar el paquete de actualización e inténtalo de nuevo. Si el problema persiste, ponte en contacto con el soporte técnico.
No se puede determinar la versión instalada actualmente en {node_name}.	Un archivo esencial del nodo está dañado.	Ponte en contacto con el soporte técnico.
Error de conexión al intentar listar las versiones en {node_name}	El nodo está desconectado o se ha interrumpido la conexión.	Comprueba que todos los nodos estén en línea y sean accesibles desde el nodo de administración principal, y vuelve a intentarlo.

Mensaje	Causa	Solución
El host del nodo {node_name} no tiene cargada la imagen de StorageGRID {upgrade_version}. Las imágenes y los servicios deben instalarse en el host antes de que puedas continuar con la actualización.	Los paquetes RPM o DEB para la actualización no se han instalado en el host donde se está ejecutando el nodo, o las imágenes todavía están en proceso de importación. Nota: Este error solo aplica a los nodos que se ejecutan como contenedores en Linux.	Comprueba que los paquetes RPM o DEB se hayan instalado en todos los hosts Linux en los que se están ejecutando los nodos. Asegúrate de que la versión sea la correcta tanto para el servicio como para el archivo de imágenes. Espera unos minutos e inténtalo de nuevo. Consulta "Linux: Instala un paquete RPM o DEB en todos los hosts" .
Error al comprobar el nodo {node_name}	Se ha producido un error inesperado.	Espera unos minutos y vuelve a intentarlo.
Error no controlado al ejecutar las comprobaciones previas. {error_string}	Se ha producido un error inesperado.	Espera unos minutos y vuelve a intentarlo.

Aplicar la corrección urgente de StorageGRID

Procedimiento de corrección urgente de StorageGRID

Es posible que tengas que aplicar una corrección urgente a tu sistema StorageGRID si se detectan y resuelven problemas con el software entre lanzamientos de funciones.

Las correcciones urgentes de StorageGRID contienen cambios de software que se ponen a disposición fuera de una versión de nuevas funciones o de parches. Los mismos cambios se incluyen en una versión futura. Además, cada versión de corrección urgente contiene un paquete acumulativo de todas las correcciones urgentes anteriores dentro de la versión de nuevas funciones o de parches.

Aspectos a tener en cuenta a la hora de aplicar una corrección urgente

No puedes aplicar una corrección urgente de StorageGRID mientras se está ejecutando otro procedimiento de mantenimiento. Por ejemplo, no puedes aplicar una corrección urgente mientras se está ejecutando un procedimiento de decomisionar, expansión o recuperación.



Si se ha pausado el procedimiento de decomisionar un nodo o una ubicación, puedes aplicar una corrección urgente de forma segura. Además, podrías aplicar una corrección urgente durante las etapas finales de un procedimiento de actualización de StorageGRID. Consulta las instrucciones para actualizar el software de StorageGRID para más detalles.

Una vez que hayas cargado la corrección urgente en el Grid Manager, la corrección urgente se aplica automáticamente al nodo de administración principal. Luego, puedes aprobar la aplicación de la corrección urgente al resto de los nodos de tu sistema StorageGRID.

Si no se consigue aplicar una corrección urgente a uno o varios nodos, el motivo del error aparece en la columna Detalles de la tabla de progreso de la corrección urgente. Debes resolver los problemas que hayan provocado los errores y luego volver a intentar todo el proceso. Los nodos en los que la aplicación de la

corrección urgente se haya realizado correctamente antes se omitirán en aplicaciones posteriores. Puedes volver a intentar el proceso de la corrección urgente tantas veces como sea necesario hasta que todos los nodos se hayan actualizado. La corrección urgente debe instalarse correctamente en todos los nodos de la grid para que la aplicación se considere completa.

Aunque los nodos de la red se actualizan con la nueva versión de la corrección urgente, es posible que los cambios reales de una corrección urgente solo afecten a servicios concretos en tipos específicos de nodos. Por ejemplo, una corrección urgente podría afectar únicamente al servicio LDR en los Storage Nodes.

Cómo se aplican las correcciones urgentes para la recuperación y la ampliación

Una vez que se ha aplicado una corrección urgente a tu grid, el nodo de administración principal instala automáticamente la misma versión de la corrección urgente en cualquier nodo restaurado mediante operaciones de recuperación o añadido en una ampliación.

Sin embargo, si necesitas recuperar el nodo de administración principal, debes instalar manualmente la versión correcta de StorageGRID y luego aplicar la corrección urgente. La versión final de StorageGRID del nodo de administración principal debe coincidir con la versión de los demás nodos de la grid.

El siguiente ejemplo ilustra cómo aplicar una corrección urgente al recuperar el nodo de administración principal:

1. Supongamos que la red ejecuta una versión de StorageGRID 11.A.B con la última corrección urgente. La «versión de la red» es 11.A.B.y.
2. El nodo de administración principal falla.
3. Vuelves a implementar el nodo de administración principal utilizando StorageGRID 11.A.B y realizas el procedimiento de recuperación.



Tal y como se requiere para que coincida con la versión de la grid, puedes utilizar una versión secundaria al implementar el nodo; no necesitas implementar primero la versión principal.

4. A continuación, aplicas la corrección urgente 11.A.B.y al nodo de administración principal.

Para más información, consulta ["Configura el nodo de administración principal de sustitución"](#).

Cómo se ve afectado StorageGRID cuando aplicas una corrección urgente

Debes comprender cómo se verá afectado tu sistema StorageGRID al aplicar una corrección urgente.

Las correcciones urgentes de StorageGRID no provocan interrupciones

El sistema StorageGRID puede recibir y recuperar datos de las aplicaciones cliente durante todo el proceso de aplicación de la corrección urgente. Si autorizas la aplicación de la corrección urgente en todos los nodos de un mismo tipo (por ejemplo, Storage Nodes), los nodos se desconectan de uno en uno, por lo que en ningún momento todos los nodos de la grid ni todos los nodos de un tipo concreto quedan indisponibles.

Para garantizar la disponibilidad continua, asegúrate de que tu política de ILM incluya reglas que especifiquen el almacenamiento de varias copias de cada objeto. También debes asegurarte de que todos los clientes externos de S3 estén configurados para enviar solicitudes a uno de los siguientes:

- Una dirección IP virtual de un grupo de alta disponibilidad (HA)

- Un equilibrador de carga de terceros de alta disponibilidad
- Varios nodos de puerta de enlace para cada cliente
- Varios nodos de almacenamiento para cada cliente

Las aplicaciones de los clientes podrían experimentar interrupciones de corta duración

El sistema StorageGRID puede recibir y recuperar datos de las aplicaciones cliente durante todo el proceso de corrección urgente; sin embargo, las conexiones de los clientes a nodos Gateway o nodos de almacenamiento concretos podrían verse interrumpidas temporalmente si la corrección urgente requiere reiniciar los servicios en esos nodos. La conectividad se restablecerá una vez que finalice el proceso de corrección urgente y se reanuden los servicios en los nodos concretos.

Es posible que tengas que programar un tiempo de inactividad para aplicar una corrección urgente si no es aceptable que se produzca una pérdida de conectividad durante un breve periodo de tiempo. Puedes utilizar la aprobación selectiva para programar cuándo se actualizan determinados nodos.



Puedes usar varias puertas de enlace y grupos de alta disponibilidad (HA) para proporcionar conmutación automática por error durante el proceso de corrección urgente. Consulta 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 funciona en un entorno de versiones mixtas (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 corrección urgente.

Los cambios en la configuración están restringidos

Al aplicar una corrección urgente a StorageGRID:

- No realices ningún cambio en la configuración de grid (por ejemplo, especificar subredes de Grid Network o aprobar nodos de grid pendientes) hasta que se haya aplicado la corrección urgente a todos los nodos.
- No actualices la configuración de ILM hasta que se haya aplicado la corrección urgente a todos los nodos.

Obtén los materiales necesarios para una corrección urgente de StorageGRID

Antes de aplicar una corrección urgente, debes conseguir todo el material necesario.

Artículo	Notas
Archivo de corrección urgente de StorageGRID	Debes descargar el archivo de corrección urgente de StorageGRID.
• Puerto de red • "Navegador web compatible" • Cliente SSH (por ejemplo, PuTTY)	

Artículo	Notas
paquete de recuperación (.zip) archivo	Antes de aplicar una corrección urgente, " Descarga el archivo del paquete de recuperación más reciente " por si ocurre algún problema durante la corrección urgente. Luego, después de aplicar la corrección urgente, descarga una nueva copia del archivo del paquete de recuperación y guárdala en un lugar seguro. El archivo actualizado del paquete de recuperación te permite restaurar el sistema si ocurre un fallo.
Archivo Passwords.txt	Opcional y solo se utiliza si aplicas una corrección urgente de forma manual usando el cliente SSH. El archivo Passwords.txt es parte del paquete de recuperación .zip.
Contraseña de aprovisionamiento	La frase de contraseña se crea y se documenta durante la primera instalación del sistema StorageGRID. La frase de contraseña de aprovisionamiento no aparece en el Passwords.txt archivo.
Documentación relacionada	readme.txt archivo de la corrección urgente. Este archivo se incluye en la página de descarga de la corrección urgente. Asegúrate de revisar el readme archivo cuidadosamente antes de aplicar la corrección urgente.

Descarga un archivo de corrección urgente de StorageGRID

Debes descargar el archivo de la corrección urgente antes de poder aplicarla.

Pasos

1. Ve a "[Descargas de NetApp: StorageGRID](#)".
2. Selecciona la flecha hacia abajo que aparece debajo de **Software disponible** para ver una lista de las correcciones urgentes disponibles para descargar.



Las versiones de los archivos de corrección urgente tienen el siguiente formato: 11.4.x.y.

3. Consulta los cambios que incluye la actualización.



Si acabas de "[se recuperó el nodo de administración principal](#)" y necesitas aplicar una corrección urgente, selecciona la misma versión de corrección urgente que está instalada en los otros nodos del grid.

- a. Selecciona la versión de la corrección urgente que quieras descargar y haz clic en **Ir**.
- b. Inicia sesión usando el nombre de usuario y la contraseña de tu cuenta de NetApp.
- c. Lee y acepta el Acuerdo de licencia de usuario final.

Aparece la página de descarga de la versión que seleccionaste.

- d. Descarga el archivo de la corrección urgente `readme.txt` para ver un resumen de los cambios incluidos en la corrección urgente.

4. Selecciona el botón de descarga de la corrección urgente y guarda el archivo.



No cambies el nombre de este archivo.



Si utilizas un dispositivo macOS, es posible que el archivo de corrección urgente se guarde automáticamente como un archivo `.txt`. Si es así, debes cambiar el nombre del archivo y quitar la extensión `.txt`.

5. Elige una ubicación para la descarga y selecciona **Guardar**.

Comprueba el estado del sistema antes de aplicar una corrección urgente de StorageGRID

Debes comprobar que el sistema está listo para instalar la corrección urgente.

1. Inicia sesión en Grid Manager usando una ["navegador web compatible"](#) cuenta.
2. Si es posible, asegúrate de que el sistema funcione con normalidad y de que todos los nodos de la red estén conectados a la red.

Los nodos conectados tienen marcas de verificación verdes  en la página de Nodos.

3. Comprueba si hay alguna alerta activa y, si es posible, resuélvela.
4. Asegúrate de que no haya ningún otro procedimiento de mantenimiento en curso, como una actualización, recuperación, ampliación o procedimiento de decomisionar.

Debes esperar a que finalicen los procedimientos de mantenimiento en curso antes de aplicar una corrección urgente.

No puedes aplicar una corrección urgente de StorageGRID mientras se está ejecutando otro procedimiento de mantenimiento. Por ejemplo, no puedes aplicar una corrección urgente mientras se está ejecutando un procedimiento de decomisionar, expansión o recuperación.



Si un nodo o un sitio ["El procedimiento de decomisionar está en pausa"](#), puedes aplicar una corrección urgente de forma segura. Además, podrías aplicar una corrección urgente durante las etapas finales de un procedimiento de actualización de StorageGRID. Consulta las instrucciones para ["Actualización del software StorageGRID"](#).

Aplica una corrección urgente en StorageGRID

La corrección urgente se aplica primero de forma automática al nodo de administración principal. Luego, debes aprobar la aplicación de la corrección urgente a otros nodos de grid hasta que todos los nodos estén ejecutando la misma versión del software. Puedes personalizar la secuencia de aprobación seleccionando aprobar nodos individuales de grid, grupos de nodos de grid o todos los nodos de grid.

Antes de empezar

- Has revisado la ["consideraciones para aplicar una corrección urgente"](#).
- Tienes la frase de contraseña de aprovisionamiento.

- Tienes acceso Root o el permiso de mantenimiento.

Acerca de esta tarea

- Puedes retrasar la aplicación de una corrección urgente a un nodo, pero el proceso de corrección urgente no se completa hasta que aplicas la corrección urgente a todos los nodos.
- No puedes realizar una actualización del software de StorageGRID ni una actualización del sistema operativo de SANtricity hasta que hayas completado el proceso de corrección urgente.

Pasos

1. Inicia sesión en Grid Manager usando una "[navegador web compatible](#)" cuenta.
2. Selecciona **Mantenimiento > Sistema > Actualización de software**.

Aparece la página «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. Selecciona **Aplicar corrección urgente**.

Aparece la página de corrección urgente 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. Selecciona el archivo de corrección urgente que descargaste del sitio de soporte de NetApp.

- a. Selecciona **Examinar**.
- b. Busca y selecciona el archivo.

`hotfix-install-version`

- c. Selecciona **Open**.

El archivo se ha subido. Cuando finaliza la subida, el nombre del archivo aparece en el campo Detalles.



No cambies el nombre del archivo porque es parte del proceso de verificación.

5. Introduce la frase de contraseña de aprovisionamiento en el cuadro de texto.

El botón **Inicio** queda activado.

6. Selecciona **Inicio**.

Aparece un aviso en el que se indica que la conexión de tu navegador podría perderse temporalmente mientras se reinician los servicios en el nodo de administración principal.

7. Selecciona **Aceptar** para comenzar a aplicar la corrección urgente al nodo de administración principal.

Cuando se inicia la corrección urgente:

- a. Se ejecutan las validaciones de la corrección urgente, incluida la verificación de la firma del código.



Si se detecta algún error, corrígelo, vuelve a cargar el archivo de corrección urgente y selecciona **Iniciar** de nuevo.

- b. Aparece la tabla de progreso de la instalación de la corrección urgente.

Esta tabla muestra todos los nodos de tu grid y la fase actual de la instalación de la corrección urgente para cada nodo. Los nodos de la tabla están agrupados por tipo (Admin Nodes, Gateway Nodes y Storage Nodes).

- c. La barra de progreso llega al final y luego el nodo de administración principal aparece como "Complete".

Hotfix Installation Progress

Approve All Remove All

Admin Nodes - 1 out of 1 completed

Site	Name	Progress	Stage	Details	Action
Vancouver	VTC-ADM1-101-191		Complete		

8. Si lo deseas, ordena las listas de nodos de cada grupo en orden ascendente o descendente por **Sitio**, **Nombre**, **Progreso**, **Fase** o **Detalles**. O introduce un término en el cuadro **Buscar** para buscar nodos específicos.
9. Aprueba los nodos de la red que están listos para ser actualizados. Los nodos aprobados del mismo tipo se actualizan de uno en uno.



No apruebes la corrección urgente para un nodo a menos que estés seguro de que el nodo está listo para ser actualizado. Cuando se aplica la corrección urgente a un nodo de la red, algunos servicios de ese nodo podrían reiniciarse. Estas operaciones pueden causar interrupciones en el servicio para los clientes que se están comunicando con el nodo.

- Selecciona uno o varios botones **Aprobar** para añadir uno o varios nodos individuales a la cola de corrección urgente.
- Selecciona el botón **Aprobar todo** dentro de cada grupo para añadir todos los nodos del mismo tipo a la cola de corrección urgente. Si has introducido criterios de búsqueda en el cuadro **Buscar**, el botón **Aprobar todo** se aplica a todos los nodos seleccionados por los criterios de búsqueda.



El botón **Aprobar todo** situado en la parte superior de la página aprueba todos los nodos que aparecen en ella, mientras que el botón **Aprobar todo** situado en la parte superior de una agrupación de tablas solo aprueba todos los nodos de ese grupo. Si el orden en el que se actualizan los nodos es importante, aprueba los nodos o grupos de nodos de uno en uno y espera a que se complete la actualización en cada nodo antes de aprobar el siguiente o los siguientes.

- Selecciona el botón de primer nivel **Aprobar todo** en la parte superior de la página para añadir todos los nodos de la cuadrícula a la cola de corrección urgente.



Debes completar la corrección urgente de StorageGRID antes de poder iniciar una actualización de software diferente. Si no puedes completar la corrección urgente, ponte en contacto con soporte técnico.

- Selecciona **Eliminar** o **Eliminar todo** para eliminar un nodo o todos los nodos de la cola de corrección urgente.

Cuando la fase pasa del estado «En cola», el botón **Eliminar** se oculta y ya no puedes eliminar el nodo del proceso de corrección urgente.

Storage Nodes - 1 out of 9 completed
Approve All Remove All

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

- Espera mientras se aplica la corrección urgente a cada nodo de grid aprobado.

Cuando la corrección urgente se haya instalado correctamente en todos los nodos, la tabla de progreso de la instalación de la corrección urgente se cerrará. Una barra verde muestra la fecha y la hora en que se completó la corrección urgente.

- Si no se pudo aplicar la corrección urgente a ningún nodo, revisa el error de cada nodo, resuelve el problema y repite estos pasos.

El procedimiento no se completa hasta que la corrección urgente se aplica correctamente en todos los nodos. Puedes volver a intentar el proceso de corrección urgente tantas veces como sea necesario hasta que se complete, sin ningún riesgo.

Configurar y gestionar un sistema StorageGRID

Administrar StorageGRID

Administrar StorageGRID

Sigue estas instrucciones para configurar y administrar un sistema StorageGRID.

Acerca de estas instrucciones

Las tareas principales para configurar y administrar StorageGRID te permiten:

- Utiliza el Grid Manager para configurar grupos y usuarios
- Crea cuentas de inquilino para permitir que las aplicaciones cliente de S3 almacenen y recuperen objetos
- Configura y gestiona redes StorageGRID
- Configura AutoSupport
- Gestiona la configuración del nodo

Antes de empezar

- Tienes un conocimiento general del sistema StorageGRID.
- Tienes conocimientos bastante detallados sobre los shells de comandos de Linux, redes y la configuración e instalación del hardware de servidores.

Empieza a utilizar Grid Manager

Requisitos del navegador web para StorageGRID

Debes utilizar un navegador web compatible.

Navegador web	Versión mínima compatible
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

Ajusta el ancho de la ventana del navegador al recomendado.

Ancho del navegador	Píxeles
Mínimo	1024
Óptimo	1280

Inicia sesión en StorageGRID Grid Manager

Accedes a la página de inicio de sesión de Grid Manager introduciendo 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 número de nodos de administración no principales. Puedes iniciar sesión en el Grid Manager en cualquier nodo de administración para gestionar el sistema StorageGRID. Sin embargo, algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración principal.

Conéctate al grupo de alta disponibilidad

Si los nodos de administración están incluidos en un grupo de alta disponibilidad (HA), te conectas usando la dirección IP virtual del grupo HA o un nombre de dominio completo que apunte a la dirección IP virtual. El nodo de administración principal debe seleccionarse como la interfaz principal del grupo, así que cuando accedas a Grid Manager, lo harás en el nodo de administración principal a menos que este no esté disponible. Consulta ["Gestiona grupos de alta disponibilidad"](#).

Usa el inicio de sesión único (SSO)

Los pasos para iniciar sesión son un poco diferentes si ["El inicio de sesión único \(SSO\) ha sido configurado"](#).

Inicia sesión en Grid Manager en el primer nodo de administración

Antes de empezar

- Ya tienes tus datos de acceso.
- Estás usando un ["navegador web compatible"](#).
- Las cookies están activadas en tu navegador web.
- Perteneces a un grupo de usuarios que tiene al menos un permiso.
- Ya tienes la URL del Grid Manager:

```
https://FQDN_or_Admin_Node_IP/
```

Puedes utilizar el nombre de dominio completo, la dirección IP de un nodo de administración o la dirección IP virtual de un grupo de HA de nodos de administración.

Para acceder al Grid Manager en un puerto distinto al puerto predeterminado para HTTPS (443), incluye el número de puerto en la URL:

```
https://FQDN_or_Admin_Node_IP:port/
```



El SSO no está disponible en el puerto restringido de Grid Manager. Debes utilizar el puerto 443.

Pasos

1. Abre un navegador web compatible.
2. En la barra de direcciones del navegador, introduce la URL del Grid Manager.
3. Si te aparece una alerta de seguridad, instala el certificado utilizando el asistente de instalación del navegador. Consulta ["Gestiona certificados de seguridad"](#).

4. Inicia sesión en Grid Manager.

La pantalla de inicio de sesión que aparece depende de si se ha configurado el inicio de sesión único (SSO) para StorageGRID.

No usas SSO

- a. Introduce tu nombre de usuario y contraseña para el Grid Manager.
- b. Selecciona **Sign In**.

Uso de SSO

- Si StorageGRID utiliza el inicio de sesión único (SSO) y es la primera vez que accedes a la URL desde este navegador:
 - i. Selecciona **Iniciar sesión**. Puedes dejar el 0 en el campo Cuenta.
 - ii. Introduce tus credenciales habituales de SSO en la página de inicio de sesión único de tu organización.

Por ejemplo, si StorageGRID utiliza el inicio de sesión único (SSO) y ya has accedido anteriormente al Grid Manager o a una cuenta de inquilino:

- A. Introduce **0** (el ID de la cuenta de Grid Manager) o selecciona **Grid Manager** si aparece en la lista de cuentas recientes.
- B. Selecciona **Sign in**.
- C. Inicia sesión con tus credenciales estándar de SSO en la página de inicio de sesión único de tu organización.

Cuando hayas iniciado sesión, aparecerá la página de inicio de Grid Manager, que incluye el panel de control. Para saber qué información se ofrece, consulta "[Ver y gestionar el panel de control](#)".

Inicia sesión en otro nodo de administración

Sigue estos pasos para iniciar sesión en otro nodo de administración.

No usas SSO

Pasos

1. En la barra de direcciones del navegador, introduce el nombre de dominio completo o la dirección IP del otro Admin Node. Incluye el número de puerto si es necesario.
2. Introduce tu nombre de usuario y contraseña para el Grid Manager.
3. Selecciona **Sign In**.

Uso de SSO

Si StorageGRID utiliza SSO y has iniciado sesión en un nodo de administración, puedes acceder a otros nodos de administración sin tener que volver a iniciar sesión.

Pasos

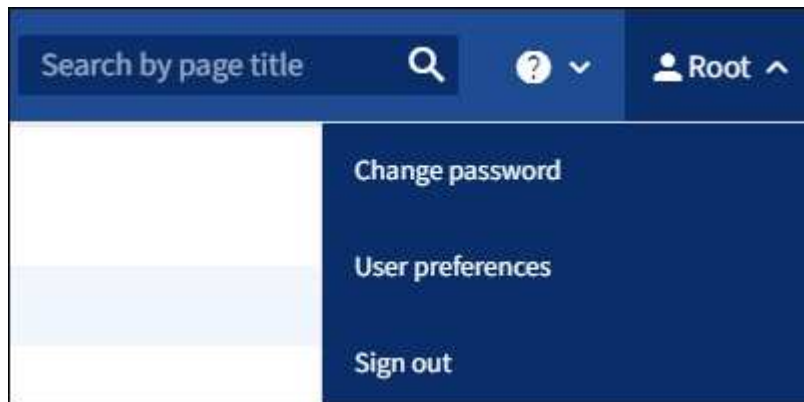
1. Introduce el nombre de dominio completo o la dirección IP del otro nodo de administración en la barra de direcciones del navegador.
2. Si tu sesión de SSO ha caducado, vuelve a introducir tus credenciales.

Sign out de StorageGRID Grid Manager

Cuando hayas terminado de trabajar con Grid Manager, debes cerrar la sesión para garantizar que los usuarios no autorizados no puedan acceder al sistema StorageGRID. Cerrar el navegador podría no cerrar tu sesión en el sistema, según la configuración de las cookies del navegador.

Pasos

1. Selecciona tu nombre de usuario en la esquina superior derecha.



2. Selecciona **Cerrar sesión**.

Opción	Descripción
SSO no está en uso	Has cerrado sesión en el nodo de administración. Se muestra la página de inicio de sesión de Grid Manager. Nota: Si has iniciado sesión en más de un nodo de administración, debes cerrar la sesión en cada uno.

Opción	Descripción
SSO activado	Se ha cerrado la sesión en todos los nodos de administración a los que tenías acceso. Se muestra la página de inicio de sesión de StorageGRID. Grid Manager aparece como opción predeterminada en el menú desplegable Cuentas recientes, y el campo ID de cuenta muestra 0. Nota: Si el inicio de sesión único (SSO) está activado y además has iniciado sesión en Tenant Manager, también debes "cerrar sesión en la cuenta de inquilino" a "cerrar sesión de SSO".

Cambia tu contraseña de StorageGRID Grid Manager

Si eres un usuario local de Grid Manager, puedes cambiar tu propia contraseña.

Antes de empezar

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

Acerca de esta tarea

Si te logueas en StorageGRID como usuario federado o si el inicio de sesión único (SSO) está habilitado, no puedes cambiar tu contraseña en Grid Manager. En su lugar, debes cambiar tu contraseña en la fuente de identidad externa, por ejemplo, Active Directory u OpenLDAP.

Pasos

1. En la barra de menú de Grid Manager, selecciona **tu nombre** > **Cambiar contraseña**.
2. Introduce tu contraseña actual.
3. Escribe una nueva contraseña.

Tu contraseña debe tener al menos 8 y no más de 32 caracteres. Las contraseñas distinguen entre mayúsculas y minúsculas.

4. Vuelve a introducir la nueva contraseña.
5. Selecciona **Guardar**.

Ver la información de la licencia de StorageGRID

Puedes ver la información de la licencia de tu sistema StorageGRID, como la capacidad de almacenamiento máxima de tu grid, cuando lo necesites.

Antes de empezar

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

Acerca de esta tarea

Si hay algún problema con la licencia de software de este sistema StorageGRID, la tarjeta de estado de salud en el panel incluye un icono de estado de licencia y un enlace **Licencia**. El número indica la cantidad de problemas relacionados con la licencia.



Pasos

1. Accede a la página «Licencia» haciendo una de las siguientes acciones:

- Selecciona **Mantenimiento > Sistema > Licencia**.
- En la tarjeta Estado de salud del panel de control, selecciona el icono de estado de la licencia o el enlace **License**.

Este enlace solo aparece si hay algún problema con la licencia.

2. Consulta los detalles de solo lectura de la licencia actual:

- ID del sistema StorageGRID, que es el número de identificación único de esta instalación de StorageGRID
- Número de serie de la licencia
- Tipo de licencia, ya sea **Perpetua** o **Por suscripción**
- Capacidad de almacenamiento autorizada de la grid
- Capacidad de almacenamiento compatible
- Fecha de vencimiento de la licencia. **N/A** aparece para una licencia perpetua.
- Fecha de finalización del soporte

Esta fecha se lee desde el archivo de licencia actual y podría estar desactualizada si ampliaste o renovaste el contrato de servicio de soporte después de obtener el archivo de licencia. Para actualizar este valor, consulta "[Actualizar la información de la licencia de StorageGRID](#)". También puedes ver la fecha de finalización real del contrato usando Active IQ.

- Contenido del archivo de texto de la licencia

Actualizar la información de la licencia de StorageGRID

Debes actualizar la información de la licencia de tu sistema StorageGRID cada vez que cambien las condiciones de tu licencia. Por ejemplo, debes actualizar la información de la licencia si adquieres capacidad de almacenamiento adicional para tu grid.

Antes de empezar

- Tienes un nuevo archivo de licencia que debes aplicar a tu sistema StorageGRID.

- Tienes ["permisos de acceso específicos"](#).
- Tienes la frase de contraseña de aprovisionamiento.

Pasos

1. Selecciona **Mantenimiento > Sistema > Licencia**.
2. En la sección Actualizar licencia, selecciona **Examinar**.
3. Busca y selecciona el nuevo archivo de licencia (.txt).

El nuevo archivo de licencia se valida y se muestra.

4. Introduce la contraseña de aprovisionamiento.
5. Selecciona **Guardar**.

Usa la API

Usa la API de gestión de StorageGRID Grid

Puedes realizar tareas de administración de sistemas mediante la API de REST de Grid Management en lugar de la interfaz de usuario de Grid Manager. Por ejemplo, es posible que quieras utilizar la API para automatizar operaciones o para crear varias entidades, como usuarios, de forma más rápida.

Recursos de primer nivel

La API de gestión de la red ofrece los siguientes recursos de primer nivel:

- /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 pertenezcan a un grupo LDAP local o federado de una cuenta de inquilino. Para obtener más información, consulta ["Utiliza 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 endpoints privados de StorageGRID también ignoran la versión de la API de la solicitud.

Realizar solicitudes a la API

La API de gestión de la red utiliza la plataforma de API de código abierto Swagger. Swagger ofrece una interfaz de usuario intuitiva que permite tanto a desarrolladores como a usuarios sin conocimientos de programación realizar operaciones en tiempo real en StorageGRID mediante la API.

La interfaz de usuario de Swagger ofrece información completa y documentación detallada para cada operación de la API.

Antes de empezar

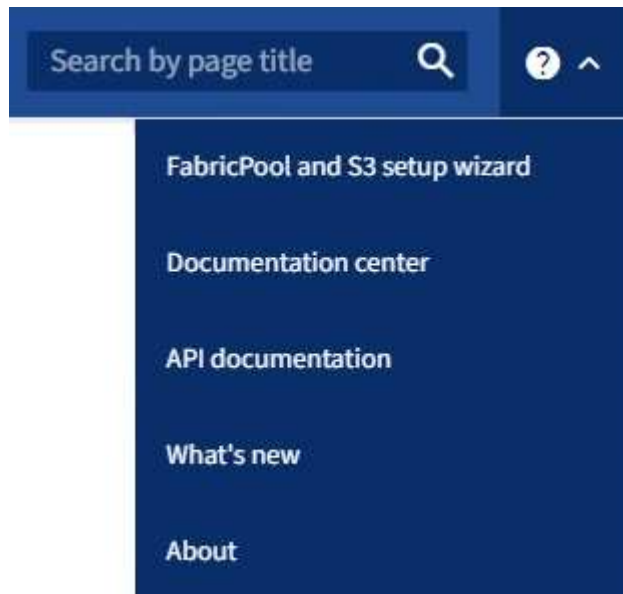
- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).



Cualquier operación de la API que realices a través de la página web de la documentación de la API es una operación en tiempo real. Ten cuidado de no crear, actualizar ni eliminar por error datos de configuración u otros datos.

Pasos

1. En la barra de encabezado de Grid Manager, selecciona el icono de ayuda y selecciona **Documentación de la API**.



2. Para realizar una operación con la API privada, selecciona **Ir a la documentación de la API privada** en la página StorageGRID Management API.

Las API privadas están sujetas a cambios sin previo aviso. Los puntos finales privados de StorageGRID también ignoran la versión de la API de la solicitud.

3. Selecciona la operación que desees.

Al desplegar una operación de la API, podrás ver las acciones HTTP disponibles, como GET, PUT, UPDATE y DELETE.

4. Selecciona una acción HTTP para ver los detalles de la solicitud, incluyendo la URL del endpoint, una lista de los parámetros obligatorios u opcionales, un ejemplo del cuerpo de la solicitud (cuando sea necesario) y las posibles respuestas.

GET
/grid/groups
Lists Grid Administrator Groups

Try it out

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 application/json

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>

- Comprueba si la solicitud requiere parámetros adicionales, como un ID de grupo o de usuario. Luego, obtén estos valores. Puede que primero tengas que enviar otra solicitud a la API para obtener la información que necesitas.
- Comprueba si es necesario modificar el cuerpo de la solicitud de ejemplo. Si es así, puedes seleccionar **Modelo** para conocer los requisitos de cada campo.
- Selecciona **Pruébalo**.
- Introduce los parámetros necesarios o modifica el cuerpo de la solicitud según sea necesario.
- Selecciona **Ejecutar**.
- Revisa el código de respuesta para determinar si la solicitud fue exitosa.

La API de gestión de la red organiza las operaciones disponibles en las siguientes secciones.



Esta lista solo incluye las operaciones disponibles en la API pública.

- **cuentas:** Operaciones para gestionar cuentas de inquilinos de almacenamiento, incluyendo la creación de nuevas cuentas y la obtención del uso de almacenamiento para una cuenta determinada.
- **historial-alertas:** Operaciones en alertas resueltas.
- **alert-receivers:** Operaciones sobre los receptores de notificaciones de alertas (correo electrónico).
- **alert-rules:** Operaciones con reglas de alerta.
- **alert-silences:** Operaciones sobre el silenciamiento de alertas.
- **alertas:** Operaciones sobre alertas.
- **audit:** Operaciones para mostrar y actualizar la configuración de auditoría.
- **auth:** Operaciones para realizar la autenticación de la sesión del usuario.

La API de gestión de la red es compatible con el esquema de autenticación mediante token de portador. Para iniciar sesión, debes introducir un nombre de usuario y una contraseña en el cuerpo JSON de la solicitud de autenticación (es decir, `POST /api/v3/authorize`). Si el usuario se autentica correctamente, se devuelve un token de seguridad. Este token debe incluirse en el encabezado de las solicitudes posteriores a la API ("`Authorization: Bearer token`"). El token caduca después de 16 horas.



Si el inicio de sesión único está habilitado para el sistema StorageGRID, debes realizar pasos diferentes para autenticarte. Consulta "Autenticación en la API si el inicio de sesión único está habilitado".

Consulta «Protección contra la falsificación de solicitudes entre sitios» para obtener información sobre cómo mejorar la seguridad de autenticación.

- **certificados de cliente:** Operaciones para configurar certificados de cliente para que se pueda acceder de forma segura a StorageGRID usando herramientas de supervisión externas.
- **config:** operaciones relacionadas con la versión del producto y las versiones de la Grid Management API. Puedes enumerar la versión del producto y las versiones principales de la Grid Management API compatibles con esa versión, y puedes desactivar las versiones obsoletas de la API.
- **funciones-desactivadas:** Operaciones para ver funciones que podrían haberse desactivado.
- **dns-servers:** Operaciones para ver y modificar los servidores DNS externos configurados.
- **drive-details:** Operaciones en unidades para modelos específicos de dispositivos de almacenamiento.
- **endpoint-domain-names:** Operaciones para mostrar y cambiar los nombres de dominio de los endpoints de S3.
- **código de borrado:** Operaciones sobre perfiles de código de borrado.
- **expansión:** Operaciones sobre expansión (a nivel de procedimiento).
- **nodos de expansión:** Operaciones en la expansión (a nivel de nodo).
- **emplazamientos-de-expansión:** Operaciones de expansión (a nivel de emplazamiento).
- **grid-networks:** Operaciones para mostrar y cambiar la lista de la Grid Network.

- **grid-passwords:** Operaciones para la gestión de contraseñas de grid.
- **grupos:** Operaciones para gestionar los grupos de administradores de Grid locales y para recuperar los grupos de administradores de Grid federados desde un servidor LDAP externo.
- **fuelle-de-identidad:** Operaciones para configurar una fuente de identidad externa y para sincronizar manualmente la información de grupos y usuarios federados.
- **ilm:** Operaciones sobre la gestión del ciclo de vida de la información (ILM).
- **procedimientos-en-curso:** Recupera los procedimientos de mantenimiento que están en curso.
- **licencia:** Operaciones para recuperar y actualizar la licencia de StorageGRID.
- **registros:** Operaciones para recopilar y descargar archivos de registro.v
- **métricas:** Operaciones con métricas de StorageGRID, incluidas consultas de métricas instantáneas en un único punto en el tiempo y consultas de métricas en un intervalo de tiempo. La Grid Management API utiliza la herramienta de monitoreo de sistemas Prometheus como fuente de datos backend. Para obtener información sobre cómo crear consultas de Prometheus, consulta el sitio web de Prometheus.



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

- **node-details:** Operaciones sobre los detalles de los nodos.
- **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 mostrar o actualizar servidores externos de Network Time Protocol (NTP).
- **objetos:** Operaciones sobre objetos y metadatos de objetos.
- **recuperación:** Operaciones para el procedimiento de recuperación.
- **paquete-de-recuperación:** Operaciones para descargar el paquete de recuperación.
- **regiones:** Operaciones para ver y crear regiones.
- **s3-object-lock:** Operaciones sobre la configuración global de S3 Object Lock.
- **certificado del servidor:** Operaciones para consultar y actualizar los certificados del servidor de Grid Manager.
- **snmp:** Operaciones sobre la configuración actual de SNMP.
- **marcas de agua de almacenamiento:** Marcas de agua de los nodos de almacenamiento.
- **clases-de-tráfico:** Operaciones para las políticas de clasificación de tráfico.
- **untrusted-client-network:** Operaciones en la configuración de la red de clientes no fiables.
- **Usuarios:** Operaciones para ver y gestionar usuarios de Grid Manager.

Versionado de la Grid Management API en StorageGRID

La API de gestión de la red utiliza versionado para permitir actualizaciones sin interrupciones.

Por ejemplo, esta URL de solicitud especifica la versión 4 de la API.

`https://hostname_or_ip_address/api/v4/authorize`

La versión principal de la API se incrementa cuando se realizan cambios que *no son compatibles* con las versiones anteriores. La versión secundaria de la API se incrementa cuando se realizan cambios que *sí son compatibles* con las versiones anteriores. Los cambios compatibles incluyen la adición de nuevos endpoints o nuevas propiedades.

El siguiente ejemplo ilustra cómo se incrementa la versión de la API en función del tipo de cambios realizados.

Tipo de cambio en la API	Versión anterior	Nueva versión
Compatible con versiones anteriores	2,1	2,2
No es compatible con versiones anteriores	2,1	3,0

Al instalar el software StorageGRID por primera vez, solo se habilita la versión más reciente de la API. Sin embargo, al actualizar a una nueva versión funcional de StorageGRID, sigues teniendo acceso a la versión anterior de la API durante al menos una versión funcional de StorageGRID.



Puedes configurar las versiones compatibles. Consulta la sección **config** de la documentación de la API de Swagger para el "[API de gestión de grid](#)" para más información. Debes desactivar la compatibilidad con la versión anterior después de actualizar todos los clientes de la API para que usen la versión más reciente.

Las solicitudes obsoletas se marcan como en desuso de las siguientes maneras:

- El encabezado de respuesta es "Deprecated: true"
- El cuerpo de la respuesta JSON incluye "deprecated": true
- Se añade una advertencia de obsolescencia a nms.log. Por ejemplo:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Averigua qué versiones de la API son compatibles en la versión actual

Utiliza la solicitud de API `GET /versions` para devolver una lista de las versiones principales de la 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
  ]
}
```

Especifica una versión de la API para una solicitud

Puedes especificar la versión de la API utilizando un parámetro de ruta (/api/v4) o un encabezado (Api-Version: 4). Si proporcionas ambos valores, el valor del encabezado tiene prioridad sobre el de la ruta.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protege contra la falsificación de petición en sitios cruzados (CSRF) en StorageGRID

Puedes ayudar a proteger StorageGRID contra los ataques de falsificación de solicitudes entre sitios (CSRF) utilizando tokens CSRF para reforzar la autenticación que usa cookies. Grid Manager y Tenant Manager activan automáticamente esta función de seguridad; otros clientes de la API pueden elegir si desean activarla al iniciar sesión.

Un atacante que pueda provocar el envío de una solicitud a otro sitio (por ejemplo, mediante un formulario HTTP POST) puede hacer que se realicen ciertas solicitudes utilizando las cookies del usuario que ha iniciado sesión.

StorageGRID ayuda a proteger contra los ataques CSRF mediante el uso de tokens CSRF. Cuando está habilitado, el contenido de una cookie específica debe coincidir con el contenido de un encabezado específico o de un parámetro específico del cuerpo de POST.

Para habilitar la función, establece el parámetro `csrfToken` en `true` durante la autenticación. El valor predeterminado es `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Cuando es verdadero, se establece una cookie `GridCsrfToken` con un valor aleatorio para los inicios de sesión en el Grid Manager, y la cookie `AccountCsrfToken` se establece con un valor aleatorio para los inicios de sesión en el Tenant Manager.

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:

- La cabecera `X-Csrf-Token`, con el valor de la cabecera establecido en el valor de la cookie de token CSRF.
- Para los puntos finales que aceptan un cuerpo codificado en formato form-encoded: un parámetro del cuerpo de la solicitud codificado en formato form-encoded. `csrfToken`

Consulta la documentación en línea de la API para ver más ejemplos y detalles.



Las solicitudes que tengan configurada una cookie con un token CSRF también aplicarán el encabezado "Content-Type: application/json" a cualquier solicitud que requiera un cuerpo de solicitud en formato JSON como protección adicional contra los ataques CSRF.

Utiliza la API si el inicio de sesión único está activado

Usa la API de StorageGRID si el inicio de sesión único está activado (Active Directory)

Si tienes ["configurado y activado el inicio de sesión único \(SSO\)"](#) y usas Active Directory como proveedor de inicio de sesión único, debes hacer una serie de solicitudes de API para obtener un token de autenticación válido para la Grid Management API o la Tenant Management API.

Inicia sesión en la API si está activado el inicio de sesión único

Estas instrucciones aplican si usas Active Directory como proveedor de identidad de inicio de sesión único (SSO).

Antes de empezar

- Conoces el nombre de usuario y la contraseña de inicio de sesión único de un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si quieres acceder a la API de gestión de inquilinos, sabes el ID de la cuenta del inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puedes usar uno de los siguientes ejemplos:

- El script de Python `storagegrid-ssoauth.py`, que se encuentra en el directorio de archivos de instalación de StorageGRID (`./rpms` para RHEL, `./debs` para Ubuntu o Debian, y `./vsphere` para VMware).
- Un ejemplo de flujo de trabajo de solicitudes con curl.

El flujo de trabajo de curl podría agotar el tiempo de espera si lo ejecutas demasiado despacio. Es posible que aparezca el siguiente error: `A valid SubjectConfirmation was not found on this Response.`



El flujo de trabajo de ejemplo de curl no protege la contraseña de ser vista por otros usuarios.

Si tienes un problema de codificación de URL, es posible que veas el error: `Unsupported SAML version.`

Pasos

1. Selecciona uno de los siguientes métodos para obtener un token de autenticación:
 - Utiliza el `storagegrid-ssoauth.py` script de Python. Ve al paso 2.
 - Utiliza solicitudes con curl. Ve al paso 3.
2. Si quieres utilizar el script `storagegrid-ssoauth.py`, pásalo al intérprete de Python y ejecútalo.

Cuando se te solicite, introduce los valores para los siguientes argumentos:

- El método SSO. Introduce ADFS o adfs.
- El nombre de usuario de SSO
- El dominio en el que está instalado StorageGRID
- La dirección de StorageGRID
- El ID de la cuenta del tenant, si deseas acceder a la API de Tenant Management.

```
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 aparece en la salida. Ahora puedes utilizar el token para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.

3. Si quieres utilizar solicitudes curl, usa el siguiente procedimiento.
 - a. Declara las variables necesarias para iniciar sesión.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```



Para acceder a la API de gestión de la red, utiliza 0 como TENANTACCOUNTID.

- b. Para recibir una URL de autenticación firmada, envía una solicitud POST a `/api/v3/authorize-saml` y elimina la codificación JSON adicional de la respuesta.

Este ejemplo muestra una solicitud POST para obtener una URL de autenticación firmada para TENANTACCOUNTID. Los resultados se enviarán 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 de este ejemplo incluye una URL firmada que está codificada como URL, pero no incluye la capa adicional de codificación JSON.

```
{
  "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. Guarda el SAMLRequest de la respuesta para usarlo en comandos posteriores.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

- d. Obtén una URL completa que incluya el ID de la 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=fZHRTOMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Guarda 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 tu sistema de SSO, el envío del formulario también contendrá la segunda contraseña u otras credenciales.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRTOMwFIZfhb...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. Guarda la MSISAuth cookie de la respuesta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Envía una solicitud GET a la ubicación especificada con las cookies de la autenticación POST.

```
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 uso posterior en el cierre de sesión, y el cuerpo de la respuesta contiene el SAMLResponse en un campo oculto del formulario.

```
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
XFXVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThtMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMj0lOVpcMQ==;
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="PHNhbWxwOlJlc3Bvb3N1scDpsZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Guarda el SAMLResponse del campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

- j. Utilizando el archivo guardado `SAMLResponse`, haz una solicitud `StorageGRID/api/saml-response` para generar un token de autenticación de StorageGRID.

Para `RelayState`, usa el ID de la cuenta de inquilino o usa 0 si quieres iniciar sesión en la API de gestión 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. Guarda el token de autenticación de la respuesta como `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ahora puedes utilizar `MYTOKEN` para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.

Cierra sesión en la API si el inicio de sesión único está activado

Si se ha habilitado el inicio de sesión único (SSO), debes realizar una serie de solicitudes de API para cerrar la sesión en la Grid Management API o en la Tenant Management API. Estas instrucciones aplican si usas Active Directory como proveedor de identidad de SSO.

Acerca de esta tarea

Si es necesario, puedes cerrar sesión en la API de StorageGRID desde la página de cierre de sesión único de tu organización. O puedes activar el cierre de sesión único (SLO) desde StorageGRID, lo que requiere un token de portador válido de StorageGRID.

Pasos

1. Para generar una solicitud de cierre de sesión con firma, pasa `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. Guarda la URL de cierre de sesión.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Envía una solicitud a la URL de cierre de sesión para activar el SLO y redirigir de nuevo a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Se devuelve la respuesta 302. La ubicación de redireccionamiento no es aplicable al cierre de sesión exclusivo de la API.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018 22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Elimina el token bearer de StorageGRID.

Eliminar el token de portador de StorageGRID funciona igual que sin SSO. Si no se proporciona la cookie "sso=true", el usuario se desconecta 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
```

Una respuesta 204 No Content indica que el usuario ha cerrado sesión.

```
HTTP/1.1 204 No Content
```

Usa la API de StorageGRID si el inicio de sesión único está activado (Entra ID)

Si tienes ["configurado y activado el inicio de sesión único \(SSO\)"](#) y usas Entra ID como proveedor de inicio de sesión único, puedes usar dos scripts de ejemplo para obtener un token de autenticación válido para la API de gestión de Grid o la API de gestión de Tenant.

Inicia sesión en la API si está activado el inicio de sesión único de Entra ID

Estas instrucciones aplican si usas Entra ID como proveedor de identidad de inicio de sesión único

Antes de empezar

- Conoces la dirección de correo electrónico y la contraseña de inicio de sesión único de un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si quieres acceder a la API de gestión de inquilinos, sabes el ID de la cuenta del inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puedes utilizar los siguientes scripts de ejemplo:

- El `storagegrid-ssoauth-azure.py` script de Python
- El `storagegrid-ssoauth-azure.js` script Node.js

Ambos scripts se encuentran en el directorio de archivos de instalación de StorageGRID (`./rpms` para RHEL, `./debs` para Ubuntu o Debian, y `./vsphere` para VMware).

Para escribir tu propia integración de API con Entra ID, consulta el script `storagegrid-ssoauth-azure.py`. El script de Python realiza dos solicitudes directamente a StorageGRID (primero para obtener el SAMLRequest y luego para obtener el token de autorización), y también llama al script de Node.js para interactuar con Entra ID y realizar las operaciones de inicio de sesión único.

Las operaciones de SSO pueden ejecutarse mediante una serie de solicitudes de API, pero hacerlo no es sencillo. Se utiliza el módulo Puppeteer de Node.js para extraer datos de la interfaz de SSO de Entra ID.

Si tienes un problema de codificación de URL, es posible que veas el error: `Unsupported SAML version`.

Pasos

1. Instala las dependencias necesarias de la siguiente manera:

- a. Instala Node.js (consulta "<https://nodejs.org/en/download/>").
- b. Instala los módulos necesarios de Node.js (puppeteer y jsdom):

```
npm install -g <module>
```

2. Pasa el script de Python al intérprete de Python para ejecutar el script.

Luego, el script de Python llamará al script correspondiente de Node.js para realizar las interacciones de inicio de sesión único de Entra ID.

3. Cuando se te solicite, introduce los valores de los siguientes argumentos (o pásalos mediante parámetros):
 - La dirección de correo electrónico de SSO utilizada para iniciar sesión en Entra ID
 - La dirección de StorageGRID
 - El ID de la cuenta del inquilino, si quieres acceder a la API de gestión de inquilinos
4. Cuando se te solicite, introduce la contraseña y prepárate para proporcionar una autorización MFA a Entra ID si se te pide.

```
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 parte de la base de que la autenticación multifactor (MFA) se realiza usando Microsoft Authenticator. Es posible que tengas que 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 aparece en la salida. Ahora puedes utilizar el token para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.

Usa la API de StorageGRID si el inicio de sesión único está activado (PingFederate)

Si tienes "[configurado y activado el inicio de sesión único \(SSO\)](#)" y usas PingFederate como proveedor de inicio de sesión único, debes realizar una serie de solicitudes de API para obtener un token de autenticación válido para la Grid Management API o la Tenant Management API.

Inicia sesión en la API si está activado el inicio de sesión único

Estas instrucciones aplican si usas PingFederate como proveedor de identidad de SSO

Antes de empezar

- Conoces el nombre de usuario y la contraseña de inicio de sesión único de un usuario federado que pertenece a un grupo de usuarios de StorageGRID.
- Si quieres acceder a la API de gestión de inquilinos, sabes el ID de la cuenta del inquilino.

Acerca de esta tarea

Para obtener un token de autenticación, puedes usar uno de los siguientes ejemplos:

- El script de Python `storagegrid-ssoauth.py`, que se encuentra en el directorio de archivos de instalación de StorageGRID (`./rpms` para RHEL, `./debs` para Ubuntu o Debian, y `./vsphere` para VMware).
- Un ejemplo de flujo de trabajo de solicitudes con curl.

El flujo de trabajo de curl podría agotar el tiempo de espera si lo ejecutas demasiado despacio. Es posible que aparezca el siguiente error: `A valid SubjectConfirmation was not found on this Response.`



El flujo de trabajo de ejemplo de curl no protege la contraseña de ser vista por otros usuarios.

Si tienes un problema de codificación de URL, es posible que veas el error: `Unsupported SAML version.`

Pasos

1. Selecciona uno de los siguientes métodos para obtener un token de autenticación:
 - Utiliza el `storagegrid-ssoauth.py` script de Python. Ve al paso 2.
 - Utiliza solicitudes con curl. Ve al paso 3.
2. Si quieres utilizar el script `storagegrid-ssoauth.py`, pásalo al intérprete de Python y ejecútalo.

Cuando se te solicite, introduce los valores para los siguientes argumentos:

- El método SSO. Puedes introducir cualquier variante de «pingfederate» (PINGFEDERATE, pingfederate, y así sucesivamente).
- El nombre de usuario de SSO
- El dominio en el que está instalado StorageGRID. Este campo no se utiliza para PingFederate. Puedes dejarlo en blanco o ingresar cualquier valor.
- La dirección de StorageGRID
- El ID de la cuenta del tenant, si deseas acceder a la API de Tenant Management.

```
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 aparece en la salida. Ahora puedes utilizar el token para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.

3. Si quieres utilizar solicitudes curl, usa el siguiente procedimiento.

a. Declara las variables necesarias para iniciar sesión.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```



Para acceder a la API de gestión de la red, utiliza 0 como TENANTACCOUNTID.

b. Para recibir una URL de autenticación firmada, envía una solicitud POST a /api/v3/authorize-saml y elimina la codificación JSON adicional de la respuesta.

Este ejemplo muestra una solicitud POST para una URL de autenticación firmada para TENANTACCOUNTID. Los resultados se pasan 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 de este ejemplo incluye una URL firmada que está codificada como URL, pero no incluye la capa adicional de codificación JSON.

```
{
  "apiVersion": "3.0",
  "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

c. Guarda el SAMLRequest de la respuesta para usarlo en comandos posteriores.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. Exporta la respuesta y la cookie, y muestra 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 muestra la respuesta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Exporta el valor de «href» (elimina la barra al final /) y muestra la respuesta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Exporta el valor 'action':

```
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. Guarda el SAMLResponse del campo oculto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizando el archivo guardado SAMLResponse, haz una solicitud StorageGRID/api/saml-response para generar un token de autenticación de StorageGRID.

Para RelayState, usa el ID de la cuenta de inquilino o usa 0 si quieres iniciar sesión en la API de gestión 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. Guarda el token de autenticación de la respuesta como MYTOKEN.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ahora puedes utilizar MYTOKEN para otras solicitudes, de forma similar a como lo harías si no se utilizara el inicio de sesión único.

Cierra sesión en la API si el inicio de sesión único está activado

Si se ha habilitado el inicio de sesión único (SSO), debes realizar una serie de solicitudes de API para cerrar la sesión en la API de gestión de Grid o en la API de gestión de Tenant. Estas instrucciones aplican si usas PingFederate como proveedor de identidad de SSO.

Acerca de esta tarea

Si es necesario, puedes cerrar sesión en la API de StorageGRID desde la página de cierre de sesión único de tu organización. O puedes activar el cierre de sesión único (SLO) desde StorageGRID, lo que requiere un token de portador válido de StorageGRID.

Pasos

1. Para generar una solicitud de cierre de sesión con firma, pasa `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. Guarda la URL de cierre de sesión.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Envía una solicitud a la URL de cierre de sesión para activar el SLO y redirigir de nuevo a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Se devuelve la respuesta 302. La ubicación de redireccionamiento no es aplicable al cierre de sesión exclusivo de la 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. Elimina el token bearer de StorageGRID.

Eliminar el token de portador de StorageGRID funciona igual que sin SSO. Si no se proporciona la cookie "sso=true", el usuario se desconecta 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
```

Una respuesta 204 No Content indica que el usuario ha cerrado sesión.

```
HTTP/1.1 204 No Content
```

Desactiva las funciones de StorageGRID con la API

Puedes usar la API de gestión de grid para desactivar por completo ciertas funciones en el sistema StorageGRID. Cuando se desactiva una función, no se pueden asignar permisos a nadie para realizar las tareas relacionadas con esa función.

Acerca de esta tarea

El sistema de funciones desactivadas te permite impedir el acceso a determinadas funciones del sistema StorageGRID. Desactivar una función es la única forma de impedir que el usuario raíz o los usuarios que pertenezcan a grupos de administración con permiso de acceso a raíz puedan utilizar esa función.

Para comprender cómo puede resultar útil esta funcionalidad, imagina la siguiente situación:

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 inquilinos, la empresa A quiere asegurarse de que sus propios empleados nunca puedan acceder a ninguna cuenta de inquilino una vez que esta se haya implementado.

*La empresa A puede alcanzar este objetivo utilizando el sistema **Deactivate Features en la Grid Management API**. Al desactivar por completo la función **Change tenant root password** en el Grid Manager (tanto en la interfaz de usuario como en la API), la empresa A se asegura de que los usuarios Admin —incluidos el usuario raíz y los usuarios que pertenecen a grupos con el permiso **Root access**— no puedan cambiar la contraseña del usuario raíz de ninguna cuenta de tenant.*

Pasos

1. Accede a la documentación de Swagger sobre la API de gestión de la red. Consulta "[Usa la API de gestión de Grid](#)".
2. Ubica el endpoint Deactivate Features.
3. Para desactivar una función, como Cambiar la contraseña raíz del inquilino, envía un cuerpo a la API como este:

```
{ "grid": { "changeTenantRootPassword": true } }
```

Cuando se completa la solicitud, la función Cambiar la contraseña de root del inquilino queda desactivada. El permiso de administración **Cambiar la 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 Forbidden".

Reactivar las funciones desactivadas

De forma predeterminada, puedes utilizar la API de gestión de la red para reactivar una función que se haya desactivado. Sin embargo, si deseas evitar que las funciones desactivadas se vuelvan a activar en ningún momento, puedes desactivar la propia función **activateFeatures**.



La función **activateFeatures** no se puede volver a activar. Si decides desactivar esta función, ten en cuenta que perderás de forma permanente la posibilidad de volver a activar cualquier otra función desactivada. Debes ponerte en contacto con el soporte técnico para recuperar cualquier funcionalidad perdida.

Pasos

1. Accede a la documentación de Swagger para la API de gestión de la red.

2. Ubica el endpoint Deactivate Features.
3. Para reactivar todas las funciones, envía un cuerpo a la API como este:

```
{ "grid": null }
```

Una vez completada esta solicitud, se reactivan todas las funciones, incluida la función **Cambiar la contraseña de root del inquilino**. El permiso de administración **Cambiar la contraseña de root del inquilino** aparece ahora en la interfaz de usuario, y cualquier solicitud de API que intente cambiar la contraseña de root de un inquilino se ejecutará con éxito, siempre que el usuario disponga del permiso de administración **Acceso a raíz** o **Cambiar la contraseña de root del inquilino**.



El ejemplo anterior hace que se reactiven *todas* las funciones desactivadas. Si se han desactivado otras funciones que deberían permanecer desactivadas, debes especificarlas explícitamente en la solicitud PUT. Por ejemplo, para reactivar la función Cambiar la contraseña raíz del inquilino y mantener desactivado el permiso de gestión storageAdmin, envía esta solicitud PUT:

```
{ "grid": {"storageAdmin": true} }
```

Controlar el acceso a StorageGRID

Controlar el acceso a StorageGRID

Puedes controlar quién puede acceder a StorageGRID y qué tareas pueden realizar los usuarios creando o importando grupos y usuarios y asignando permisos a cada grupo. Opcionalmente, puedes habilitar el inicio de sesión único (SSO), crear certificados de cliente y cambiar las contraseñas de grid.

Controla el acceso al Grid Manager

Tú determinas quién puede acceder a Grid Manager y a la API de gestión de la red importando grupos y usuarios desde un servicio de federación de identidades o configurando grupos y usuarios locales.

Usar "[federación de identidades](#)" hace que configurar "[grupos](#)" y "[usuarios](#)" sea más rápido, y permite que los usuarios inicien sesión en StorageGRID con sus credenciales habituales. Puedes configurar la federación de identidades si usas Active Directory, OpenLDAP u Oracle Directory Server.



Ponte en contacto con el soporte técnico si deseas utilizar otro servicio LDAP v3.

Determinas qué tareas puede realizar cada usuario asignando diferentes "[permisos](#)" a cada grupo. Por ejemplo, es posible que quieras que los usuarios de un grupo puedan gestionar las reglas de ILM y que los usuarios de otro grupo realicen tareas de mantenimiento. Un usuario debe pertenecer al menos a un grupo para acceder al sistema.

Opcionalmente, puedes configurar un grupo para que sea de solo lectura. Los usuarios de un grupo de solo lectura solo pueden ver la configuración y las funciones. No pueden realizar ningún cambio ni llevar a cabo ninguna operación en el Grid Manager o en la Grid Management API.

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 que "[configura y activa el SSO](#)", todos los usuarios deben

autenticarse mediante un proveedor de identidad externo antes de poder acceder al Grid Manager, al Tenant Manager, a la API de Grid Management o a la API de Tenant Management. 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 del grid y las claves de cifrado para el sistema StorageGRID. Puedes ["cambiar la contraseña"](#) según sea necesario.

Cambiar las contraseñas de la consola de los nodos

Cada nodo de tu grid tiene una contraseña de consola de nodo, que necesitas para iniciar sesión en el nodo como "admin" usando SSH, o como usuario raíz en una conexión de consola de VM/física. Si lo necesitas, puedes ["cambiar la contraseña de la consola del nodo"](#) para cada nodo.

Cambia la contraseña de aprovisionamiento de StorageGRID

Usa 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 de paquetes de recuperación que incluyen la información de la topología de la grid, las contraseñas de la consola de los nodos de la grid y las claves de cifrado del sistema StorageGRID.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes permisos de mantenimiento o de 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 ["descargar el paquete de recuperación"](#). La frase de contraseña de aprovisionamiento no aparece en el archivo `Passwords.txt`. Asegúrate de documentar la frase de contraseña de aprovisionamiento y de guardarla en un lugar seguro.

Pasos

1. Selecciona **Configuración > Control de acceso > Contraseñas de grid**.
2. En **Cambiar la frase de acceso de aprovisionamiento**, selecciona **Realizar un cambio**
3. Introduce tu contraseña de aprovisionamiento actual.
4. Introduce la nueva frase de contraseña. La frase de contraseña debe contener al menos 8 y no más de 32 caracteres. Las frases de contraseña distinguen mayúsculas de minúsculas.



Guarda la frase de contraseña de aprovisionamiento en un lugar seguro. Es necesaria para los procedimientos de instalación, ampliación y mantenimiento.

5. Vuelve a introducir la nueva frase de contraseña y selecciona **Guardar**.

El sistema muestra un mensaje verde de éxito cuando se completa el cambio de la contraseña de

aprovisionamiento.



Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

6. Selecciona **Paquete de recuperación**.

7. Introduce la nueva frase de contraseña de aprovisionamiento para descargar el nuevo paquete de recuperación.



Tras cambiar la contraseña de aprovisionamiento, debes descargar inmediatamente un nuevo paquete de recuperación. El archivo del paquete de recuperación te permite restaurar el sistema en caso de que se produzca un fallo.

Cambia las contraseñas de la consola de nodo en StorageGRID

Cada nodo de tu grid tiene una contraseña de consola de nodo, que usas para iniciar sesión en el nodo. Por defecto, cada nodo tiene una contraseña única. Puedes cambiar cada contraseña por una nueva contraseña única, o puedes cambiar la contraseña de todos los nodos para usar una contraseña global. Las contraseñas se almacenan en el paquete de recuperación.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- Tienes la contraseña de aprovisionamiento actual.

Acerca de esta tarea

Usas una contraseña de la consola del nodo para iniciar sesión en un nodo como "admin" usando SSH, o como usuario raíz en una conexión de consola de una máquina virtual o física. Puedes cambiar las contraseñas de la consola del nodo usando una de estas opciones:

- Aplicar automáticamente contraseñas aleatorias a cada nodo
- Especifica y aplica una contraseña global a todos los nodos
- Especifica y aplica una contraseña única a uno o varios nodos

Las contraseñas se almacenan en un archivo actualizado `Passwords.txt` que se encuentra en el paquete de recuperación. Las contraseñas aparecen en la columna Password del archivo.



El ["Contraseñas de acceso SSH"](#) de las claves SSH utilizadas para la comunicación entre nodos es independiente de las contraseñas de la consola de los nodos. Este procedimiento no cambia las contraseñas de acceso SSH.

Accede al asistente

Pasos

1. Selecciona **Configuración > Control de acceso > Contraseñas de grid**.
2. En **Cambiar contraseñas de la consola del nodo**, selecciona **Realizar un cambio**.

Descargar el paquete de recuperación actual

Antes de cambiar las contraseñas de la consola de los nodos, descarga el paquete de recuperación actual. Puedes utilizar las contraseñas de este archivo si el proceso de cambio de contraseña falla en algún nodo.

Pasos

1. Introduce la frase de contraseña de aprovisionamiento de tu grid.
2. Selecciona **Descargar paquete de recuperación**.
3. Copia el archivo del paquete de recuperación (.zip) en dos ubicaciones seguras y distintas.



El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

4. Selecciona **Continuar**.

Proporciona nuevas contraseñas

1. Selecciona el método de cambio de contraseña que quieras utilizar.
 - **Automático:** StorageGRID asigna automáticamente una nueva contraseña aleatoria de consola a todos los nodos.
 - **Personalizado:** Tú proporcionas las contraseñas de la consola.

Automático

1. Selecciona **Continuar**.

Personalizado

1. Selecciona una de las siguientes:
 - **Contraseña global de la consola:** aplica la misma contraseña de la consola a todos los nodos.
 - **Contraseñas únicas de consola:** Establece una contraseña diferente en uno o varios nodos.
2. Si has seleccionado **Contraseña global de la consola**, introduce la contraseña que quieras usar para todos los nodos.
3. Si has seleccionado **Contraseñas únicas de consola**, introduce una contraseña única para uno o más nodos.
4. Selecciona **Continuar**.

Finaliza el cambio de contraseña

1. Cuando aparezca el cuadro de diálogo de confirmación, selecciona **Sí** si estás listo para que StorageGRID comience a cambiar las contraseñas de la consola de los nodos.



No puedes cancelar este proceso después de que comienza.

StorageGRID genera un nuevo paquete de recuperación que contiene la nueva contraseña.

2. Cuando el nuevo paquete de recuperación esté listo, selecciona **Descargar nuevo paquete de recuperación** y guarda el paquete de recuperación.
3. Abre el archivo .zip.

4. Comprueba que puedes acceder a los contenidos, incluido el archivo `Passwords.txt`, que contiene las nuevas contraseñas de la consola de nodo.
5. Copia el nuevo archivo del paquete de recuperación (.zip) en dos ubicaciones seguras y distintas.



No sobrescribas el paquete de recuperación anterior.

Debes proteger el archivo de recuperación, porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

6. Marca la casilla de verificación para indicar que has descargado el nuevo paquete de recuperación y has verificado el contenido.
7. Selecciona **Continuar**.

StorageGRID actualiza la contraseña de cada nodo.

Si se produce un error durante el proceso de actualización, la barra de progreso muestra el número de nodos en los que no se pudo cambiar la contraseña. El sistema volverá a intentar automáticamente el proceso en cualquier nodo en el que no se pudo cambiar la contraseña. Si el proceso termina y todavía hay algunos nodos en los que no se cambió la contraseña, aparece el botón **Reintentar**.

8. Si la actualización de la contraseña falló en uno o varios nodos:
 - a. Revisa los mensajes de error que aparecen en la tabla.
 - b. Resuelve los problemas.
 - c. Selecciona **Reintentar**.



Al volver a intentarlo, solo se modifican las contraseñas de la consola de los nodos en los que falló el cambio de contraseña en intentos anteriores.

9. Cuando la barra de progreso indique que ya no quedan actualizaciones, selecciona **Finalizar**.
10. Una vez que se hayan cambiado las contraseñas de la consola de todos los nodos, elimina el [el primer paquete de recuperación que descargaste](#).

Cambia las contraseñas de acceso SSH para StorageGRID Admin Nodes

Al cambiar las contraseñas de acceso SSH de los nodos de administración, también se actualizan los conjuntos únicos de claves SSH internas de cada nodo de la grid. El nodo de administración principal utiliza estas claves SSH para acceder a los nodos mediante una autenticación segura y sin contraseña.

Utiliza una clave SSH para iniciar sesión en un nodo como `admin` o como usuario raíz en una máquina virtual o mediante una conexión a la consola física.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- 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 de cada nodo se almacenan en el archivo `Passwords.txt` del paquete de recuperación. Las claves aparecen en la columna Contraseña de dicho archivo.

Existen contraseñas de acceso SSH independientes para las claves SSH que se utilizan para la comunicación entre nodos. Este procedimiento no las modifica.

Accede al asistente

Pasos

1. Selecciona **Configuración > Control de acceso > Contraseñas de grid**.
2. En **Cambiar claves SSH**, selecciona **Realizar un cambio**.

Descargar el paquete de recuperación actual

Antes de cambiar las claves de acceso SSH, descarga el paquete de recuperación actual. Puedes utilizar las claves de este archivo si el proceso de cambio de claves falla en algún nodo.

Pasos

1. Introduce la frase de contraseña de aprovisionamiento de tu grid.
2. Selecciona **Descargar paquete de recuperación**.
3. Copia el archivo del paquete de recuperación (`.zip` en dos ubicaciones seguras y distintas.



El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

4. Selecciona **Continuar**.
5. Cuando aparezca el cuadro de diálogo de confirmación, selecciona **Sí** si estás listo para empezar a modificar las claves de acceso SSH.



No puedes cancelar este proceso después de que comienza.

Cambiar las claves de acceso SSH

Cuando se inicia el proceso de cambio de las 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. Espera 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 activo, selecciona **Descargar nuevo paquete de recuperación** y guarda el nuevo archivo del paquete de recuperación (`.zip` en dos ubicaciones seguras y separadas.
3. Cuando finalice la descarga:
 - a. Abre el archivo `.zip`.
 - b. Confirma que puedes acceder al contenido, incluido el archivo `Passwords.txt`, que contiene las nuevas claves de acceso SSH.
 - c. Copia el nuevo archivo del paquete de recuperación (`.zip` en dos ubicaciones seguras y distintas.



No sobrescribas el paquete de recuperación anterior.

El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

4. Espera a que las claves se actualicen en cada nodo, lo cual puede tardar unos minutos.

Si se cambian las claves de todos los nodos, aparece un banner verde de éxito.

Si se produce un error durante el proceso de actualización, un mensaje en un banner indica el número de nodos en los que no se pudo cambiar la clave. El sistema volverá a intentar automáticamente el proceso en cualquier nodo en el que no se pudo cambiar la clave. Si el proceso termina y algunos nodos siguen sin tener la clave cambiada, aparece el botón **Retry**.

Si la actualización de la clave falló en uno o varios nodos:

- a. Revisa los mensajes de error que aparecen en la tabla.
- b. Resuelve los problemas.
- c. Selecciona **Reintentar**.

Al volver a intentarlo, solo se modifican las claves de acceso SSH en los nodos que fallaron durante los intentos anteriores de cambio de clave.

5. Una vez que se hayan cambiado las claves de acceso SSH para todos los nodos, elimina el [el primer paquete de recuperación que descargaste](#).
6. Si lo deseas, selecciona **Mantenimiento > Sistema > Paquete de recuperación** para descargar una copia adicional del nuevo paquete de recuperación.

Usa la federación de identidades en StorageGRID

El uso de la federación de identidades agiliza la configuración de grupos y usuarios, y permite a los usuarios iniciar sesión en StorageGRID utilizando credenciales que ya conocen.

Configura la federación de identidades para Grid Manager

Puedes configurar la federación de identidades en Grid Manager si deseas que los grupos de administradores y los usuarios se gestionen en otro sistema, como Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server.

Antes de empezar

- Has iniciado sesión en Grid Manager usando una ["navegador web compatible"](#).
- Has ["permisos de acceso específicos"](#).
- Estás utilizando Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server como proveedor de identidades.



Si deseas utilizar un servicio LDAP v3 que no figure en la lista, ponte en contacto con soporte técnico.

- Si tienes previsto utilizar OpenLDAP, debes configurar el servidor OpenLDAP. Consulta [Guía para configurar un servidor OpenLDAP](#).

- Si tienes previsto habilitar el inicio de sesión único (SSO), ya revisaste la ["Requisitos y consideraciones para el inicio de sesión único"](#).
- Si tienes previsto utilizar Transport Layer Security (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidad está usando TLS 1.2 o 1.3. Consulta ["Algoritmos de cifrado compatibles para las conexiones TLS salientes"](#).

Acerca de esta tarea

Puedes configurar un origen de identidad para el Grid Manager si quieres importar grupos desde otro sistema como Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server. Puedes importar los siguientes tipos de grupos:

- Grupos de administradores. Los usuarios que forman parte de los grupos de administradores pueden iniciar sesión en Grid Manager y realizar tareas, en función de los permisos de gestión asignados al grupo.
- Grupos de usuarios de inquilinos para inquilinos que no usan su propia fuente de identidad. Los usuarios de los grupos de inquilinos pueden iniciar sesión en el Tenant Manager y realizar tareas según los permisos asignados al grupo en el Tenant Manager. Consulta ["Crear cuenta de inquilino"](#) y ["Utiliza una cuenta de inquilino"](#) para obtener más detalles.

Accede a la configuración

Pasos

1. Selecciona **Configuración > Control de acceso > Federación de identidades**.
2. Selecciona **Habilitar federación de identidades**.
3. En la sección de tipo de servicio LDAP, selecciona el tipo de servicio LDAP que quieres configurar.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Entra ID	OpenLDAP	Other

Selecciona **Other** para configurar los valores de un servidor LDAP que utilice Oracle Directory Server.

4. Si has seleccionado **Other**, rellena los campos de la sección «Atributos LDAP». De lo contrario, pasa al siguiente paso.
 - **Nombre único de usuario:** El nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo equivale a `sAMAccountName` para Active Directory y `uid` para OpenLDAP. Si estás configurando Oracle Directory Server, introduce `uid`.
 - **UUID de usuario:** El nombre del atributo que contiene el identificador único permanente de un usuario LDAP. Este atributo es equivalente a `objectGUID` en Active Directory y `entryUUID` en OpenLDAP. Si estás configurando Oracle Directory Server, introduce `nsuniqueid`. El valor de cada usuario para el atributo especificado debe ser un número hexadecimal de 32 dígitos, ya sea en formato de 16 bytes o de cadena, donde se ignoran los guiones.
 - **Nombre único de 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 estás configurando Oracle Directory Server, introduce `cn`.

- **UUID del 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 estás configurando Oracle Directory Server, introduce `nsuniqueid`. El valor de cada grupo para el atributo especificado debe ser un número hexadecimal de 32 dígitos, ya sea en formato de 16 bytes o de cadena, donde se ignoran los guiones.

5. Para todos los tipos de servicio LDAP, introduce la información necesaria sobre el servidor LDAP y la conexión de red en la sección Configurar el 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 usar cualquier puerto siempre que tu firewall esté configurado correctamente.

- **Nombre de usuario:** La ruta completa del nombre distintivo (DN) del usuario que se conectará al servidor LDAP.

Para Active Directory, también puedes especificar el Down-Level Logon Name o el User Principal Name.

El usuario especificado debe tener permiso para ver la lista de grupos y usuarios y para acceder a los siguientes atributos:

- `sAMAccountName` o `uid`
- `objectGUID`, `entryUUID`, o `nsuniqueid`
- `cn`
- `memberOf` o `isMemberOf`
- **Active Directory:** `objectSid`, `primaryGroupID`, `userAccountControl` y `userPrincipalName`
- **Entra ID:** `accountEnabled` y `userPrincipalName`

- **Contraseña:** la contraseña asociada al nombre de usuario.



Si cambias la contraseña en el futuro, debes actualizarla en esta página.

- **DN base del grupo:** La ruta completa del nombre distintivo (DN) de un subárbol LDAP en el que quieres buscar grupos. En el ejemplo de Active Directory (a continuación), todos los grupos cuyo nombre distintivo sea relativo al DN base (`DC=storagegrid,DC=example,DC=com`) pueden usarse como grupos federados.



Los valores de **Nombre único del grupo** deben ser únicos dentro del **DN base del grupo** al que pertenecen.

- **DN de base de usuarios:** La ruta completa del nombre distintivo (DN) de un subárbol LDAP en el que quieres buscar usuarios.



Los valores de **Nombre único de usuario** deben ser únicos dentro del **User Base DN** al que pertenecen.

- **Formato de nombre de usuario de enlace** (opcional): el patrón de nombre de usuario predeterminado que StorageGRID debe utilizar si no es posible determinar el patrón automáticamente.

Se recomienda especificar el **formato de nombre de usuario de enlace** porque puede permitir que los usuarios inicien sesión si StorageGRID no puede enlazarse con la cuenta de servicio.

Introduce uno de estos patrones:

- **Patrón UserPrincipalName (AD y Entra ID):** `[USERNAME]@example.com`
- **Patrón de nombre de inicio de sesión de nivel inferior (AD y Entra ID):**
`example\[USERNAME]`
- **Patrón de nombre distintivo:** `CN=[USERNAME],CN=Users,DC=example,DC=com`

Incluye **[USERNAME]** tal y como aparece escrito.

6. En la sección Transport Layer Security (TLS), selecciona una configuración de seguridad.

- **Usar STARTTLS:** Utiliza STARTTLS para proteger las comunicaciones con el servidor LDAP. Esta es la opción recomendada para Active Directory, OpenLDAP u Other, pero no es compatible con Microsoft Entra ID.
- **Usar LDAPS:** La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debes seleccionar esta opción para Microsoft Entra ID.
- **No utilices TLS:** El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Microsoft Entra ID.



El uso de la opción **No usar TLS** no se admite si tu servidor de Active Directory exige la firma LDAP. Debes usar STARTTLS o LDAPS.

7. Si has seleccionado STARTTLS o LDAPS, elige el certificado que se usa para proteger la conexión.

- **Utilizar el certificado CA del sistema operativo:** Utiliza el certificado CA de Grid predeterminado instalado en el sistema operativo para proteger las conexiones.
- **Usar certificado CA personalizado:** Usa un certificado de seguridad personalizado.

Si seleccionas esta opción, copia y pega el certificado de seguridad personalizado en el cuadro de texto de certificado de la CA.

Comprueba la conexión y guarda la configuración

Una vez introducidos todos los valores, debes comprobar la conexión antes de poder guardar la configuración. StorageGRID verifica los parámetros de conexión del servidor LDAP y el formato del nombre de usuario de enlace, si has especificado alguno.

Pasos

1. Selecciona **Probar conexión**.
2. Si no proporcionaste un formato para el nombre de usuario de bind:
 - Si los parámetros de conexión son correctos, aparece el mensaje «Prueba de conexión realizada con éxito». Selecciona **Guardar** para guardar la configuración.
 - Aparecerá el mensaje «No se ha podido establecer una conexión de prueba» si la configuración de la conexión no es válida. Selecciona **Cerrar**. Luego, soluciona cualquier problema y vuelve a probar la conexión.

3. Si has especificado un formato de nombre de usuario de enlace, introduce el nombre de usuario y la contraseña de un usuario federado válido.

Por ejemplo, introduce tu propio nombre de usuario y contraseña. No incluyas caracteres especiales 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](#)

- Si los parámetros de conexión son correctos, aparece el mensaje «Prueba de conexión realizada con éxito». Selecciona **Guardar** para guardar la configuración.
- Aparece un mensaje de error si la configuración de la conexión, el formato del nombre de usuario de enlace o el nombre de usuario y la contraseña de prueba no son válidos. Soluciona cualquier problema y vuelve a probar la conexión.

Forzar la sincronización con la fuente de identidad

El sistema StorageGRID sincroniza periódicamente los grupos y usuarios federados desde la fuente de identidades. Puedes forzar la sincronización si quieres habilitar o restringir los permisos de los usuarios lo más rápido posible.

Pasos

1. Ve a la página de federación de identidades.
2. Selecciona **Sync server** en la parte superior de la página.

El proceso de sincronización puede tardar un tiempo dependiendo de tu entorno.



La alerta **Error de sincronización de la federación de identidades** se activa si hay un problema al sincronizar los grupos y usuarios federados desde la fuente de identidades.

Desactivar la federación de identidades

Puedes desactivar de forma temporal o permanente la federación de identidades para grupos y usuarios. Cuando la federación de identidades está desactivada, no hay comunicación entre StorageGRID y el origen de identidad. Sin embargo, se conserva cualquier configuración que hayas realizado, lo que te permitirá volver a activar fácilmente la federación de identidades en el futuro.

Acerca de esta tarea

Antes de desactivar la federación de identidades, debes tener en cuenta lo siguiente:

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que están conectados actualmente seguirán teniendo acceso al sistema StorageGRID hasta que su sesión expire, pero no podrán iniciar sesión después de que su sesión expire.
- No se llevará a cabo la sincronización entre el sistema StorageGRID y la fuente de identidades, y no se generarán alertas para las cuentas que no se hayan sincronizado.
- La casilla de selección **Habilitar federación de identidades** aparece desactivada si el estado del inicio de sesión único (SSO) es **Habilitado** o **Modo Sandbox**. El estado del SSO en la página de inicio de sesión único debe estar **Desactivado** antes de que puedas desactivar la federación de identidades. Consulta ["Desactivar el inicio de sesión único"](#).

Pasos

1. Ve a la página de federación de identidades.
2. Desmarca la casilla **Habilitar federación de identidades**.

Guía para configurar un servidor OpenLDAP

Si deseas utilizar un servidor OpenLDAP para la federación de identidades, debes configurar determinados parámetros en el servidor OpenLDAP.



En el caso de las fuentes de identidad que no sean Active Directory o Microsoft Entra ID, StorageGRID no bloqueará automáticamente el acceso a S3 a los usuarios que hayan sido desactivados externamente. Para bloquear el acceso a S3, elimina cualquier clave de S3 del usuario o elimina al usuario de todos los grupos.

Superposiciones Memberof y refint

Los overlays memberof y refint deben estar habilitados. Para obtener más información, consulta las instrucciones para el mantenimiento de la pertenencia inversa a grupos en ["Documentación de OpenLDAP: Guía del administrador versión 2.4"](#).

Indexación

Debes configurar los siguientes atributos de 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, asegúrate de que los campos mencionados en la ayuda para Nombre de usuario estén indexados para un rendimiento óptimo.

Consulta la información sobre el mantenimiento inverso de la pertenencia a grupos en la ["Documentación de OpenLDAP: Guía del administrador versión 2.4"](#).

Administra grupos de administración en StorageGRID

Puedes crear grupos de administradores para gestionar los permisos de seguridad de

uno o varios usuarios administradores. Los usuarios deben pertenecer a un grupo para que se les conceda acceso al sistema StorageGRID.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).
- Si planeas importar un grupo federado, ya has configurado la federación de identidades y el grupo federado ya existe en la fuente de identidades configurada.

Crear un grupo de administradores

Los grupos de administradores te permiten determinar qué usuarios pueden acceder a qué funciones y operaciones en el Grid Manager y en la Grid Management API.

Accede al asistente

Pasos

1. Selecciona **Configuración > Control de acceso > Grupos de administradores**.
2. Selecciona **Crear grupo**.

Elige un tipo de grupo

Puedes crear un grupo local o importar un grupo federado.

- Crea un grupo local si quieres asignar permisos a los usuarios locales.
- Crea un grupo federado para importar usuarios desde la fuente de identidad.

Grupo local

Pasos

1. Selecciona **Grupo local**.
2. Introduce un nombre para mostrar para el grupo, que podrás modificar más adelante si es necesario. Por ejemplo, «Usuarios de mantenimiento» o «Administradores de ILM».
3. Introduce un nombre único para el grupo, que no podrás actualizar más adelante.
4. Selecciona **Continuar**.

Grupo federado

Pasos

1. Selecciona **Federated group**.
2. Introduce el nombre del grupo que deseas importar, exactamente como aparece en la fuente de identidad configurada.
 - Para Active Directory y Microsoft Entra ID, utiliza el sAMAccountName.
 - Para OpenLDAP, usa el CN (Common Name).
 - Para otro LDAP, utiliza el nombre único correspondiente para el servidor LDAP.
3. Selecciona **Continuar**.

Gestiona los permisos de los grupos

Pasos

1. Para **Modo de acceso**, selecciona si los usuarios del grupo pueden cambiar la configuración y realizar operaciones en el Grid Manager y la Grid Management API o si solo pueden ver la configuración y las funciones.
 - **Lectura/escritura** (por defecto): los usuarios pueden modificar la configuración y realizar las operaciones que les permiten sus permisos de gestión.
 - **Solo lectura**: los usuarios solo pueden ver la configuración y las funciones. No pueden realizar ningún cambio ni llevar a cabo ninguna operación en el Grid Manager o la Grid Management API. 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 todos los ajustes y funciones seleccionados.

2. Selecciona uno o varios ["Permisos del grupo admin"](#).

Debes asignar al menos un permiso a cada grupo; de lo contrario, los usuarios que pertenezcan al grupo no podrán iniciar sesión en StorageGRID.

3. Si vas a crear un grupo local, selecciona **Continuar**. Si vas a crear un grupo federado, selecciona **Crear grupo** y **Finalizar**.

Agregar usuarios (solo grupos locales)

Pasos

1. Si lo deseas, selecciona uno o más usuarios locales para este grupo.

Si aún no has creado usuarios locales, puedes guardar el grupo sin añadir usuarios. Puedes añadir este grupo al usuario en la página «Usuarios». Consulta ["Gestiona usuarios"](#) para obtener más información.

2. Selecciona **Crear grupo** y **Finalizar**.

Ver y editar grupos de administradores

Puedes consultar los detalles de los grupos existentes, modificar un grupo o duplicar un grupo.

- Para consultar la información básica de todos los grupos, revisa la tabla de la página «Grupos».
- Para ver todos los detalles de un grupo concreto o para editar un grupo, usa el menú **Actions** o la página de detalles.

Tarea	Menú de acciones	Página de detalles
Ver detalles del grupo	a. Selecciona la casilla para el grupo. b. Selecciona Acciones > Ver detalles del grupo .	Selecciona el nombre del grupo en la tabla.

Tarea	Menú de acciones	Página de detalles
Editar nombre para mostrar (solo grupos locales)	a. Selecciona la casilla para el grupo. b. Selecciona Acciones > Editar nombre del grupo . c. Introduce el nuevo nombre. d. Selecciona Guardar cambios .	a. Selecciona el nombre del grupo para ver los detalles. b. Selecciona el icono de edición  . c. Introduce el nuevo nombre. d. Selecciona Guardar cambios .
Editar el modo de acceso o los permisos	a. Selecciona la casilla para el grupo. b. Selecciona Acciones > Ver detalles del grupo . c. Opcionalmente, cambia el modo de acceso del grupo. d. Opcionalmente, selecciona o desmarca " Permisos del grupo admin ". e. Selecciona Guardar cambios .	a. Selecciona el nombre del grupo para ver los detalles. b. Opcionalmente, cambia el modo de acceso del grupo. c. Opcionalmente, selecciona o desmarca " Permisos del grupo admin ". d. Selecciona Guardar cambios .

Duplicar un grupo

Pasos

1. Selecciona la casilla para el grupo.
2. Selecciona **Acciones > Duplicar grupo**.
3. Completa el asistente para duplicar grupos.

Borrar un grupo

Puedes eliminar un grupo de administradores cuando quieras quitar el grupo del sistema y eliminar todos los permisos asociados con el grupo. Al eliminar un grupo de administradores, se eliminan los usuarios del grupo, pero no se eliminan los usuarios.

Pasos

1. En la página «Grupos», marca la casilla correspondiente a cada grupo que quieras eliminar.
2. Selecciona **Acciones > Eliminar grupo**.
3. Selecciona **Eliminar grupos**.

Permisos del grupo Admin en StorageGRID

Al crear grupos de usuarios administradores, seleccionas uno o varios permisos para controlar el acceso a funciones específicas de Grid Manager. Luego, puedes asignar a cada usuario a uno o varios de estos grupos de administradores para determinar qué tareas puede realizar ese usuario.

Debes asignar al menos un permiso a cada grupo; de lo contrario, los usuarios que pertenezcan a ese grupo no podrán iniciar sesión en Grid Manager ni en la Grid Management API.

De forma predeterminada, cualquier usuario que pertenezca a un grupo que tenga al menos un permiso puede realizar las siguientes tareas:

- Inicia sesión en Grid Manager
- Ver el panel de control
- Ver las páginas de Nodes
- Ver alertas actuales y resueltas
- Cambiar su propia contraseña (solo usuarios locales)
- Ver determinada información que aparece en las páginas de Configuración y Mantenimiento

Interacción entre los permisos y el modo de acceso

Para todos los permisos, la configuración del **modo de acceso** del grupo determina si los usuarios pueden cambiar los ajustes y realizar operaciones o si solo pueden ver los ajustes y funciones relacionados. Si un usuario pertenece a varios grupos y cualquier grupo está configurado como **solo lectura**, el usuario tendrá acceso de solo lectura a todos los ajustes y funciones seleccionados.

En los apartados siguientes se describen los permisos que puedes asignar al crear o editar un grupo de administradores. Cualquier funcionalidad que no se mencione explícitamente requiere el permiso **Root access**.

Acceso a raíz

Este permiso permite acceder a todas las funciones de administración de grid.

Cambiar la contraseña de root del inquilino

Este permiso proporciona acceso a la opción **Cambiar contraseña de root** en la página Tenants, lo que te permite controlar quién puede cambiar la contraseña del usuario raíz local del tenant. Este permiso también se utiliza para migrar claves S3 cuando la función de importación de claves S3 está habilitada. Los usuarios que no tengan este permiso no pueden ver la opción **Cambiar contraseña de root**.



Para conceder acceso a la página Tenants, que contiene la opción **Change root password**, asigna también el permiso **Tenant accounts**.

ILM

Este permiso permite acceder a las siguientes opciones del menú **ILM**:

- Reglas
- Políticas
- Etiquetas de políticas
- Grupos de almacenamiento
- Grados de almacenamiento
- Regiones
- Búsqueda de metadatos de objetos



Los usuarios deben tener el permiso **Other grid configuration** para gestionar los grados de almacenamiento.

Mantenimiento

Los usuarios deben tener el permiso de Mantenimiento para usar estas opciones:

- **Configuración > Control de acceso:**
 - Contraseñas de grid
- **Configuración > Red:**
 - Nombres de dominio de los endpoints S3
- **Mantenimiento > Tareas:**
 - Decomisionar
 - Expansión
 - Comprobación de la existencia de un objeto
 - Recuperación
- **Mantenimiento > Sistema:**
 - Paquete de recuperación
 - Actualización de software
- **Soporte > Herramientas:**
 - Registros

Los usuarios que no tengan el permiso de Maintenance pueden ver, pero no editar, estas páginas:

- **Mantenimiento > Red:**
 - Servidores DNS
 - Red de grid
 - Servidores NTP
- **Mantenimiento > Sistema:**
 - Licencia
- **Configuración > Red:**
 - Nombres de dominio de los endpoints S3
- **Configuración > Seguridad:**
 - Certificados
- **Configuración > Supervisión:**
 - Servidor de auditoría y syslog

Gestiona alertas

Este permiso proporciona acceso a las opciones para gestionar alertas. Los usuarios deben tener este permiso para gestionar silencios, notificaciones de alerta y reglas de alerta.

Consulta de métricas

Este permiso permite acceder a:

- **Soporte > Herramientas > Métricas** página

- Consultas personalizadas de métricas de Prometheus usando la sección **Metrics** de la Grid Management API
- Tarjetas del panel de control de Grid Manager que contienen métricas

Búsqueda de metadatos de objetos

Este permiso permite acceder a la página **ILM > Búsqueda de metadatos de objetos**.

Otra configuración de grid

Este permiso permite acceder a estas opciones adicionales de configuración de la red:

- **ILM:**
 - Grados de almacenamiento
- **Configuración > Sistema:**
- **Asistencia > Other:**
 - Coste del enlace

Administrador de almacenamiento

Este permiso proporciona lo siguiente:

- Acceso al E-Series SANtricity System Manager en los dispositivos de almacenamiento a través de Grid Manager.
- La posibilidad de realizar tareas de resolución de problemas y mantenimiento en la pestaña Manage drives para los dispositivos que admiten estas operaciones.

Cuentas de inquilinos

Este permiso permite:

- Accede a la página Tenants, donde puedes crear, editar y eliminar cuentas de tenant
- Ver las políticas de clasificación de tráfico existentes
- Ver las tarjetas del panel de Grid Manager que contienen los detalles de los inquilinos

Administra usuarios en StorageGRID

Puedes ver los usuarios locales y federados. También puedes crear usuarios locales y asignarlos a grupos de administradores locales para determinar a qué funciones de Grid Manager pueden acceder dichos usuarios.

Antes de empezar

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

Crear un usuario local

Puedes crear uno o varios usuarios locales y asignar cada usuario a uno o varios grupos locales. Los permisos del grupo controlan a qué funciones de Grid Manager y de Grid Management API puede acceder el usuario.

Solo puedes crear usuarios locales. Utiliza la fuente de identidades externa para gestionar usuarios y grupos federados.

El Grid Manager incluye un usuario local predefinido, llamado "root". No puedes eliminar el usuario raíz.



Si el inicio de sesión único (SSO) está activado, los usuarios locales no pueden iniciar sesión en StorageGRID.

Accede al asistente

Pasos

1. Selecciona **Configuración > Control de acceso > Usuarios administradores**.
2. Selecciona **Crear usuario**.

Introduce las credenciales de usuario

Pasos

1. Introduce el nombre completo del usuario, un nombre de usuario único y una contraseña.
2. Si lo deseas, selecciona **Sí** si este usuario no debe tener acceso a Grid Manager ni a Grid Management API.
3. Selecciona **Continuar**.

Asignar a grupos

Pasos

1. Si lo deseas, asigna al usuario a uno o varios grupos para determinar sus permisos.

Si aún no has creado ningún grupo, puedes guardar el usuario sin seleccionar grupos. Puedes añadir este usuario a un grupo en la página Grupos.

Si un usuario pertenece a varios grupos, los permisos son acumulativos. Consulta "[Gestiona grupos de administradores](#)" para ver los detalles.

2. Selecciona **Crear usuario** y selecciona **Finalizar**.

Ver y editar usuarios locales

Puedes consultar los detalles de los usuarios locales y federados existentes. Puedes modificar un usuario local para cambiar su nombre completo, contraseña o pertenencia a grupos. También puedes impedir temporalmente que un usuario acceda a Grid Manager y a la Grid Management API.

Solo puedes editar usuarios locales. Utiliza la fuente de identidades externa para gestionar usuarios federados.

- Para consultar la información básica de todos los usuarios locales y federados, revisa la tabla de la página Usuarios.
- Para ver todos los detalles de un usuario concreto, editar un usuario local o cambiar la contraseña de un usuario local, utiliza el menú **Acciones** o la página de detalles.

Cualquier cambio se aplica la próxima vez que el usuario cierre sesión y vuelva a iniciar sesión en Grid Manager.



Los usuarios locales pueden cambiar sus propias contraseñas mediante la opción **Cambiar contraseña** del banner de Grid Manager.

Tarea	Menú de acciones	Página de detalles
Ver los datos del usuario	a. Marca la casilla de selección para el usuario. b. Selecciona Acciones > Ver detalles del usuario.	Selecciona el nombre del usuario en la tabla.
Editar nombre completo (solo usuarios locales)	a. Marca la casilla de selección para el usuario. b. Selecciona Acciones > Editar nombre completo. c. Introduce el nuevo nombre. d. Selecciona Guardar cambios.	a. Selecciona el nombre del usuario para ver los detalles. b. Selecciona el icono de edición . c. Introduce el nuevo nombre. d. Selecciona Guardar cambios.
Denegar o permitir el acceso a StorageGRID	a. Marca la casilla de selección para el usuario. b. Selecciona Acciones > Ver detalles del usuario. c. Selecciona la pestaña Acceso. d. Selecciona Sí para impedir que el usuario inicie sesión en Grid Manager o en la Grid Management API, o selecciona No para permitirle iniciar sesión. e. Selecciona Guardar cambios.	a. Selecciona el nombre del usuario para ver los detalles. b. Selecciona la pestaña Acceso. c. Selecciona Sí para impedir que el usuario inicie sesión en Grid Manager o en la Grid Management API, o selecciona No para permitirle iniciar sesión. d. Selecciona Guardar cambios.
Cambiar contraseña (solo usuarios locales)	a. Marca la casilla de selección para el usuario. b. Selecciona Acciones > Ver detalles del usuario. c. Selecciona la pestaña «Contraseña». d. Introduce una nueva contraseña. e. Selecciona Cambiar contraseña.	a. Selecciona el nombre del usuario para ver los detalles. b. Selecciona la pestaña «Contraseña». c. Introduce una nueva contraseña. d. Selecciona Cambiar contraseña.

Tarea	Menú de acciones	Página de detalles
Cambiar grupos (solo usuarios locales)	a. Marca la casilla de selección para el usuario. b. Selecciona Acciones > Ver detalles del usuario . c. Selecciona la pestaña Grupos. d. Si lo deseas, selecciona el enlace que aparece junto al nombre de un grupo para ver los detalles del grupo en una nueva pestaña del navegador. e. Selecciona Editar grupos para elegir diferentes grupos. f. Selecciona Guardar cambios .	a. Selecciona el nombre del usuario para ver los detalles. b. Selecciona la pestaña Grupos. c. Si lo deseas, selecciona el enlace que aparece junto al nombre de un grupo para ver los detalles del grupo en una nueva pestaña del navegador. d. Selecciona Editar grupos para elegir diferentes grupos. e. Selecciona Guardar cambios .

Importar usuarios federados

Puedes importar uno o varios usuarios federados, hasta un máximo de 100 usuarios, directamente en la página de Usuarios.

Pasos

1. Selecciona **Configuración > Control de acceso > Usuarios administradores**.
2. Selecciona **Importar usuarios federados**.
3. Introduce el UUID o el nombre de usuario de uno o varios usuarios federados.

Si hay varias entradas, añade cada UUID o nombre de usuario en una nueva línea.

4. Selecciona **Importar**.

Si la importación al campo «Usuarios» falla para uno o varios usuarios, realiza los siguientes pasos:

- a. Despliega **Usuarios no importados** y selecciona **Copiar usuarios**.
- b. Vuelve a intentar la importación seleccionando **Anterior** y pegando los usuarios copiados en el cuadro de diálogo **Import federated users**.

Después de que cierres el cuadro de diálogo **Importar usuarios federados**, la información de los usuarios federados importados correctamente se muestra en la página Usuarios.

Duplicar un usuario

Puedes duplicar un usuario existente para crear un usuario nuevo con los mismos permisos.

Pasos

1. Marca la casilla de selección para el usuario.
2. Selecciona **Acciones > Duplicar usuario**.
3. Completa el asistente para duplicar usuarios.

Eliminar un usuario

Puedes eliminar un usuario local para borrarlo definitivamente del sistema.



No puedes eliminar el usuario raíz.

Pasos

1. En la página «Usuarios», marca la casilla correspondiente a cada usuario que quieras eliminar.
2. Selecciona **Acciones** > **Eliminar usuario**.
3. Selecciona **Eliminar usuario**.

Utiliza el inicio de sesión único (SSO)

Conoce StorageGRID SSO

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 tu organización. Los usuarios locales no pueden iniciar sesión en StorageGRID.

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), revisa cómo se ven afectados los procesos de inicio y cierre de sesión de StorageGRID cuando se habilita el SSO.

Inicia sesión cuando el inicio de sesión único está habilitado

Cuando el SSO está activado y te conectas a StorageGRID, se te redirige a la página de SSO de tu organización para validar tus credenciales.

Pasos

1. Introduce 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 accedes a la URL desde este navegador, se te pedirá que introduzcas un ID de cuenta.
- Si ya has accedido anteriormente al Grid Manager o al Tenant Manager, se te pedirá que selecciones una cuenta reciente o que introduzcas un ID de cuenta.



La página de inicio de sesión de StorageGRID no aparece cuando introduces la URL completa de una cuenta de inquilino (es decir, un dominio completo o una dirección IP seguida de `?accountId=20-digit-account-id`). En su lugar, te redirigen inmediatamente a la página de inicio de sesión único (SSO) de tu organización, donde puedes [inicia sesión con tus credenciales de SSO](#).

2. Indica si deseas acceder al Grid Manager o al Tenant Manager:

- Para acceder al Grid Manager, deja en blanco el campo **ID de cuenta**, introduce **0** como ID de cuenta o selecciona **Grid Manager** si aparece en la lista de cuentas recientes.
- Para acceder al Gestor de inquilinos, introduce el ID de cuenta del inquilino de 20 dígitos o selecciona un inquilino por su nombre si aparece en la lista de cuentas recientes.

3. Selecciona **Sign in**

StorageGRID te redirige a la página de inicio de sesión único (SSO) de tu organización. Por ejemplo:

4. Inicia sesión con tus credenciales de SSO.

Si tus 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 perteneces a un grupo federado con permisos de acceso a StorageGRID, has iniciado sesión en Grid Manager o en Tenant Manager, dependiendo de la cuenta que hayas seleccionado.



Si no se puede acceder a la cuenta de servicio, aún puedes iniciar sesión, siempre y cuando seas un usuario existente que pertenezca a un grupo federado con permisos de acceso a StorageGRID.

5. Si lo deseas, accede a otros nodos de administración o accede al Grid Manager o al Tenant Manager, si tienes los permisos adecuados.

No es necesario que vuelvas a introducir tus credenciales de SSO.

Cerrar sesión cuando el SSO está activado

Cuando el SSO está habilitado para StorageGRID, lo que ocurre al cerrar sesión depende de en qué hayas iniciado sesión y desde dónde la cierres.

Pasos

- Busca el enlace **Cerrar sesión** en la esquina superior derecha de la interfaz de usuario.
- Selecciona **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, así puedes acceder a estas interfaces de usuario más rápido en el futuro.



La tabla resume lo que ocurre al cerrar sesión si estás usando una sola sesión del navegador. Si has iniciado sesión en StorageGRID en varias sesiones del navegador, debes cerrar sesión en todas ellas por separado.

Si has iniciado sesión en...	Y cierras sesión en...	Se te ha desconectado de...
Grid Manager en uno o varios nodos de administración	Grid Manager en cualquier nodo de administración	Grid Manager en todos los nodos de administración Nota: Si utilizas Entra ID para el inicio de sesión único, es posible que tardes unos minutos en cerrar sesión en todos los nodos de administración.
Tenant Manager en uno o varios nodos de administración	Tenant Manager en cualquier nodo de administración	Tenant Manager en todos los nodos de administración
Tanto Grid Manager como Tenant Manager	Grid Manager	Solo el Grid Manager. También debes cerrar la sesión en el Tenant Manager para cerrar la sesión de inicio de sesión único.

Requisitos y consideraciones para StorageGRID SSO

Antes de habilitar el inicio de sesión único (SSO) para un sistema StorageGRID, revisa los requisitos y consideraciones.

Requisitos del proveedor de identidad

StorageGRID es compatible con los siguientes proveedores de identidad (IdP) de SSO:

- Servicio de federación de Active Directory (AD FS)
- Microsoft Entra ID
- PingFederate

Debes configurar la federación de identidades para tu sistema StorageGRID antes de poder configurar un proveedor de identidades de SSO. El tipo de servicio LDAP que utilices para la federación de identidades controla qué tipo de SSO puedes implementar.

Tipo de servicio LDAP configurado	Opciones para el proveedor de identidad de SSO
Active Directory	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

Requisitos de AD FS

Puedes utilizar cualquiera de las siguientes versiones de AD FS:

- Windows Server 2022 AD FS

- Windows Server 2019 AD FS
- Windows Server 2016 AD FS



Windows Server 2016 debería estar usando el ["Actualización KB3201845"](#), o una versión superior.

Requisitos adicionales

- Transport Layer Security (TLS) 1.2 o 1.3
- Microsoft .NET Framework, versión 3.5.1 o superior

Aspectos a tener en cuenta sobre Entra ID

Si utilizas Entra ID como tipo de SSO y los usuarios tienen nombres principales de usuario que no usan sAMAccountName como prefijo, pueden ocurrir problemas de inicio de sesión si StorageGRID pierde la conexión con el servidor LDAP. Para permitir que los usuarios inicien sesión, debes restablecer la conexión con el servidor LDAP.

Requisitos del certificado del servidor

De forma predeterminada, StorageGRID utiliza un certificado de interfaz de gestión en cada nodo de administración para proteger el acceso a Grid Manager, Tenant Manager, la Grid Management API y la Tenant Management API. Cuando configuras relaciones de confianza con partes de confianza (AD FS), aplicaciones empresariales (Entra ID) o conexiones de proveedor de servicios (PingFederate) para StorageGRID, utilizas el certificado de servidor como certificado de firma para las solicitudes de StorageGRID.

Si aún no has ["he configurado un certificado personalizado para la interfaz de gestión"](#), deberías hacerlo ahora. Cuando instalas un certificado de servidor personalizado, este se utiliza para todos los Admin Nodes, y puedes usarlo en todas las relying party trusts de StorageGRID, aplicaciones empresariales o conexiones SP.



No se recomienda utilizar el certificado de servidor predeterminado de un nodo de administración en una relación de confianza de parte confiable, una aplicación empresarial o una conexión SP. Si el nodo falla y lo recuperas, se genera un nuevo certificado de servidor predeterminado. Antes de poder iniciar sesión en el nodo recuperado, debes actualizar la relación de confianza de parte confiable, la aplicación empresarial o la conexión SP con el nuevo certificado.

Puedes acceder al certificado de servidor de un Admin Node iniciando sesión en la línea de comandos del nodo y yendo al directorio `/var/local/mgmt-api`. Un certificado de servidor personalizado se llama `custom-server.crt`. El certificado de servidor predeterminado del nodo se llama `server.crt`.

Requisitos de puertos

El inicio de sesión único (SSO) no está disponible en los puertos restringidos de Grid Manager o Tenant Manager. Debes utilizar el puerto HTTPS predeterminado (443) si deseas que los usuarios se autenticuen mediante el inicio de sesión único. Consulta ["Controla el acceso en el cortafuegos externo"](#).

Comprueba que los usuarios federados puedan iniciar sesión en StorageGRID

Antes de habilitar el inicio de sesión único (SSO), debes comprobar 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

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).
- Ya has configurado la federación de identidades.

Pasos

1. Si ya existen cuentas de inquilinos, comprueba que ninguno de los inquilinos esté usando su propia fuente de identidad.



Cuando habilitas el SSO, el origen de identidad configurado en el Tenant Manager se sustituye por el origen de identidad configurado en el Grid Manager. Los usuarios que pertenecen al origen de identidad del inquilino ya no podrán iniciar sesión a menos que tengan una cuenta en el origen de identidad del Grid Manager.

- a. Inicia sesión en Tenant Manager con cada cuenta de inquilino.
 - b. Selecciona **Gestión de acceso > Federación de identidades**.
 - c. Comprueba que la casilla **Habilitar federación de identidades** no esté marcada.
 - d. Si es así, comprueba que ya no se necesiten los grupos federados que puedan estar en uso para esta cuenta de inquilino, desmarca la casilla de selección y selecciona **Guardar**.
2. Comprueba que un usuario federado pueda acceder al Grid Manager:
 - a. En Grid Manager, selecciona **Configuración > Control de acceso > Grupos de administradores**.
 - b. Asegúrate de que se haya importado al menos un grupo federado desde la fuente de identidades de Active Directory y de que se le haya asignado el permiso de acceso Root.
 - c. Cerrar sesión.
 - d. Confirma que puedes volver a iniciar sesión en Grid Manager como usuario del grupo federado.
 3. Si ya existen cuentas de inquilinos, confirma que un usuario federado con permiso de acceso de usuario raíz pueda iniciar sesión:
 - a. Desde el Grid Manager, selecciona **Tenants**.
 - b. Selecciona la cuenta del inquilino y selecciona **Acciones > Editar**.
 - c. En la pestaña «Introducir datos», selecciona **Continuar**.
 - d. Si la casilla **Usar fuente de identidad propia** está marcada, desmárcala y selecciona **Guardar**.

Aparece la página Tenant.

 - e. Selecciona la cuenta de inquilino, selecciona **Sign in** e inicia sesión en la cuenta de inquilino como usuario raíz local.
 - f. En Tenant Manager, selecciona **Gestión de accesos > Grupos**.
 - g. Asegúrate de que al menos un grupo federado del Grid Manager tenga asignado el permiso de acceso raíz para este inquilino.
 - h. Cerrar sesión.
 - i. Confirma que puedes volver a iniciar sesión en el inquilino como usuario del grupo federado.

Información relacionada

- ["Requisitos y aspectos a tener en cuenta para el inicio de sesión único"](#)

- ["Gestiona grupos de administradores"](#)
- ["Utiliza una cuenta de inquilino"](#)

Configura el inicio de sesión único en StorageGRID

Puedes seguir el asistente Configurar SSO y entrar en el modo sandbox para configurar y probar el inicio de sesión único (SSO) antes de habilitarlo para todos los usuarios de StorageGRID. Después de habilitar el SSO, puedes volver al modo sandbox cuando lo necesites para cambiar o volver a probar la configuración.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).
- Has configurado la federación de identidades para tu sistema StorageGRID.
- Para la federación de identidades **tipo de servicio LDAP**, seleccionaste Active Directory o Entra ID, según el proveedor de identidades SSO que planeas usar.

Tipo de servicio LDAP configurado	Opciones para el proveedor de identidad de SSO
Servicio de federación de Active Directory (AD FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

Acerca de esta tarea

Cuando el SSO está habilitado y un usuario intenta iniciar sesión en un nodo de administración, StorageGRID envía una solicitud de autenticación al proveedor de identidad del SSO. A su vez, el proveedor de identidad del 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 Entra ID incluye un nombre principal de usuario (UPN).

Para que StorageGRID (el proveedor de servicios) y el proveedor de identidad SSO puedan comunicarse de forma segura sobre las solicitudes de autenticación de los usuarios, deberás realizar estas tareas:

1. Configura los ajustes en StorageGRID.
2. Utiliza el software del proveedor de identidad de SSO para crear una confianza de parte confiable (AD FS), una aplicación empresarial (Entra ID) o un proveedor de servicios (PingFederate) para cada Admin Node.
3. Vuelve a StorageGRID para activar el inicio de sesión único.

El modo sandbox facilita realizar esta configuración iterativa y probar todos los ajustes antes de habilitar SSO. Cuando usas el modo sandbox, los usuarios no pueden iniciar sesión mediante SSO.

Accede al asistente

Pasos

1. Selecciona **Configuración > Control de acceso > Inicio de sesión único**. Aparece la página de inicio de sesión único.



Si el botón «Configurar ajustes de SSO» aparece desactivado, comprueba que hayas configurado el proveedor de identidad como fuente de identidad federada. Consulta ["Requisitos y aspectos a tener en cuenta para el inicio de sesión único"](#).

2. Selecciona **Configurar ajustes de SSO**. Aparece la página «Proporcionar datos del proveedor de identidad».

Facilita los datos del proveedor de identidad

Pasos

1. Selecciona el **tipo de SSO** en la lista desplegable.
2. Si has seleccionado Active Directory como tipo de SSO, introduce el **nombre del servicio de federación** del proveedor de identidad, tal y como aparece en el Servicio de federación de Active Directory (AD FS).



Para localizar el nombre del servicio de federación, ve al Administrador de servidores de Windows Server. Selecciona **Herramientas > Administración de AD FS**. En el menú Acción, selecciona **Editar propiedades del servicio de federación**. El nombre del servicio de federación aparece en el segundo campo.

3. Especifica qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe la información de configuración de inicio de sesión único en respuesta a las solicitudes de StorageGRID.
 - **Utilizar el certificado de CA del sistema operativo:** Utiliza el certificado de CA predeterminado instalado en el sistema operativo para proteger la conexión.
 - **Utilizar un certificado de CA personalizado:** Utiliza un certificado de CA personalizado para proteger la conexión.

Si seleccionas esta opción, copia el texto del certificado personalizado y pégalo en el cuadro de texto **Certificado de la CA**.

 - **No utilices TLS:** No utilices un certificado TLS para proteger la conexión.



Si cambias el certificado de la CA, ["Reinicia el servicio mgmt-api en los nodos de administración"](#) y prueba que el inicio de sesión único en Grid Manager funciona correctamente.

4. Selecciona **Continuar**. Aparece la página Proporcionar identificador de la parte confiable.

Proporciona el identificador de la parte que confía

1. Rellena los campos de la página Proporcionar el identificador de la parte que confía según el tipo de SSO que seleccionaste.

Active Directory

- a. Especifica el **identificador de la parte de confianza** para StorageGRID. Este valor controla el nombre que usas para cada relación de confianza con una parte de confianza en AD FS.
 - Por ejemplo, si tu grid solo tiene un Admin Node y no tienes previsto añadir más Admin Nodes en el futuro, introduce SG o StorageGRID.
 - Si tu grid incluye más de un Admin Node, incluye la cadena [HOSTNAME] en el identificador. Por ejemplo, SG-[HOSTNAME]. Incluir esta cadena da como resultado una tabla que muestra el identificador de la relying party para cada Admin Node en el grid, basado en el hostname del nodo.



Debes crear una relación de confianza de parte confiable para cada Admin Node en tu sistema StorageGRID. Contar con una relación de confianza de parte confiable para cada Admin Node garantiza que los usuarios puedan iniciar sesión y cerrar sesión de forma segura en cualquier Admin Node.

- b. Selecciona **Guardar y entrar en modo sandbox**.

Entra ID

- a. En la sección «Aplicación empresarial», especifica el **nombre de la aplicación empresarial** para StorageGRID. Este valor controla el nombre que usas para cada aplicación empresarial en Entra ID.
 - Por ejemplo, si tu grid solo tiene un Admin Node y no tienes previsto añadir más Admin Nodes en el futuro, introduce SG o StorageGRID.
 - Si tu grid incluye más de un Admin Node, incluye la cadena [HOSTNAME] en el identificador. Por ejemplo, SG-[HOSTNAME]. Incluir esta cadena da como resultado una tabla que muestra un nombre de aplicación empresarial para cada Admin Node en tu sistema, basado en el hostname del nodo.



Debes crear una aplicación empresarial para cada nodo de administración de tu sistema StorageGRID. Contar con una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar sesión y cerrar sesión de forma segura en cualquier nodo de administración.

- b. Sigue los pasos en "[Crear aplicaciones empresariales en Entra ID](#)" para crear una aplicación empresarial para cada Admin Node que aparece en la tabla.
- c. En Entra ID, copia la URL de metadatos de federación de cada aplicación empresarial. Luego, pega esta URL en el campo correspondiente **Federation metadata URL** en StorageGRID.
- d. Una vez que hayas copiado y pegado una URL de metadatos de federación para todos los nodos de administración, selecciona **Guardar y entrar en modo sandbox**.

PingFederate

- a. En la sección SP (Proveedor de servicios), especifica el **SP connection ID** para StorageGRID. Este valor controla el nombre que usas para cada conexión de SP en PingFederate.
 - Por ejemplo, si tu grid solo tiene un Admin Node y no tienes previsto añadir más Admin Nodes en el futuro, introduce SG o StorageGRID.
 - Si tu grid incluye más de un Admin Node, incluye la cadena [HOSTNAME] en el identificador. Por ejemplo, SG-[HOSTNAME]. Incluir esta cadena da como resultado una tabla que muestra

el ID de conexión SP de cada Admin Node en tu sistema, según el hostname del nodo.



Debes crear una conexión SP para cada nodo de administración de tu sistema StorageGRID. Disponer de 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.

- b. Indica la URL de los metadatos de la federación para cada Admin Node en el campo **Federation metadata URL**.

Utiliza el siguiente formato:

```
https://<Federation Service  
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP  
Connection ID>
```

- c. Selecciona **Guardar y entrar en modo sandbox**.

Configura relaciones de confianza de terceros, aplicaciones empresariales o conexiones SP

Después de guardar la configuración y entrar en el modo de prueba, puedes completar y probar la configuración para el tipo de SSO que seleccionaste.

StorageGRID puede permanecer en modo «sandbox» todo el tiempo que sea necesario. Sin embargo, solo pueden iniciar sesión los usuarios federados y los usuarios locales.

Active Directory

Pasos

1. Ve a Servicios de federación de Active Directory (AD FS).
2. Crea una o varias relaciones de confianza con las partes confiables para StorageGRID, usando cada identificador de parte confiable que aparece en la tabla de la página Configurar SSO.

Debes crear un trust para cada Admin Node que aparece en la tabla.

Para obtener instrucciones, visita ["Crear relaciones de confianza de terceros en AD FS"](#).

Entra ID

Pasos

1. En la página de inicio de sesión único del Admin Node en el que has iniciado sesión actualmente, selecciona el botón para descargar y guardar los metadatos SAML.
2. Luego, para cualquier otro nodo de administración en tu grid, repite estos pasos:
 - a. Inicia sesión en el nodo.
 - b. Selecciona **Configuración > Control de acceso > inicio de sesión único**.
 - c. Descarga y guarda los metadatos SAML de ese nodo.
3. Accede al portal de Azure.
4. Sigue los pasos en ["Crear aplicaciones empresariales en Entra ID"](#) para cargar el archivo de metadatos SAML de cada Admin Node en su aplicación empresarial de Entra ID correspondiente.

PingFederate

Pasos

1. En la página de inicio de sesión único del Admin Node en el que has iniciado sesión actualmente, selecciona el botón para descargar y guardar los metadatos SAML.
2. Luego, para cualquier otro nodo de administración en tu grid, repite estos pasos:
 - a. Inicia sesión en el nodo.
 - b. Selecciona **Configuración > Control de acceso > inicio de sesión único**.
 - c. Descarga y guarda los metadatos SAML de ese nodo.
3. Entra en PingFederate.
4. ["Crea una o varias conexiones de proveedor de servicios \(SP\) para StorageGRID"](#). Utiliza el ID de conexión SP de cada nodo de administración (que aparece en la tabla de la página Configurar SSO) y los metadatos SAML que descargaste para ese nodo de administración.

Debes crear una conexión SP para cada nodo de administración que aparece en la tabla.

Configuración de prueba

Antes de aplicar el inicio de sesión único en todo tu sistema StorageGRID, comprueba que el inicio de sesión único y el cierre de sesión único estén correctamente configurados en cada Admin Node.

Active Directory

Pasos

1. En la página Configurar SSO, busca el enlace en el paso Probar la configuración del asistente.

La URL se deriva del valor que has introducido en el campo **Federation service name**.

2. Selecciona el enlace o copia y pega la URL en un navegador para acceder a la página de inicio de sesión de tu proveedor de identidad.
3. Para confirmar que puedes utilizar el inicio de sesión único (SSO) para iniciar sesión en StorageGRID, selecciona **Sign in to one of the following sites**, selecciona el identificador de la parte de confianza correspondiente a tu nodo de administración principal y selecciona **Sign in**.
4. Introduce tu nombre de usuario y contraseña federados.
 - Si el inicio de sesión y el cierre de sesión mediante SSO se realizan correctamente, aparece un mensaje de éxito.
 - Si la operación de SSO no se realiza correctamente, aparece un mensaje de error. Soluciona el problema, borra las cookies del navegador e inténtalo de nuevo.
5. Repite estos pasos para comprobar la conexión de inicio de sesión único (SSO) de cada Admin Node en tu grid.

Entra ID

Pasos

1. Accede a la página de inicio de sesión único en el portal de Azure.
2. Selecciona **Probar esta aplicación**.
3. Introduce las credenciales de un usuario federado.
 - Si el inicio de sesión y el cierre de sesión mediante SSO se realizan correctamente, aparece un mensaje de éxito.
 - Si la operación de SSO no se realiza correctamente, aparece un mensaje de error. Soluciona el problema, borra las cookies del navegador e inténtalo de nuevo.
4. Repite estos pasos para comprobar la conexión de inicio de sesión único (SSO) de cada Admin Node en tu grid.

PingFederate

Pasos

1. En la página Configurar SSO, selecciona el primer enlace en el mensaje de modo Sandbox.

Selecciona y comprueba un enlace cada vez.

2. Introduce las credenciales de un usuario federado.
 - Si el inicio de sesión y el cierre de sesión mediante SSO se realizan correctamente, aparece un mensaje de éxito.
 - Si la operación de SSO no se realiza correctamente, aparece un mensaje de error. Soluciona el problema, borra las cookies del navegador e inténtalo de nuevo.
3. Selecciona el siguiente enlace para verificar la conexión de inicio de sesión único para cada Admin Node en tu grid.

Si aparece el mensaje «Página caducada», selecciona el botón **Atrás** de tu navegador y vuelve a

introducir tus credenciales.

Habilitar el inicio de sesión único

Cuando hayas comprobado que puedes usar el inicio de sesión único (SSO) para acceder a cada nodo de administración, puedes habilitar el inicio de sesión único para todo tu sistema StorageGRID.



Cuando el SSO está habilitado, todos los usuarios deben usar el SSO para acceder al Grid Manager, al Tenant Manager, a la Grid Management API y a la Tenant Management API. Los usuarios locales ya no pueden acceder a StorageGRID.

Pasos

1. En el paso «Configuración de la prueba» del asistente de configuración de SSO, selecciona **Enable SSO**.
2. Lee el mensaje de advertencia y selecciona **Enable SSO**.

El inicio de sesión único ya está activado. Aparece la página de inicio de sesión único y ahora incluye los detalles del SSO que acabas de configurar.

3. Para editar la configuración, selecciona **Editar**.
4. Para desactivar el inicio de sesión único, selecciona **Desactivar SSO**.



Si utilizas el Portal de Azure y accedes a StorageGRID desde el mismo ordenador que usas para acceder a Entra ID, asegúrate de que el usuario del Portal de Azure también sea un usuario autorizado de StorageGRID (un usuario de un grupo federado que se haya importado a StorageGRID) o cierra la sesión del Portal de Azure antes de intentar iniciar sesión en StorageGRID.

Crea confianzas de terceros en AD FS para StorageGRID

Debes utilizar los Servicios de federación de Active Directory (AD FS) para crear una relación de confianza de parte confiable para cada nodo de administración de tu sistema. Puedes crear relaciones de confianza de parte confiable usando comandos de PowerShell, importando metadatos SAML desde StorageGRID o introduciendo los datos manualmente.

Antes de empezar

- Has configurado el inicio de sesión único para StorageGRID y seleccionaste **AD FS** como tipo de SSO.
- Tienes ["ha entrado en modo sandbox"](#) en Grid Manager.
- Conoces el nombre de dominio completo (o la dirección IP) y el identificador de la parte de confianza de cada nodo de administración en tu sistema. Puedes encontrar estos valores en la tabla de detalles de los nodos de administración en la página StorageGRID Configure SSO.



Debes crear una relación de confianza de parte confiable para cada Admin Node en tu sistema StorageGRID. Contar con una relación de confianza de parte confiable para cada Admin Node garantiza que los usuarios puedan iniciar sesión y cerrar sesión de forma segura en cualquier Admin Node.

- Tienes experiencia en la creación de relaciones de confianza entre partes en AD FS, o tienes acceso a la

documentación de Microsoft AD FS.

- Estás utilizando el complemento de administración de AD FS y perteneces al grupo Administrators.
- Si vas a crear manualmente la relación de confianza con la parte confiable, tienes el certificado personalizado que se subió para la interfaz de gestión de StorageGRID, o sabes cómo iniciar sesión en un Admin Node desde la línea de comandos.

Acerca de esta tarea

Estas instrucciones se aplican a Windows Server 2016 AD FS. Si utilizas una versión diferente de AD FS, notarás ligeras diferencias en el procedimiento. Consulta la documentación de Microsoft AD FS si tienes preguntas.

Crea una relación de confianza de parte confiable usando Windows PowerShell

Puedes usar Windows PowerShell para crear rápidamente una o más relaciones de confianza con la parte de confianza.

Pasos

1. En el menú de inicio de Windows, haz clic con el botón derecho en el icono de PowerShell y selecciona **Ejecutar como administrador**.
2. En el símbolo del sistema de PowerShell, introduce el siguiente comando:

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL  
"https://Admin_Node_FQDN/api/saml-metadata"
```

- Para *Admin_Node_Identifier*, introduce el identificador de la parte de confianza para el Admin Node, exactamente como aparece en la página de inicio de sesión único. Por ejemplo, SG-DC1-ADM1.
- Para *Admin_Node_FQDN*, introduce el nombre de dominio completo para ese mismo nodo de administración. (Si es necesario, puedes usar la dirección IP del nodo en su lugar. Sin embargo, si introduces aquí una dirección IP, ten en cuenta que deberás actualizar o volver a crear esta relación de confianza entre partes si esa dirección IP llega a cambiar.)

3. En el Administrador de servidores de Windows Server, selecciona **Herramientas > Administración de AD FS**.

Aparece la herramienta de gestión de AD FS.

4. Selecciona **AD FS > Relying Party Trusts**.

Aparece la lista de relaciones de confianza de las partes que confían.

5. Añade una política de control de acceso a la relación de confianza de parte confiable recién creada:
 - a. Busca la confianza de la parte confiable que acabas de crear.
 - b. Haz clic con el botón derecho del ratón sobre la confianza y selecciona **Editar política de control de acceso**.
 - c. Selecciona una política de control de acceso.
 - d. Selecciona **Aplicar** y, a continuación, **OK**
6. Agrega una directiva de emisión de declaraciones a la nueva relación de confianza de la parte confiable:
 - a. Busca la confianza de la parte confiable que acabas de crear.
 - b. Haz clic con el botón derecho del ratón sobre la confianza y selecciona **Editar política de emisión de reclamaciones**.

- c. Selecciona **Add rule**.
- d. En la página «Seleccionar plantilla de regla», selecciona **Enviar atributos LDAP como reclamaciones** en la lista y selecciona **Siguiente**.
- e. En la página Configurar regla, introduce 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, selecciona **Active Directory**.
 - g. En la columna Atributo LDAP de la tabla de asignación, escribe **objectGUID** o selecciona **User-Principal-Name**.
 - h. En la columna Outgoing Claim Type de la tabla de correspondencias, selecciona **Name ID** en la lista desplegable.
 - i. Selecciona **Finalizar** y, a continuación, **OK**.
7. Comprueba que los metadatos se hayan importado correctamente.
 - a. Haz clic con el botón derecho del ratón sobre la confianza de la parte dependiente para abrir sus propiedades.
 - b. Comprueba que los campos de las pestañas **Puntos finales**, **Identificadores** y **Firma** estén rellenos.

Si faltan los metadatos, comprueba que la dirección de metadatos de la Federación sea correcta o introduce los valores manualmente.
 8. Repite estos pasos para configurar una relación de confianza de parte confiable para todos los nodos de administración en tu sistema StorageGRID.
 9. Cuando hayas terminado, vuelve a StorageGRID y "[probar todas las relaciones de confianza de las relying party](#)" para confirmar que están configurados correctamente.

Crea una relación de confianza con una parte confiable importando metadatos de federación

Puedes importar los valores de cada relación de confianza de la parte que confía accediendo a los metadatos SAML de cada Admin Node.

Pasos

1. En el Administrador de servidores de Windows Server, selecciona **Herramientas** y, a continuación, selecciona **Administración de AD FS**.
2. En Acciones, selecciona **Add Relying Party Trust**.
3. En la página de bienvenida, elige **Claims aware** y selecciona **Start**.
4. Selecciona **Importar datos sobre la parte de confianza publicados en línea o en una red local**.
5. En **Dirección de metadatos de la federación (nombre de host o URL)**, escribe la ubicación de los metadatos SAML de este nodo de administración:

`https://Admin_Node_FQDN/api/saml-metadata`

Para *Admin_Node_FQDN*, introduce el nombre de dominio completo para ese mismo nodo de administración. (Si es necesario, puedes usar la dirección IP del nodo en su lugar. Sin embargo, si introduces aquí una dirección IP, ten en cuenta que deberás actualizar o volver a crear esta relación de confianza entre partes si esa dirección IP llega a cambiar.)

6. Completa el asistente de confianza de parte dependiente, guarda la confianza de parte dependiente y cierra el asistente.



Al introducir el nombre para mostrar, utiliza el identificador de la parte de confianza del nodo de administración, exactamente como aparece en la página de inicio de sesión único de Grid Manager. Por ejemplo, SG-DC1-ADM1.

7. Agrega una regla de reclamación:
 - a. Haz clic con el botón derecho del ratón sobre la confianza y selecciona **Editar política de emisión de reclamaciones**.
 - b. Selecciona **Add rule**:
 - c. En la página «Seleccionar plantilla de regla», selecciona **Enviar atributos LDAP como reclamaciones** en la lista y selecciona **Siguiente**.
 - d. En la página Configurar regla, introduce 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, selecciona **Active Directory**.
 - f. En la columna Atributo LDAP de la tabla de asignación, escribe **objectGUID** o selecciona **User-Principal-Name**.
 - g. En la columna Outgoing Claim Type de la tabla de correspondencias, selecciona **Name ID** en la lista desplegable.
 - h. Selecciona **Finalizar** y, a continuación, **OK**.
8. Comprueba que los metadatos se hayan importado correctamente.
 - a. Haz clic con el botón derecho del ratón sobre la confianza de la parte dependiente para abrir sus propiedades.
 - b. Comprueba que los campos de las pestañas **Puntos finales**, **Identificadores** y **Firma** estén rellenos.

Si faltan los metadatos, comprueba que la dirección de metadatos de la Federación sea correcta o introduce los valores manualmente.
9. Repite estos pasos para configurar una relación de confianza de parte confiable para todos los nodos de administración en tu sistema StorageGRID.
10. Cuando hayas terminado, vuelve a StorageGRID y "[probar todas las relaciones de confianza de las relying party](#)" para comprobar que están configurados correctamente.

Crear una relación de confianza de parte confiable manualmente

Si decides no importar los datos de los relying part trusts, puedes introducir los valores manualmente.

Pasos

1. En el Administrador de servidores de Windows Server, selecciona **Herramientas** y, a continuación, selecciona **Administración de AD FS**.
2. En Acciones, selecciona **Add Relying Party Trust**.
3. En la página de bienvenida, elige **Claims aware** y selecciona **Start**.
4. Selecciona **Introducir manualmente los datos de la parte confiable** y selecciona **Siguiente**.

5. Completa el asistente de confianza de la parte que confía:

- a. Introduce un nombre para este nodo de administración.

Para garantizar la coherencia, utiliza el identificador de la parte de confianza del nodo de administración exactamente como aparece en la página de inicio de sesión único de Grid Manager. Por ejemplo, SG-DC1-ADM1.

- b. Omite el paso para configurar un certificado opcional de cifrado de tokens.

- c. En la página «Configurar URL», selecciona la casilla **Habilitar compatibilidad con el protocolo WebSSO de SAML 2.0**.

- d. Escribe la URL del punto final del servicio SAML para el nodo de administración:

`https://Admin_Node_FQDN/api/saml-response`

Para *Admin_Node_FQDN*, introduce el nombre de dominio completo para el Admin Node. (Si es necesario, puedes usar la dirección IP del nodo en su lugar. Sin embargo, si introduces una dirección IP aquí, ten en cuenta que deberás actualizar o volver a crear esta relying party trust si esa dirección IP cambia en algún momento.)

- e. En la página Configurar identificadores, especifica el Relying Party Identifier para el mismo Admin Node:

Admin_Node_Identifier

Para *Admin_Node_Identifier*, introduce el identificador de la parte de confianza para el Admin Node, exactamente como aparece en la página de inicio de sesión único. Por ejemplo, SG-DC1-ADM1.

- f. Revisa la configuración, guarda la confianza de la parte confiable y cierra el asistente.

Aparece el cuadro de diálogo «Edit Claim Issuance Policy».



Si no aparece el cuadro de diálogo, haz clic con el botón derecho sobre la relación de confianza y selecciona **Editar política de emisión de reclamaciones**.

6. Para iniciar el asistente de reglas de reclamación, selecciona **Add rule**:

- a. En la página «Seleccionar plantilla de regla», selecciona **Enviar atributos LDAP como reclamaciones** en la lista y selecciona **Siguiente**.

- b. En la página Configurar regla, introduce 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, selecciona **Active Directory**.

- d. En la columna Atributo LDAP de la tabla de asignación, escribe **objectGUID** o selecciona **User-Principal-Name**.

- e. En la columna Outgoing Claim Type de la tabla de correspondencias, selecciona **Name ID** en la lista desplegable.

- f. Selecciona **Finalizar** y, a continuación, **OK**.

7. Haz clic con el botón derecho del ratón sobre la confianza de la parte dependiente para abrir sus propiedades.

8. En la pestaña **Puntos finales**, configura el punto final para el cierre de sesión único (SLO):
 - a. Selecciona **Add SAML**.
 - b. Selecciona **Tipo de endpoint > Cierre de sesión SAML**.
 - c. Selecciona **Binding > Redirect**.
 - d. En el campo **URL de confianza**, introduce la URL utilizada para el cierre de sesión único (SLO) desde este Admin Node:

`https://Admin_Node_FQDN/api/saml-logout`

Para *Admin_Node_FQDN*, introduce el nombre de dominio completo del nodo de administración. (si es necesario, puedes usar la dirección IP del nodo en su lugar. Sin embargo, si introduces una dirección IP aquí, ten en cuenta que deberás actualizar o volver a crear esta relación de confianza entre partes si esa dirección IP cambia en algún momento).

- a. Selecciona **Aceptar**.
9. En la pestaña **Firma**, especifica el certificado de firma para esta relación de confianza de parte confiable:
 - a. Agrega el certificado personalizado:
 - Si dispones del certificado de gestión personalizado que has subido a StorageGRID, selecciona ese certificado.
 - Si no tienes el certificado personalizado, inicia sesión en el Admin Node, ve al directorio `/var/local/mgmt-api` del Admin Node y añade el archivo de certificado `custom-server.crt`.



No se recomienda utilizar el certificado predeterminado del nodo de administración (`server.crt`). Si el nodo de administración falla, el certificado predeterminado se volverá a generar al recuperar el nodo, y será necesario actualizar la confianza de la parte que confía.

- b. Selecciona **Aplicar** y selecciona **Aceptar**.

Se guardan y se cierran las propiedades de la parte que confía.

10. Repite estos pasos para configurar una relación de confianza de parte confiable para todos los nodos de administración en tu sistema StorageGRID.
11. Cuando hayas terminado, vuelve a StorageGRID y "[probar todas las relaciones de confianza de las relying party](#)" para comprobar que están configurados correctamente.

Crea aplicaciones empresariales en Entra ID para StorageGRID

Utiliza Entra ID para crear una aplicación empresarial para cada Admin Node en tu sistema.

Antes de empezar

- Has comenzado a configurar el inicio de sesión único para StorageGRID y seleccionaste **Entra ID** como tipo de SSO.
- Tienes "[ha entrado en modo sandbox](#)" en Grid Manager.
- Tienes el **nombre de la aplicación empresarial** para cada nodo de administración de tu sistema. Puedes copiar estos valores de la tabla de detalles del nodo de administración en la página Configurar SSO.



Debes crear una aplicación empresarial para cada nodo de administración de tu sistema StorageGRID. Contar con una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar sesión y cerrar sesión de forma segura en cualquier nodo de administración.

- Tienes experiencia creando aplicaciones empresariales en Entra ID.
- Tienes una cuenta de Entra ID con una suscripción activa.
- Tienes uno de los siguientes roles en la cuenta de Entra ID: Global Administrator, Cloud Application Administrator, Application Administrator o propietario del service principal.

Accede a Entra ID

Pasos

1. Inicia sesión en el "[Portal de Azure](#)".
2. Accede a "[Entra ID](#)".
3. Selecciona "[Aplicaciones empresariales](#)".

Crear aplicaciones empresariales y guardar la configuración de SSO de StorageGRID

Para guardar la configuración de SSO para Entra ID en StorageGRID, debes usar Entra ID para crear una aplicación empresarial para cada nodo de administración. Copiarás las URL de metadatos de federación de Entra ID y las pegarás en los campos correspondientes de **URL de metadatos de federación** en la página Configurar SSO.

Pasos

1. Repite los siguientes pasos para cada Admin Node.
 - a. En el panel de aplicaciones de Entra ID Enterprise, selecciona **New application**.
 - b. Selecciona **Crear tu propia aplicación**.
 - c. En el campo «Nombre», introduce el **nombre de la aplicación Enterprise** que copiaste de la tabla de detalles del nodo de administración en la página Configurar SSO.
 - d. Deja seleccionado el botón de opción **Integrar cualquier otra aplicación que no encuentres en la galería (fuera de la galería)**.
 - e. Selecciona **Crear**.
 - f. Selecciona el enlace **Empezar** en el recuadro **2. Configura el inicio de sesión único**, o selecciona el enlace **Inicio de sesión único** en el margen izquierdo.
 - g. Selecciona la casilla **SAML**.
 - h. Copia la **App Federation Metadata Url**, que puedes encontrar en **Step 3 SAML Signing Certificate**.
 - i. Ve a la página «Configurar SSO» y pega la URL en el campo **URL de metadatos de federación** que corresponde al **Enterprise application name** que usaste.
2. Una vez que hayas pegado la URL de metadatos de la federación para cada nodo de administración y hayas realizado todos los demás cambios necesarios en la configuración de SSO, selecciona **Guardar** en la página Configure SSO.

Descarga los metadatos SAML de cada nodo de administración

Una vez guardada la configuración de SSO, puedes descargar un archivo de metadatos SAML para cada nodo de administración en tu sistema StorageGRID.

Pasos

1. Repite estos pasos para cada Admin Node.
 - a. Inicia sesión en StorageGRID desde el nodo de administración.
 - b. Selecciona **Configuración > Control de acceso > inicio de sesión único**.
 - c. Pulsa el botón para descargar los metadatos SAML de ese nodo de administración.
 - d. Guarda el archivo, que luego subirás a Entra ID.

Sube los metadatos SAML a cada aplicación empresarial

Después de descargar un archivo de metadatos SAML para cada nodo de administración de StorageGRID, realiza los siguientes pasos en Entra ID:

Pasos

1. Vuelve al Portal de Azure.
2. Repite estos pasos para cada aplicación empresarial:



Es posible que tengas que actualizar la página de aplicaciones de Enterprise para ver en la lista las aplicaciones que añadiste anteriormente.

- a. Ve a la página Propiedades de la aplicación empresarial.
 - b. Establece **Asignación obligatoria** en **No** (a menos que quieras configurar las asignaciones por separado).
 - c. Accede a la página de inicio de sesión único.
 - d. Completa la configuración de SAML.
 - e. Pulsa el botón **Cargar archivo de metadatos** y selecciona el archivo de metadatos SAML que descargaste para el Admin Node correspondiente.
 - f. Una vez que se cargue el archivo, selecciona **Guardar** y luego selecciona **X** para cerrar el panel. Regresarás a la página Configurar el inicio de sesión único con SAML.
3. ["Prueba cada aplicación"](#).

Crea conexiones de proveedores de servicios en PingFederate para StorageGRID

Utilizas PingFederate para crear una conexión de proveedor de servicios (SP) para cada nodo de administración en tu sistema. Para agilizar el proceso, importarás los metadatos SAML desde StorageGRID.

Antes de empezar

- Has configurado el inicio de sesión único para StorageGRID y seleccionaste **Ping Federate** como tipo de SSO.
- Tienes ["ha entrado en modo sandbox"](#) en Grid Manager.
- Dispones del **ID de conexión SP** de cada nodo de administración de tu sistema. Puedes encontrar estos valores en la tabla de detalles de los nodos de administración en la página Configurar SSO.
- Has descargado los **metadatos SAML** de cada nodo de administración en tu sistema.
- Tienes experiencia creando conexiones de SP en PingFederate Server.
- Tienes el ["Guía de referencia para administradores"](#) para PingFederate Server. La documentación de

PingFederate ofrece instrucciones detalladas paso a paso y explicaciones.

- Tienes el "[Permiso de administrador](#)" para PingFederate Server.

Acerca de esta tarea

Estas instrucciones resumen cómo configurar PingFederate Server versión 10.3 como proveedor de SSO para StorageGRID. Si estás usando otra versión de PingFederate, puede que necesites adaptar estas instrucciones. Consulta la documentación de PingFederate Server para obtener instrucciones detalladas para tu versión.

Completa los requisitos previos en PingFederate

Antes de poder crear las conexiones SP que utilizarás para StorageGRID, debes completar las tareas previas en PingFederate. Utilizarás la información de estos requisitos previos cuando configures las conexiones SP.

Crear almacén de datos

Si aún no lo has hecho, crea un almacén de datos para conectar PingFederate al servidor LDAP de AD FS. Utiliza los valores que usaste al "[configuración de la federación de identidades](#)" en StorageGRID.

- **Tipo:** Directorio (LDAP)
- **Tipo de LDAP:** Active Directory
- **Nombre del atributo binario:** Introduce **objectGUID** en la pestaña de atributos binarios de LDAP exactamente como se muestra.

Crear un validador de credenciales de contraseña

Si aún no lo has hecho, crea un validador de credenciales de contraseña.

- **Tipo:** Validador de credenciales de nombre de usuario y contraseña LDAP
- **Almacén de datos:** Selecciona el almacén de datos que creaste.
- **Base de búsqueda:** Introduce información de LDAP (por ejemplo, DC=saml,DC=sgws).
- **Filtro de búsqueda:** sAMAccountName=\${username}
- **Ámbito:** Subárbol

Crear instancia del adaptador IdP

Si aún no lo has hecho, crea una instancia del adaptador IdP.

Pasos

1. Ve a **Autenticación > Integración > Adaptadores de IdP**.
2. Selecciona **Crear nueva instancia**.
3. En la pestaña Tipo, selecciona **HTML Form IdP Adapter**.
4. En la pestaña «Adaptador IdP», selecciona **Add a new row to 'Credential Validators'**.
5. Selecciona el [validador de credenciales de contraseña](#) que creaste.
6. En la pestaña «Atributos del adaptador», selecciona el atributo **username** para **Pseudonym**.
7. Selecciona **Guardar**.

Crear o importar un certificado de firma

Si aún no lo has hecho, crea o importa el certificado de firma.

Pasos

1. Ve a **Seguridad > Claves de firma y descifrado y certificados**.
2. Crea o importa el certificado de firma.

Crea una conexión de SP en PingFederate

Al crear una conexión SP en PingFederate, debes importar los metadatos SAML que descargaste de StorageGRID para el nodo de administración. El archivo de metadatos contiene muchos de los valores específicos que necesitas.



Debes crear una conexión de SP para cada nodo de administración en tu sistema StorageGRID, de modo que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo. Usa estas instrucciones para crear la primera conexión de SP. Luego, ve a [Crear conexiones SP adicionales](#) para crear las conexiones adicionales que necesites.

Selecciona el tipo de conexión SP

Pasos

1. Ve a **Aplicaciones > Integración > Conexiones SP**.
2. Selecciona **Crear conexión**.
3. Selecciona **No utilizar una plantilla para esta conexión**.
4. Selecciona **Perfiles de SSO del navegador y SAML 2.0** como el protocolo.

Importar metadatos de SP

Pasos

1. En la pestaña «Importar metadatos», selecciona **File**.
2. Selecciona el archivo de metadatos SAML que descargaste desde la página Configurar SSO para el nodo de administración.
3. Revisa el resumen de metadatos y la información que aparece en la pestaña General Info.

El ID de entidad del partner y el nombre de la conexión se establecen con el ID de conexión del SP de StorageGRID. (por ejemplo, 10.96.105.200-DC1-ADM1-105-200). La URL base es la dirección IP del nodo de administración de StorageGRID.

4. Selecciona **Siguiente**.

Configura el inicio de sesión único (SSO) del IdP en el navegador

Pasos

1. En la pestaña SSO del navegador, selecciona **Configurar SSO del navegador**.
2. En la pestaña «Perfiles SAML», selecciona las opciones **SSO iniciado por el SP**, **SLO iniciado por el SP**, **SSO iniciado por el IdP** y **SLO iniciado por el IdP**.
3. Selecciona **Siguiente**.
4. En la pestaña «Duración de la afirmación», no hagas ningún cambio.

5. En la pestaña «Creación de aserciones», selecciona **Configurar la creación de aserciones**.
 - a. En la pestaña Asignación de identidad, selecciona **Estándar**.
 - b. En la pestaña «Contrato de atributos», usa **SAML_SUBJECT** como contrato de atributos y el formato de nombre no especificado que se importó.
6. Para "Extend the Contract", selecciona **Eliminar** para quitar el `urn:oid`, que no se usa.

Instancia del adaptador de mapas

Pasos

1. En la pestaña «Asignación de fuentes de autenticación», selecciona **Asignar nueva instancia de adaptador**.
2. En la pestaña Adapter instance, selecciona el [instancia del adaptador](#) que creaste.
3. En la pestaña «Método de asignación», selecciona **Recuperar atributos adicionales de un almacén de datos**.
4. En la pestaña «Fuente de atributos y búsqueda de usuarios», selecciona **Add Attribute Source**.
5. En la pestaña Data Store, proporciona una descripción y selecciona el [almacén de datos](#) que añadiste.
6. En la pestaña «Búsqueda en el directorio LDAP»:
 - Introduce el **DN base**, que debe coincidir exactamente con el valor que has introducido en StorageGRID para el servidor LDAP.
 - Para el Search Scope, selecciona **Subtree**.
 - En la clase de objeto raíz, busca y añade cualquiera de estos atributos: **objectGUID** o **userPrincipalName**.
7. En la pestaña «Tipos de codificación de atributos binarios LDAP», selecciona **Base64** para el atributo **objectGUID**.
8. En la pestaña «Filtro LDAP», introduce **sAMAccountName=\${username}**.
9. En la pestaña «Cumplimiento del contrato de atributos», selecciona **LDAP (atributo)** en el menú desplegable «Origen» y selecciona **objectGUID** o **userPrincipalName** en el menú desplegable «Valor».
10. Revisa y luego guarda la fuente de atributos.
11. En la pestaña «Failsave Attribute Source», selecciona **Abort the SSO Transaction**.
12. Revisa el resumen y selecciona **Hecho**.
13. Selecciona **Hecho**.

Configura los ajustes del protocolo

Pasos

1. En la pestaña **Conexión SP > SSO del navegador > Configuración del protocolo**, selecciona **Configurar los ajustes del protocolo**.
2. En la pestaña «URL del servicio de consumidor de aserciones», acepta los valores predeterminados, que se importaron de los metadatos SAML de StorageGRID (**POST** para Binding y `/api/saml-response` para Endpoint URL).
3. En la pestaña «URL de servicio SLO», acepta los valores predeterminados, que se importaron de los metadatos SAML de StorageGRID (**REDIRECT** para Binding y `/api/saml-logout` para Endpoint URL).
4. En la pestaña «Enlaces SAML permitidos», desmarca **ARTIFACT** y **SOAP**. Solo son obligatorios **POST** y **REDIRECT**.

5. En la pestaña Signature Policy, deja seleccionadas las casillas de verificación **Require Authn Requests to be Signed** y **Always Sign Assertion**.
6. En la pestaña Directiva de cifrado, selecciona **Ninguno**.
7. Revisa el resumen y selecciona **Hecho** para guardar la configuración del protocolo.
8. Revisa el resumen y selecciona **Hecho** para guardar la configuración de SSO del navegador.

Configura credenciales

Pasos

1. En la pestaña Conexión de SP, selecciona **Credenciales**.
2. En la pestaña «Credenciales», selecciona **Configurar credenciales**.
3. Selecciona el [certificado de firma](#) que creaste o importaste.
4. Selecciona **Siguiente** para ir a **Administrar la configuración de verificación de firmas**.
 - a. En la pestaña Trust Model, selecciona **Unanchored**.
 - b. En la pestaña «Certificado de verificación de firma», revisa la información del certificado de firma, que se importó desde los metadatos SAML de StorageGRID.
5. Revisa las pantallas de resumen y selecciona **Guardar** para guardar la conexión SP.

Crear conexiones SP adicionales

Puedes copiar la primera conexión SP para crear las conexiones SP que necesites para cada Admin Node en tu grid. Subes nuevos metadatos para cada copia.



Las conexiones SP para los distintos nodos de administración utilizan una configuración idéntica, salvo en lo que respecta al Partner's Entity ID, la Base URL, el Connection ID, el Connection Name, la verificación de la firma y la SLO Response URL.

Pasos

1. Selecciona **Acción > Copiar** para crear una copia de la conexión SP inicial para cada Admin Node adicional.
2. Introduce el ID de conexión y el nombre de conexión de la copia y selecciona **Guardar**.
3. Selecciona el archivo de metadatos correspondiente al nodo de administración:
 - a. Selecciona **Action > Actualizar con metadatos**.
 - b. Selecciona **Elegir archivo** y sube los metadatos.
 - c. Selecciona **Siguiente**.
 - d. Selecciona **Guardar**.
4. Soluciona el error provocado por el atributo no utilizado:
 - a. Selecciona la nueva conexión.
 - b. Selecciona **Configurar SSO del navegador > Configurar la creación de aserciones > Contrato de atributos**.
 - c. Elimina la entrada para **urn:oid**.
 - d. Selecciona **Guardar**.

Desactiva el inicio de sesión único en StorageGRID

Puedes desactivar el inicio de sesión único (SSO) si ya no quieres usar esta funcionalidad. Debes desactivar el inicio de sesión único antes de poder desactivar la federación de identidades.

Antes de empezar

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

Pasos

1. Selecciona **Configuración > Control de acceso > inicio de sesión único**.

Aparece la página de inicio de sesión único.

2. Selecciona **Desactivar SSO**.
3. Selecciona **Sí**.

Aparece un mensaje de aviso en el que se indica que los usuarios locales ahora podrán iniciar sesión.

La próxima vez que inicies sesión en StorageGRID, aparece la página de Sign in de StorageGRID y debes introducir el nombre de usuario y la contraseña de un usuario local o federado de StorageGRID.

Deshabilita temporalmente y vuelve a habilitar SSO para un nodo de administración StorageGRID

Es posible que no puedas iniciar sesión en el Grid Manager si el sistema de inicio de sesión único (SSO) deja de funcionar. En este caso, puedes desactivar y volver a activar temporalmente el SSO para un nodo de administración. Para desactivar y luego volver a activar el SSO, debes acceder al shell de comandos del nodo.

Antes de empezar

- Tienes ["permisos de acceso específicos"](#).
- Tienes el archivo `Passwords.txt`.
- Conoces la contraseña del usuario raíz local.

Acerca de esta tarea

Después de deshabilitar el SSO para un nodo de administración, puedes iniciar sesión en el Grid Manager como el usuario raíz local. Para proteger tu sistema StorageGRID, debes usar el shell de comandos del nodo para volver a habilitar el SSO en el nodo de administración tan pronto como cierres sesión.



Desactivar el SSO en un nodo de administración no afecta la configuración del SSO de los demás nodos de administración en la grid. La casilla **Habilitar SSO** en la página de inicio de sesión único en el Grid Manager permanece seleccionada y todos los ajustes de SSO existentes se mantienen a menos que los actualices.

Pasos

1. Inicia sesión en un nodo de administración:
 - a. Introduce el siguiente comando: `ssh admin@Admin_Node_IP`

- b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
- d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Ejecuta el siguiente comando: `disable-saml`

Un mensaje indica que el comando solo se aplica a este Admin Node.

3. Confirma que deseas desactivar el SSO.

Aparece un mensaje que indica que el inicio de sesión único está desactivado en el nodo.

4. Desde un navegador web, accede al Grid Manager en el mismo nodo de administración.

Ahora se muestra la página de inicio de sesión de Grid Manager porque se ha desactivado el inicio de sesión único.

5. Inicia sesión con el nombre de usuario root y la contraseña del usuario raíz local.
6. Si has desactivado temporalmente el SSO porque tenías que corregir la configuración del SSO:
- a. Selecciona **Configuración > Control de acceso > inicio de sesión único**.
 - b. Modifica los ajustes de SSO que sean incorrectos o estén desactualizados.
 - c. Selecciona **Guardar**.

Al seleccionar **Guardar** en la página de inicio de sesión único, se vuelve a activar automáticamente el SSO para toda la grid.

7. Si has desactivado temporalmente el SSO porque necesitabas acceder al Grid Manager por cualquier otro motivo:
- a. Realiza la tarea o tareas que tengas que realizar.
 - b. Selecciona **Cerrar sesión** y cierra el Grid Manager.
 - c. Vuelve a activar el SSO en el nodo de administración. Puedes seguir cualquiera de los siguientes pasos:

- Ejecuta el siguiente comando: `enable-saml`

Un mensaje indica que el comando solo se aplica a este Admin Node.

Confirma que deseas activar el inicio de sesión único.

Aparece un mensaje que indica que el inicio de sesión único está activado en el nodo.

- Reinicia el nodo de grid: `reboot`

8. Desde un navegador web, accede al Grid Manager desde el mismo Admin Node.
9. Comprueba que aparece la página de Sign in de StorageGRID y que debes introducir tus credenciales de SSO para acceder a Grid Manager.

Usa la federación de grid

Conoce la federación de grid de StorageGRID

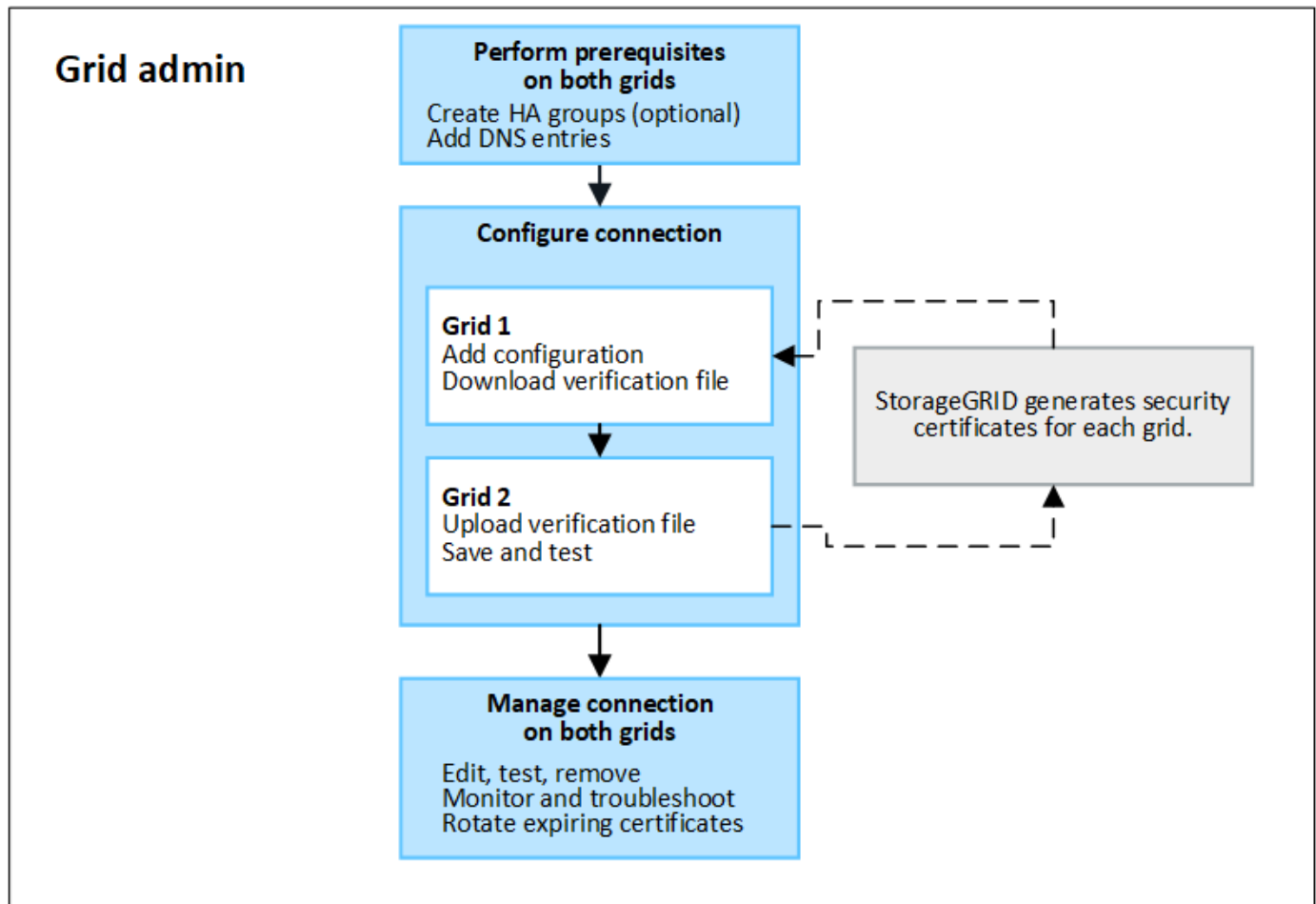
Puedes utilizar la federación de grid para clonar inquilinos y replicar sus objetos entre dos sistemas StorageGRID para recuperación ante desastres.

¿Qué es una conexión de federación de grid?

Una conexión de federación de grid es una conexión bidireccional, confiable y segura entre los nodos Admin y Gateway en dos sistemas StorageGRID.

Flujo de trabajo para la federación de grid

El diagrama de flujo resume los pasos para configurar una conexión de federación de grid entre dos grids.



Consideraciones y requisitos para las conexiones de federación de grid

- Las redes utilizadas para la federación de redes deben ejecutar versiones de StorageGRID que sean idénticas o que no tengan más de una diferencia de versión principal entre ellas.

Para obtener más información sobre los requisitos de versión, consulta la ["Notas de publicación"](#). Debes iniciar sesión con tu cuenta de NetApp o crear una cuenta para acceder a las notas de la versión.

- Un grid puede tener una o más conexiones de federación de grid con otros grids. Cada conexión de federación de grid es independiente de cualquier otra conexión. Por ejemplo, si Grid 1 tiene una conexión

con Grid 2 y una segunda conexión con Grid 3, no existe ninguna conexión implícita entre Grid 2 y Grid 3.

- Las conexiones de la federación de redes son bidireccionales. Después de que se establece la conexión, puedes supervisar y gestionar la conexión desde cualquiera de las dos redes.
- Debe existir al menos una conexión a la federación de grid para que puedas usar ["clon de cuenta"](#) o ["replicación entre grids"](#).

Requisitos de red y dirección IP

- Las conexiones de la federación de grid pueden ocurrir en la Grid Network, Admin Network o Client Network.
- Una conexión de federación de grid conecta un grid con otro grid. La configuración de cada grid especifica un endpoint de federación de grid en el otro grid, que consiste en Admin Nodes, Gateway Nodes o ambos.
- La mejor práctica es conectar ["grupos de alta disponibilidad \(HA\)"](#) de nodos de Gateway y de administración en cada grid. El uso de grupos de HA ayuda a garantizar que las conexiones de federación de grid permanezcan en línea si los nodos dejan de estar disponibles. Si la interfaz activa de cualquiera de los grupos de HA falla, la conexión puede usar una interfaz de respaldo.
- No se recomienda crear una conexión de federación de grid que use la dirección IP de un solo Admin Node o Gateway Node. Si el nodo deja de estar disponible, la conexión de federación de grid también dejará de estar disponible.
- ["Replicación entre grids"](#) El almacenamiento de objetos requiere que los nodos de almacenamiento de cada grid puedan acceder a los nodos de administración y Gateway configurados en el otro grid. Para cada grid, comprueba que todos los nodos de almacenamiento tengan una ruta con alto ancho de banda hacia los nodos de administración o Gateway utilizados para la conexión.

Utiliza nombres de dominio completos (FQDN) para equilibrar la carga de la conexión

En un entorno de producción, utiliza nombres de dominio completos (FQDN) para identificar cada grid en la conexión. Luego, crea las entradas DNS correspondientes, así:

- El FQDN de Grid 1 está asociado a una o varias direcciones IP virtuales (VIP) de los grupos de alta disponibilidad (HA) en Grid 1 o a la dirección IP de uno o varios nodos Admin o Gateway en Grid 1.
- El FQDN de Grid 2 asignado a una o varias direcciones VIP de Grid 2 o a la dirección IP de uno o varios nodos Admin o Gateway en Grid 2.

Cuando usas varias entradas DNS, las solicitudes para usar la conexión se distribuyen de la siguiente manera:

- Las entradas DNS que se asignan a las direcciones VIP de varios grupos de alta disponibilidad se distribuyen de forma equilibrada entre los nodos activos de los grupos de alta disponibilidad.
- Las entradas DNS que se asignan a las direcciones IP de varios nodos de administración o nodos de puerta de enlace se equilibran la carga entre los nodos asignados.

Requisitos de puertos

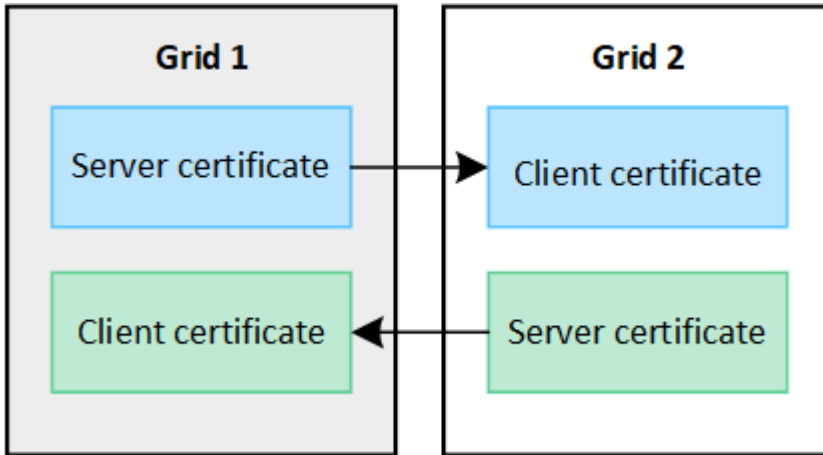
Al crear una conexión de federación de grid, puedes especificar cualquier número de puerto no utilizado entre 23000 y 23999. Ambos grids en esta conexión usarán el mismo puerto.

Debes asegurarte de que ningún nodo de ninguna de las dos grids utilice este puerto para otras conexiones.

Requisitos del certificado

Al configurar una conexión de federación de grid, StorageGRID genera automáticamente cuatro certificados SSL:

- Certificados de servidor y de cliente para autenticar y cifrar la información enviada desde la grid 1 a la grid 2
- Certificados de servidor y de cliente para autenticar y cifrar la información enviada desde la grid 2 a la grid 1



De forma predeterminada, los certificados tienen una validez de 730 días (2 años). Cuando estos certificados se acercan a su fecha de caducidad, la alerta **Expiration of grid federation certificate** te recuerda que debes renovarlos, lo cual puedes hacer usando el Grid Manager.



Si los certificados de cualquiera de los extremos de la conexión caducan, la conexión dejará de funcionar. La replicación de datos quedará pendiente hasta que se actualicen los certificados.

Más información

- ["Crear conexiones de federación de grid"](#)
- ["Gestiona las conexiones de la federación de grid"](#)
- ["Solucionar errores de federación de grid"](#)

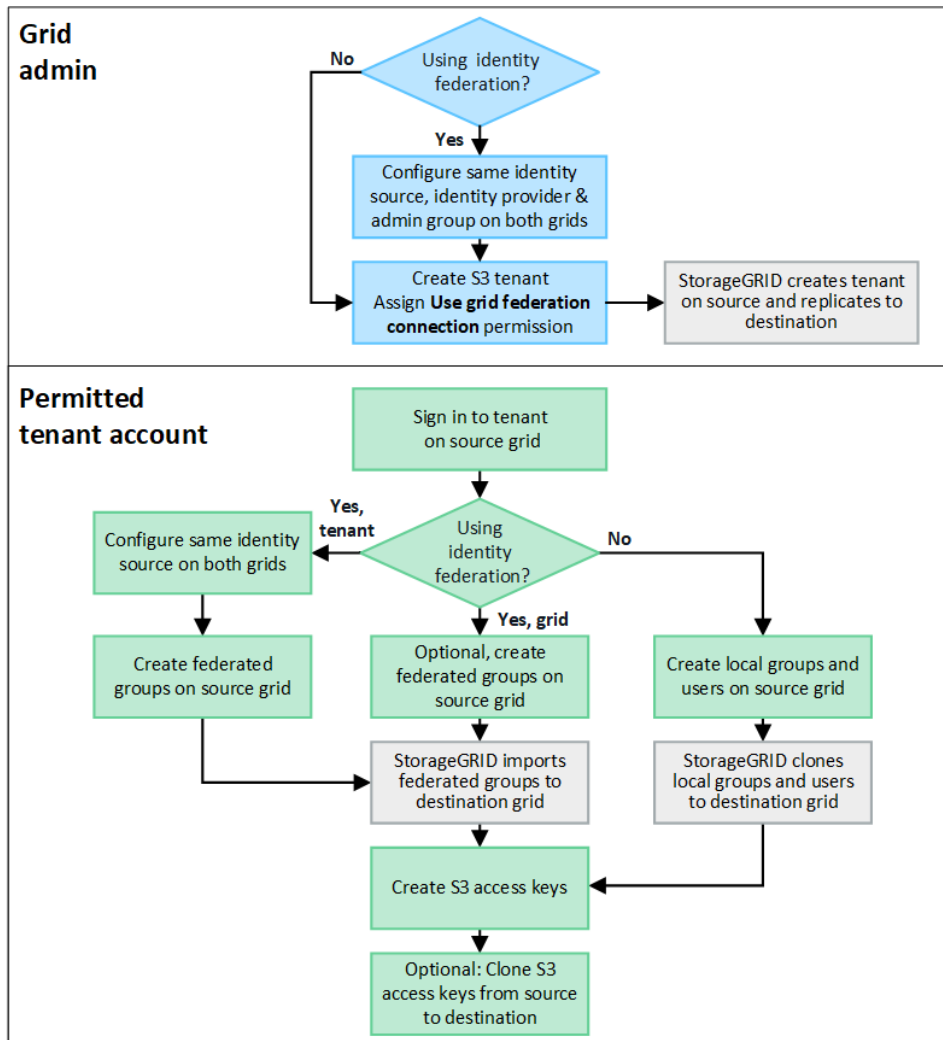
Conoce la clonación de cuentas en StorageGRID

La clonación de cuentas es la replicación automática de una cuenta de inquilino, grupos de inquilinos, usuarios de inquilinos y, opcionalmente, claves de acceso de S3 entre los sistemas StorageGRID de una ["conexión de federación de grid"](#).

Es necesario clonar la cuenta para ["replicación entre grids"](#). Clonar la información de la cuenta desde un sistema StorageGRID de origen a un sistema StorageGRID de destino garantiza que los usuarios y grupos de los inquilinos puedan acceder a los buckets y objetos correspondientes en cualquiera de las dos grids.

Flujo de trabajo para la clonación de cuentas

El diagrama de flujo muestra los pasos que los administradores de grid y los inquilinos permitidos realizarán para configurar la clonación de cuentas. Estos pasos se realizan después del ["La conexión de federación de grid está configurada"](#).



Flujo de trabajo de administración del grid

Los pasos que realizan los administradores de grid dependen de si los sistemas StorageGRID en el "conexión de federación de grid" utilizan el inicio de sesión único (SSO) o la federación de identidades.

Configura el inicio de sesión único para la clonación de cuentas (opcional)

Si alguno de los sistemas StorageGRID de la conexión de federación de redes utiliza SSO, ambas redes deben utilizar SSO. Antes de crear las cuentas de inquilino para la federación de redes, los administradores de las redes de origen y destino del inquilino deben seguir estos pasos.

Pasos

1. Configura el mismo origen de identidad para ambos grids. Consulta ["Usa la federación de identidades"](#).
2. Configura el mismo proveedor de identidad de inicio de sesión único (SSO) para ambos grids. Consulta ["Configura el inicio de sesión único"](#).
3. ["Crea el mismo grupo de administradores"](#) en ambos grids al importar el mismo grupo federado.

Al crear el inquilino, deberás seleccionar este grupo para que tenga el permiso de acceso a raíz inicial tanto para la cuenta de inquilino de origen como para la de destino.



Si este grupo de administradores no existe en ambas grids antes de crear el tenant, el tenant no se replica en el destino.

Configura la federación de identidades a nivel de grid para la clonación de cuentas (opcional)

Si alguno de los sistemas StorageGRID utiliza la federación de identidades sin SSO, ambas grids deben utilizar la federación de identidades. Antes de crear las cuentas de tenant para la federación de grids, los administradores de las grids de origen y destino del tenant deben realizar estos pasos.

Pasos

1. Configura el mismo origen de identidad para ambos grids. Consulta ["Usa la federación de identidades"](#).
2. Opcionalmente, si un grupo federado va a tener permiso de acceso de usuario raíz inicial tanto para las cuentas de inquilino de origen como de destino, ["crear el mismo grupo de administradores"](#) en ambas grids importando el mismo grupo federado.



Si asignas el permiso de acceso de usuario raíz a un grupo federado que no existe en ambas grids, el tenant no se replica en la grid de destino.

3. Si no quieres que un grupo federado tenga permiso de acceso inicial de usuario raíz para ambas cuentas, especifica una contraseña para el usuario raíz local.

Crear cuenta de inquilino S3 permitida

Después de configurar opcionalmente SSO o federación de identidades, un administrador de grid realiza estos pasos para determinar qué tenants pueden replicar objetos de los buckets a otros sistemas StorageGRID.

Pasos

1. Determina qué grid quieres que sea el grid de origen del inquilino para las operaciones de clonación de cuentas.

La red en la que se crea inicialmente el inquilino se conoce como la *red de origen* del inquilino. La red en la que se replica el inquilino se conoce como la *red de destino* del inquilino.

2. En esa cuadrícula, crea una nueva cuenta de inquilino de S3 o edita una cuenta existente.
3. Asigna el permiso **Usar conexión de federación de grid**.
4. Si la cuenta de inquilino va a gestionar sus propios usuarios federados, asígnale el permiso **Usar fuente de identidad propia**.

Si se asigna este permiso, tanto la cuenta del inquilino de origen como la de destino deben configurar la misma fuente de identidad antes de crear grupos federados. Los grupos federados añadidos al inquilino de origen no se pueden clonar en el inquilino de destino a menos que ambas grids utilicen la misma fuente de identidad.

5. Selecciona una conexión específica de la federación de grid.
6. Guarda el inquilino nuevo o modificado.

Cuando se guarda un nuevo inquilino con el permiso **Utilizar conexión de federación de redes**, StorageGRID crea automáticamente una réplica de ese inquilino en la otra grid, de la siguiente manera:

- Ambas cuentas de inquilino tienen el mismo ID de cuenta, nombre, cuota de almacenamiento y permisos asignados.

- Si seleccionaste un grupo federado para que tenga permiso de acceso Root para el inquilino, ese grupo se clona en el inquilino de destino.
- Si has seleccionado un usuario local para que tenga permiso de acceso de usuario raíz en el inquilino, ese usuario se clona en el inquilino de destino. Sin embargo, la contraseña de ese usuario no se clona.

Para más detalles, consulta ["Gestiona los inquilinos permitidos para la federación de grid"](#).

Flujo de trabajo permitido para la cuenta de inquilino

Después de que un inquilino con el permiso **Use grid federation connection** se replica en la grid de destino, las cuentas de inquilino autorizadas pueden seguir estos pasos para clonar grupos de inquilinos, usuarios y claves de acceso S3.

Pasos

1. Inicia sesión en la cuenta del inquilino en el grid de origen del inquilino.
2. Si está permitido, configura la federación de identidad tanto en la cuenta del inquilino de origen como en la de destino.
3. Crea grupos y usuarios en el tenant 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 realiza ninguna clonación desde el inquilino de destino hacia el de origen.

4. Crea claves de acceso a S3.
5. Opcionalmente, clona las claves de acceso S3 del inquilino de origen al inquilino de destino.

Para obtener más información sobre el flujo de trabajo permitido para las cuentas de inquilino y para saber cómo se clonan los grupos, los usuarios y las claves de acceso S3, consulta ["Clonar grupos de inquilinos y usuarios"](#) y ["Clonar claves de acceso a S3 mediante la API"](#).

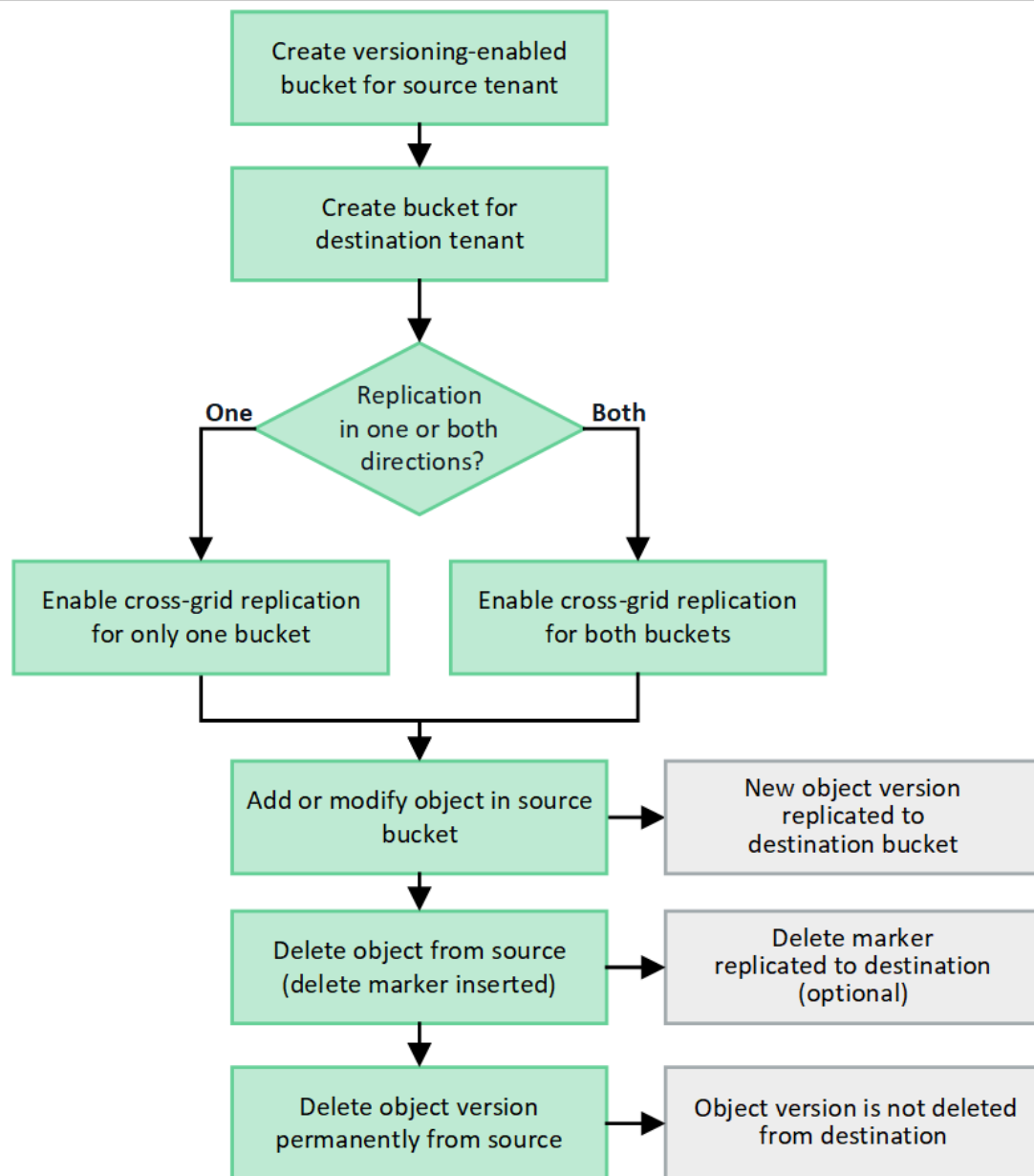
Conoce la replicación entre grids en StorageGRID

La replicación entre grids es la replicación automática de objetos entre buckets S3 seleccionados en dos sistemas StorageGRID que están conectados en una ["conexión de federación de grid"](#). ["Clon de cuenta"](#) es necesario para la replicación entre grids.

Flujo de trabajo para la replicación entre grids

El diagrama de flujo resume los pasos para configurar la replicación entre grids entre buckets de dos grids.

Tenant user



Requisitos para la replicación entre grids

Si una cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** para usar una o más "conexiones de federación de grid", un usuario de inquilino con permiso de acceso raíz puede crear buckets en las cuentas de inquilino correspondientes de cada grid. Estos buckets:

- Pueden tener nombres diferentes entre sí
- Puede tener diferentes regiones
- Debe tener activado el control de versiones
- Debe estar vacío

Después de que se hayan creado ambos buckets, puedes configurar la replicación entre grids para cualquiera de los buckets o para ambos.

Más información

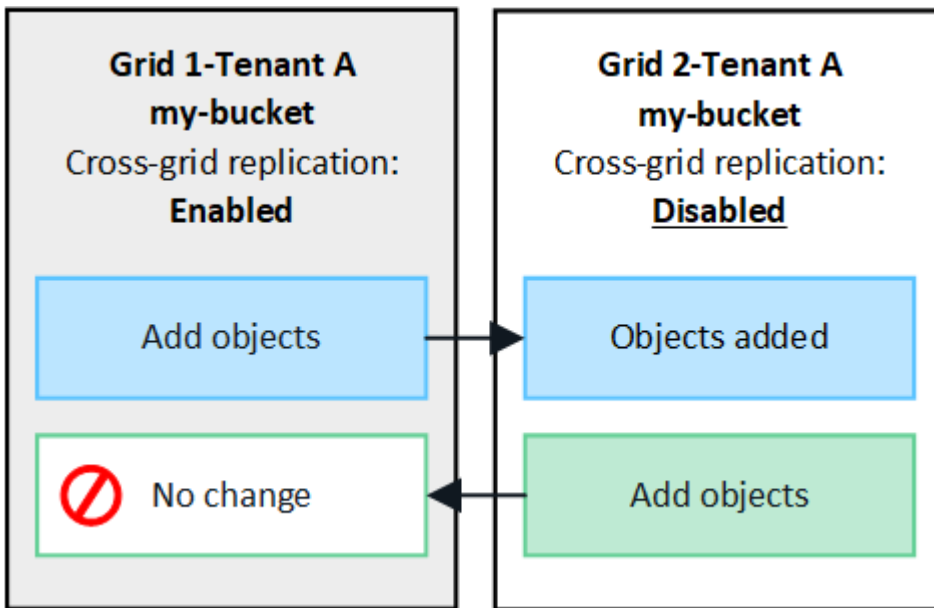
"Gestiona la replicación entre grids"

Cómo funciona la replicación entre grids

Puedes configurar la replicación entre redes para que se realice en una sola dirección o en ambas direcciones.

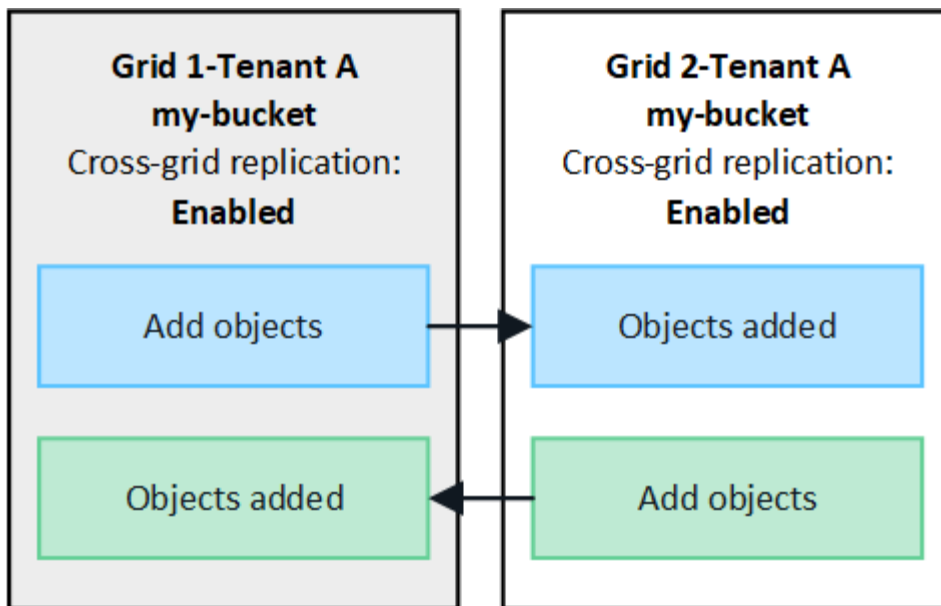
Replicación en una dirección

Si habilitas la replicación entre redes para un bucket en solo una red, los objetos añadidos a ese bucket (el bucket de origen) se replican al bucket correspondiente en la otra red (el bucket de destino). Sin embargo, los objetos añadidos al bucket de destino no se replican de vuelta al de origen. En la figura, la replicación entre redes está habilitada para `my-bucket` desde Grid 1 a Grid 2, pero no está habilitada en la otra dirección.



Replicación en ambas direcciones

Si habilitas la replicación entre grids para el mismo bucket en ambos grids, los objetos añadidos a cualquiera de los buckets se replican en el otro grid. En la figura, la replicación entre grids está habilitada para `my-bucket` en ambas direcciones.



¿Qué ocurre cuando se ingieren objetos?

Cuando un cliente de S3 añade un objeto a un bucket que tiene habilitada la replicación entre grids, ocurre lo siguiente:

1. StorageGRID replica automáticamente el objeto desde el bucket de origen al bucket de destino. El tiempo necesario para realizar esta operación de replicación en segundo plano depende de varios factores, incluido el número de otras operaciones de replicación que estén pendientes.

El cliente S3 puede verificar el estado de replicación de un objeto enviando una solicitud `GetObject` o `HeadObject`. La respuesta incluye un encabezado de respuesta específico de StorageGRID `x-ntap-sg-cgr-replication-status`, que tiene uno de los siguientes valores:

Grid	Estado de la replicación
Fuente	• FINALIZADO: La replicación se realizó correctamente en todas las conexiones de grid. • PENDIENTE: El objeto no se ha replicado en al menos una conexión de grid. • ERROR: No hay ninguna replicación pendiente para ninguna conexión de grid y al menos una ha fallado con un error permanente. Un usuario debe resolver el error.
Destino	RÉPLICA: El objeto fue replicado desde la cuadrícula de origen.



StorageGRID no admite la cabecera `x-amz-replication-status`.

2. StorageGRID utiliza las políticas de ILM activas de cada grid para gestionar los objetos, tal como lo haría con cualquier otro objeto. Por ejemplo, el objeto A en el grid 1 se podría almacenar como dos copias replicadas y conservar para siempre, mientras que la copia del objeto A que se replicó en el grid 2 se podría almacenar mediante codificación de borrado 2+1 y eliminar después de tres años.

¿Qué ocurre cuando se eliminan objetos?

Tal y como se describe en ["Eliminar flujo de datos"](#), StorageGRID puede eliminar un objeto por cualquiera de estas razones:

- El cliente S3 envía una solicitud de eliminación.
- Un usuario de Tenant Manager selecciona la opción ["Eliminar objetos en el depósito"](#) para eliminar todos los objetos de un bucket.
- El bucket tiene una configuración de ciclo de vida que caduca.
- Finaliza el último periodo de tiempo en la regla ILM para el objeto y no hay más ubicaciones especificadas.

Cuando StorageGRID elimina un objeto debido a una operación de Delete objects in bucket, a la expiración del ciclo de vida del bucket o a la expiración de la ubicación de ILM, el objeto replicado nunca se elimina de la otra grid en una conexión de grid federation. Sin embargo, los marcadores de eliminación añadidos al bucket de origen mediante eliminaciones del cliente S3 pueden replicarse opcionalmente al bucket de destino.

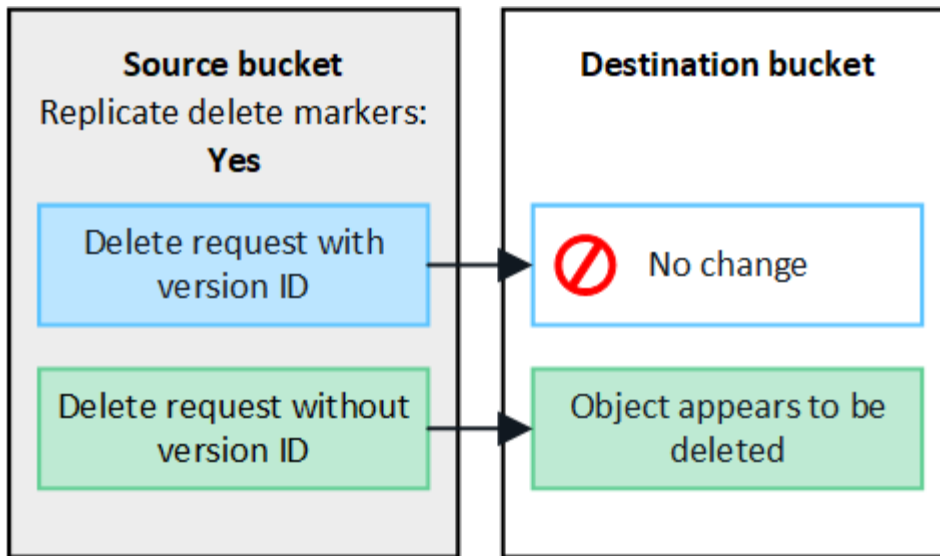
Para comprender qué ocurre cuando un cliente de S3 elimina objetos de un bucket que tiene habilitada la replicación entre grids, revisa cómo los clientes de S3 eliminan objetos de buckets que tienen habilitado el versionado, como sigue:

- Si un cliente de S3 envía una solicitud de eliminación que incluye un identificador de versión, esa versión del objeto se elimina de forma permanente. No se añade 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 del objeto. En su lugar, añade un marcador de eliminación al bucket. El marcador de eliminación hace que StorageGRID actúe como si el objeto se hubiera eliminado:
 - Una solicitud GetObject sin un ID de versión falla con 404 No Object Found
 - Una solicitud GetObject con un ID de versión válido se realiza correctamente y devuelve la versión del objeto solicitada.

Cuando un cliente de S3 elimina un objeto de un depósito que tiene habilitada la replicación entre redes, StorageGRID determina si debe replicar la solicitud de eliminación al destino, como sigue:

- Si la solicitud de eliminación incluye un ID de versión, esa versión del objeto se elimina de forma permanente del grid de origen. Sin embargo, StorageGRID no replica las solicitudes de eliminación que incluyen un ID de versión, por lo que esa misma versión del objeto no se elimina del destino.
- Si la solicitud de eliminación no incluye un identificador de versión, StorageGRID puede, de forma opcional, replicar el marcador de eliminación, en función de cómo esté configurada la replicación entre grids para el bucket:
 - Si eliges replicar los marcadores de eliminación (predeterminado), se añade un marcador de eliminación al bucket de origen y se replica en el bucket de destino. En efecto, el objeto parece estar eliminado en ambos grids.
 - Si eliges no replicar los marcadores de eliminación, se añade un marcador de eliminación al bucket de origen, pero no se replica en el bucket de destino. En efecto, los objetos que se eliminan en el grid de origen no se eliminan en el grid de destino.

En la figura, **Replicate delete markers** se estableció en **Yes** cuando ["Se habilitó la replicación entre grids"](#). Las solicitudes de eliminación para el bucket de origen que incluyen un ID de versión no eliminan objetos del bucket de destino. Las solicitudes de eliminación para el bucket de origen que no incluyen un ID de versión parecen eliminar objetos en el bucket de destino.



Si quieres mantener sincronizadas las eliminaciones de objetos entre grids, crea ["Configuraciones del ciclo de vida de S3"](#) correspondientes para los buckets en ambos grids.

Cómo se replican los objetos cifrados

Cuando usas la replicación entre grids para replicar objetos entre grids, puedes cifrar objetos individuales, usar el cifrado de bucket predeterminado o configurar el cifrado a nivel de grid. Puedes añadir, modificar o eliminar la configuración de cifrado predeterminado de bucket o a nivel de grid antes o después de habilitar la replicación entre grids para un bucket.

Para cifrar objetos individuales, puedes usar SSE (cifrado del lado del servidor con claves gestionadas por StorageGRID) al añadir los objetos al bucket de origen. Usa la cabecera de solicitud `x-amz-server-side-encryption` y especifica AES256. Consulta ["Utiliza el cifrado del lado del servidor"](#).



El uso de SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente) no es compatible con la replicación entre grids. La operación de ingesta fallará.

Para usar el cifrado predeterminado para un bucket, usa una solicitud `PutBucketEncryption` y establece el parámetro `SSEAlgorithm` en AES256. El cifrado a nivel de bucket se aplica a cualquier objeto que se ingrese sin el encabezado de solicitud `x-amz-server-side-encryption`. Consulta ["Operaciones en cubos"](#).

Para utilizar el cifrado a nivel de grid, configura la opción **Cifrado de objetos almacenados** en **AES-256**. El cifrado a nivel de grid se aplica a cualquier objeto que no esté cifrado a nivel de bucket o que se ingrese sin el encabezado de solicitud `x-amz-server-side-encryption`. Consulta ["Configura las opciones de red y de objetos"](#).



SSE no admite AES-128. Si la opción **Stored object encryption** está habilitada para el grid de origen mediante la opción **AES-128**, el uso del algoritmo AES-128 no se propaga al objeto replicado. En su lugar, el objeto replicado utiliza la configuración de cifrado predeterminada a nivel de grid o de bucket del destino, si está disponible.

A la hora de determinar cómo cifrar los objetos de origen, StorageGRID aplica estas reglas:

1. Utiliza el encabezado de ingesta `x-amz-server-side-encryption`, si está presente.
2. Si no hay ningún encabezado de ingesta, usa la configuración de cifrado predeterminada del bucket, si

está configurada.

3. Si no se ha configurado un parámetro para el bucket, usa el parámetro de cifrado para toda la grid, si está configurado.
4. Si no existe una configuración para toda la grid, no cifres el objeto de origen.

A la hora de determinar cómo cifrar los objetos replicados, StorageGRID aplica estas reglas en este orden:

1. Utiliza el mismo cifrado que el objeto de origen, a menos que ese objeto use cifrado AES-128.
2. Si el objeto de origen no está cifrado o utiliza AES-128, usa la configuración de cifrado predeterminada del bucket de destino, si está configurada.
3. Si el bucket de destino no tiene una configuración de cifrado, usa la configuración de cifrado para toda la grid del destino, si está configurada.
4. Si no existe una configuración válida para toda la grid, no cifres el objeto de destino.

Replicación entre grids con S3 Object Lock

Puedes configurar la replicación entre redes de StorageGRID entre buckets de StorageGRID con S3 Object Lock habilitado en las siguientes circunstancias.

Cuando S3 Object Lock en el bucket de origen está...	Y el S3 Object Lock en el bucket de destino es...
Habilitado	Habilitado
Deshabilitado	Habilitado

Cuando S3 Object Lock está activado en el bucket de origen:

- Los objetos se bloquean con los parámetros de retención en el destino en este orden:

- a. Los valores del encabezado de retención del objeto de origen para:

`x-amz-object-lock-mode`

`x-amz-object-lock-retain-until-date`

- b. El tiempo de retención predeterminado del bucket de origen, si se ha configurado.
- c. El tiempo de retención predeterminado del depósito de destino, si se ha configurado.

La retención predeterminada del bucket de destino no anula los parámetros de retención replicados desde el objeto de origen.

- Puedes establecer el estado de retención legal del objeto de destino utilizando `x-amz-object-lock-legal-hold` al cargar el objeto.
- Se produce un error si el inquilino o el bucket de destino no admiten la configuración de S3 Object Lock del objeto de origen. Consulta ["Alertas y errores de replicación entre grids."](#)

Cuando la función S3 Object Lock del bucket de origen está desactivada:

- Puedes configurar la retención predeterminada en el bucket de destino para aplicar la configuración de retención de S3 Object Lock al objeto de destino.

- El objeto de destino no puede establecer un estado de retención legal.

PutObjectTagging y DeleteObjectTagging no son compatibles

Las solicitudes PutObjectTagging y DeleteObjectTagging no son compatibles para los objetos en los buckets que tienen habilitada la replicación entre grids.

Si un cliente S3 envía una solicitud PutObjectTagging o DeleteObjectTagging, 501 Not Implemented se devuelve. El mensaje es Put (Delete) ObjectTagging isn't available for buckets that have cross-grid replication configured.

PutObjectRetention y PutObjectLegalHold no son compatibles

Las solicitudes PutObjectRetention y PutObjectLegalHold no son totalmente compatibles con los objetos de buckets que tienen habilitada la replicación entre grids.

Si un cliente S3 realiza una solicitud PutObjectRetention o PutObjectLegalHold, la configuración del objeto de origen se modifica, pero los cambios no se aplican al destino.

Cómo se replican los objetos segmentados

El tamaño máximo de segmento de la grid de origen se aplica a los objetos replicados en la grid de destino. Cuando los objetos se replican en otra grid, el parámetro **Maximum Segment Size (Configuration > System > Storage options)** de la grid de origen se utiliza en ambas grids. Por ejemplo, supón que el tamaño máximo de segmento de la grid de origen es de 1 GB, mientras que el tamaño máximo de segmento de la grid de destino es de 50 MB. Si ingestas un objeto de 2 GB en la grid de origen, ese objeto se guarda como dos segmentos de 1 GB. También se replica en la grid de destino como dos segmentos de 1 GB, aunque el tamaño máximo de segmento de esa grid sea de 50 MB.

Compara la replicación entre grids y la replicación CloudMirror en StorageGRID

A medida que empieces a usar la federación de grid, revisa las similitudes y diferencias entre "[replicación entre grids](#)" y "[Servicio de replicación CloudMirror de StorageGRID](#)".



No puedes usar CloudMirror en un bucket replicado por replicación entre grids, y viceversa.

	Replicación entre grids	Servicio de replicación de CloudMirror
¿Cuál es el objetivo principal?	Un sistema StorageGRID actúa como sistema de recuperación ante desastres. Los objetos de un bucket pueden replicarse entre las grids en una o en ambas direcciones.	Permite a un inquilino replicar automáticamente objetos desde un bucket en StorageGRID (origen) a un bucket externo de S3 (destino). La replicación CloudMirror crea una copia independiente de un objeto en una infraestructura S3 independiente. Esta copia independiente no se utiliza como copia de backup, sino que a menudo se procesa posteriormente en la nube.

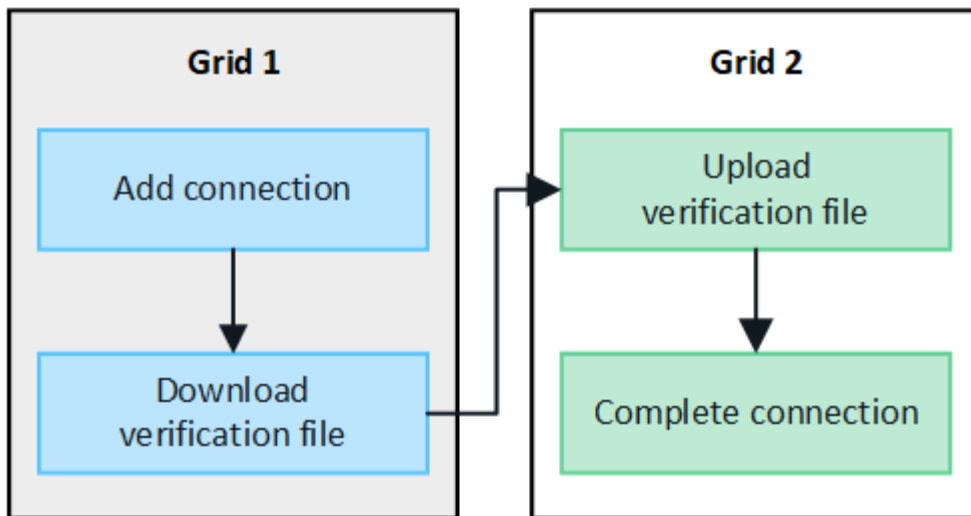
	Replicación entre grids	Servicio de replicación de CloudMirror
¿Cómo se configura?	1. Configura una conexión de federación de grid entre dos grids. 2. Agrega nuevas cuentas de inquilinos, que se clonan automáticamente en la otra grid. 3. Agrega nuevos grupos de inquilinos y usuarios, que también se clonan. 4. Crea los buckets correspondientes en cada grid y activa la replicación entre grids en una o ambas direcciones.	1. Un usuario inquilino configura la replicación de CloudMirror definiendo un endpoint de CloudMirror (dirección IP, credenciales, etc.) usando el Tenant Manager o la API de S3. 2. Cualquier bucket que pertenezca a esa cuenta de inquilino se puede configurar para que apunte al punto de conexión de CloudMirror.
¿Quién se encarga de configurarlo?	• Un administrador de grid configura la conexión y los tenants. • Los usuarios del tenant configuran los grupos, los usuarios, las claves y los buckets.	Normalmente, un usuario arrendatario.
¿Cuál es el destino?	Un bucket S3 correspondiente e idéntico en el otro sistema StorageGRID en la conexión de la federación de la grid.	• Cualquier infraestructura S3 compatible (incluido Amazon S3). • Google Cloud Platform (GCP)
¿Es necesario el control de versiones de los objetos?	Sí, tanto el bucket de origen como el de destino deben tener activado el versionado de objetos.	No, la replicación de CloudMirror admite cualquier combinación de depósitos sin versionar y versionados, tanto en el origen como en el destino.
¿Qué hace que los objetos se trasladen al destino?	Los objetos se replican automáticamente cuando se añaden a un bucket que tiene habilitada la replicación entre grids.	Los objetos se replican automáticamente cuando se añaden a un bucket que se ha configurado con un endpoint CloudMirror. Los objetos que existían en el bucket de origen antes de que el bucket se configurara con el endpoint CloudMirror no se replican, a menos que se modifiquen.
¿Cómo se replican los objetos?	La replicación entre grids crea objetos versionados y replica el ID de versión del bucket de origen al bucket de destino. Esto permite mantener el orden de las versiones en ambas grids.	CloudMirror replication no requiere buckets con control de versiones habilitado, así que CloudMirror solo puede mantener el orden de una clave dentro de un sitio. No hay garantías de que se mantenga el orden en las solicitudes a un objeto en un sitio diferente.
¿Y si un objeto no se puede replicar?	El objeto está en cola para replicación, sujeto a los límites de almacenamiento de metadatos.	El objeto se ha puesto en cola para su replicación, dentro de los límites de los servicios de la plataforma (véase "Recomendaciones para usar los servicios de la plataforma").

	Replicación entre grids	Servicio de replicación de CloudMirror
¿Se replican los metadatos del sistema del objeto?	Sí, cuando un objeto se replica en el otro grid, sus metadatos del sistema también se replican. Los metadatos serán idénticos en ambos grids.	No, cuando un objeto se replica en el depósito externo, se actualizan sus metadatos del sistema. Los metadatos variarán entre las distintas ubicaciones, dependiendo del momento de la ingesta y del comportamiento de la infraestructura independiente de S3.
¿Cómo se recuperan los objetos?	Las aplicaciones pueden recuperar o leer objetos haciendo una solicitud al bucket en cualquiera de los dos grids.	Las aplicaciones pueden recuperar o leer objetos enviando una solicitud a StorageGRID o al destino S3. Por ejemplo, supón que usas la replicación de CloudMirror para duplicar objetos en una organización asociada. La organización asociada puede usar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario usar StorageGRID.
¿Qué ocurre si se elimina un objeto?	- Las solicitudes de eliminación que incluyen un identificador de versión nunca se replican en el grid de destino. - Las solicitudes de eliminación que no incluyan un identificador de versión añaden un marcador de eliminación al bucket de origen, que opcionalmente puede replicarse en el grid de destino. - Si la replicación entre grids está configurada solo en una dirección, los objetos en el bucket de destino pueden eliminarse sin afectar al origen.	Los resultados variarán en función del estado de las versiones de los buckets de origen y destino (que no tienen por qué ser iguales): - Si ambos buckets tienen control de versiones, una solicitud de eliminación añadirá un marcador de eliminación en ambas ubicaciones. - Si solo el bucket de origen tiene control de versiones, una solicitud de eliminación añadirá un marcador de eliminación al origen pero no al destino. - Si ninguno de los dos buckets tiene control de versiones, una solicitud de eliminación borrará el objeto del origen pero no del destino. Del mismo modo, los objetos en el bucket de destino se pueden eliminar sin afectar al de origen.

Crear conexiones de federación de grid StorageGRID

Puedes crear una conexión de federación de grid entre dos sistemas StorageGRID si quieres clonar los detalles de los inquilinos y replicar los datos de los objetos.

Como se muestra en la figura, crear una conexión de federación de grid incluye pasos en ambos grids. Añades la conexión en un grid y la completas en el otro grid. Puedes empezar desde cualquiera de los grids.



Antes de empezar

- Has revisado "[consideraciones y requisitos](#)" para configurar conexiones de federación de grid.
- Si planeas usar nombres de dominio completos (FQDN) para cada grid en lugar de direcciones IP o VIP, sabes qué nombres usar y has confirmado que el servidor DNS de cada grid tiene las entradas adecuadas.
- Estás usando un "[navegador web compatible](#)".
- Tienes permiso de acceso Root y la frase de contraseña de aprovisionamiento para ambas grids.

Agregar conexión

Sigue estos pasos en cualquiera de los dos sistemas StorageGRID.

Pasos

1. Inicia sesión en Grid Manager desde el nodo Admin principal de cualquiera de las grids.
2. Selecciona **Configuración > Sistema > Grid federation**.
3. Selecciona **Add connection**.
4. Introduce los datos de la conexión.

Campo	Descripción
Nombre de la conexión	Un nombre único que te ayude a reconocer esta conexión, por ejemplo, «Grid 1-Grid 2».
FQDN o dirección IP de esta grid	Una de las siguientes opciones: • El nombre de dominio completo (FQDN) de la grid en la que has iniciado sesión actualmente • Una dirección VIP de un grupo HA en esta grid • Una dirección IP de un nodo de administración o de un nodo de puerta de enlace en este grid. La dirección IP puede estar en cualquier red a la que pueda acceder el grid de destino.

Campo	Descripción
Puerto	El puerto que deseas utilizar para esta conexión. Puedes introducir cualquier número de puerto no utilizado comprendido entre 23000 y 23999. Ambas redes de esta conexión utilizarán el mismo puerto. Debes asegurarte de que ningún nodo de ninguna de las dos redes utilice este puerto para otras conexiones.
Días de validez del certificado para este grid	El número de días que quieres que los certificados de seguridad para este grid en la conexión sean válidos. El valor predeterminado es 730 días (2 años), pero puedes ingresar cualquier valor entre 1 y 762 días. StorageGRID genera automáticamente certificados de cliente y de servidor para cada grid cuando guardas la conexión.
Frase de contraseña de aprovisionamiento para este grid	La frase de acceso de aprovisionamiento de la grid en la que has iniciado sesión.
FQDN o dirección IP de la otra grid	Una de las siguientes opciones: • El dominio completo (FQDN) de la grid a la que quieres conectarte • Una dirección VIP de un grupo HA en la otra grid • Una dirección IP de un nodo de administración o un nodo de puerta de enlace en la otra grid. La dirección IP puede estar en cualquier red a la que la grid de origen pueda acceder.

5. Selecciona **Guardar y continuar**.

6. En el paso «Descargar el archivo de verificación», selecciona **Descargar el archivo de verificación**.

Después de que se complete la conexión en la otra grid, ya no podrás descargar el archivo de verificación de ninguna de las dos grids.

7. Busca el archivo descargado (*connection-name.grid-federation*) y guárdalo en una ubicación segura.



Este archivo contiene secretos (enmascarados como *****) y otros detalles confidenciales, y debes almacenarlo y transmitirlo de forma segura.

8. Selecciona **Cerrar** para volver a la página de Grid federation.

9. Comprueba que aparezca la nueva conexión y que su **Estado de la conexión** sea **Esperando a conectarse**.

10. Facilita el archivo *connection-name.grid-federation* al administrador de grid de la otra grid.

Conexión completa

Sigue estos pasos en el sistema StorageGRID al que te vas a conectar (la otra grid).

Pasos

1. Inicia sesión en Grid Manager desde el nodo Admin principal.
2. Selecciona **Configuración > Sistema > Grid federation**.
3. Selecciona **Subir archivo de verificación** para acceder a la página de subida.
4. Selecciona **Subir archivo de verificación**. Luego, busca y selecciona el archivo que descargaste de la primera grid (`connection-name.grid-federation`).

Se muestran los detalles de la conexión.

5. Opcionalmente, introduce un número diferente de días de validez para los certificados de seguridad de este grid. La entrada **Días de validez del certificado** toma de forma predeterminada el valor que introdujiste en el primer grid, pero cada grid puede usar diferentes fechas de caducidad.

En general, utiliza el mismo número de días para los certificados de ambos extremos de la conexión.



Si caducan los certificados de cualquiera de los extremos de la conexión, la conexión dejará de funcionar y las replicaciones quedarán pendientes hasta que se actualicen los certificados.

6. Introduce la frase de contraseña de aprovisionamiento de la grid en la que has iniciado sesión actualmente.
7. Selecciona **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 se muestra en la página de federación de Grid. El **Estado de la conexión** será **Conectado**.

Si aparece un mensaje de error, soluciona cualquier problema. Consulta ["Solucionar errores de federación de grid"](#).

8. Ve a la página Grid federation en el primer grid y actualiza el navegador. Confirma que el **Estado de la conexión** ahora es **Conectado**.
9. Una vez establecida la conexión, elimina de forma segura todas las copias del archivo de verificación.

Si editas esta conexión, se creará un nuevo archivo de verificación. El archivo original no se podrá volver a utilizar.

Después de que termines

- Consulta las consideraciones para ["gestión de inquilinos autorizados"](#).
- ["Crear una o varias cuentas de inquilino nuevas"](#), asigna el permiso **Usar conexión de federación de grid** y selecciona la nueva conexión.
- ["Gestiona la conexión"](#) según sea necesario. Puedes editar los valores de conexión, comprobar una conexión, rotar los certificados de conexión o eliminar una conexión.
- ["Supervisa la conexión"](#) como parte de tus actividades habituales de supervisión de StorageGRID.
- ["Soluciona los problemas de conexión"](#), incluida la resolución de cualquier alerta o error relacionado con la clonación de cuentas y la replicación entre grids.

Administra las conexiones de la federación de grid de StorageGRID

La gestión de las conexiones de la federación de redes entre sistemas StorageGRID incluye editar los detalles de las conexiones, rotar los certificados, quitar permisos de los inquilinos y eliminar conexiones en desuso.

Antes de empezar

- Has iniciado sesión en el Grid Manager de cualquiera de las dos grids usando un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#) de la grid en la que has iniciado sesión.

Editar una conexión de federación de grid

Puedes editar una conexión de federación de grid iniciando sesión en el nodo Admin principal de cualquiera de los grids en la conexión. Después de hacer cambios en el primer grid, debes descargar un nuevo archivo de verificación y subirlo al otro grid.



Mientras editas la conexión, las solicitudes de clonación de cuentas o de replicación entre grids seguirán usando la configuración de conexión existente. Cualquier cambio que hagas en el primer grid se guarda localmente, pero no se utilizará hasta que se haya subido al segundo grid, guardado y probado.

Empieza a editar la conexión

Pasos

1. Inicia sesión en Grid Manager desde el nodo Admin principal de cualquiera de las grids.
2. Selecciona **Nodos** y comprueba que todos los demás Admin Nodes de tu sistema estén online.



Al editar una conexión de federación de grid, StorageGRID intenta guardar un archivo de "configuración candidata" en todos los nodos de administración del primer grid. Si no se puede guardar este archivo en todos los nodos de administración, aparece un mensaje de advertencia cuando seleccionas **Guardar y probar**.

3. Selecciona **Configuración > Sistema > Grid federation**.
4. Edita los datos de conexión mediante el menú **Acciones** de la página Grid federation o de la página de detalles de una conexión concreta. Consulta ["Crear conexiones de federación de grid"](#) para saber qué datos debes introducir.

Menú de acciones

- a. Selecciona el botón de opción correspondiente a la conexión.
- b. Selecciona **Acciones > Editar**.
- c. Introduce la nueva información.

Página de detalles

- a. Selecciona un nombre de conexión para ver sus detalles.
- b. Selecciona **Editar**.
- c. Introduce la nueva información.

5. Introduce la contraseña de aprovisionamiento de la grid en la que has iniciado sesión.

6. Selecciona **Guardar y continuar**.

Los nuevos valores se guardan, pero no se aplicarán a la conexión hasta que hayas subido el nuevo archivo de verificación en la otra grid.

7. Selecciona **Descargar archivo de verificación**.

Para descargar este archivo más adelante, ve a la página de detalles de la conexión.

8. Busca el archivo descargado (*connection-name.grid-federation*) y guárdalo en una ubicación segura.



El archivo de verificación contiene secretos y debe almacenarse y transmitirse de forma segura.

9. Selecciona **Cerrar** para volver a la página de Grid federation.

10. Comprueba que el **Estado de la conexión** sea **Pendiente de edición**.



Si el estado de la conexión era algo diferente de **Conectado** cuando empezaste a editar la conexión, no cambiará a **Pendiente de edición**.

11. Facilita el archivo *connection-name.grid-federation* al administrador de grid de la otra grid.

Termina de editar la conexión

Finaliza la edición de la conexión subiendo el archivo de verificación en la otra grid.

Pasos

1. Inicia sesión en Grid Manager desde el nodo Admin principal.

2. Selecciona **Configuración > Sistema > Grid federation**.

3. Selecciona **Subir archivo de verificación** para acceder a la página de carga.

4. Selecciona **Cargar archivo de verificación**. Luego, busca y selecciona el archivo que descargaste desde el primer grid.

5. Introduce la frase de contraseña de aprovisionamiento de la grid en la que has iniciado sesión actualmente.

6. Selecciona **Guardar y probar**.

Si se puede establecer la conexión utilizando los valores modificados, aparecerá un mensaje de éxito. En caso contrario, aparecerá un mensaje de error. Revisa el mensaje y soluciona cualquier problema.

7. Cierra el asistente para volver a la página de federación de Grid.

8. Comprueba que el **Estado de la conexión** sea **Conectado**.

9. Ve a la página Grid federation en el primer grid y actualiza el navegador. Confirma que el **Estado de la conexión** ahora es **Conectado**.

10. Una vez establecida la conexión, elimina de forma segura todas las copias del archivo de verificación.

Probar una conexión de federación de grid

Pasos

1. Inicia sesión en Grid Manager desde el nodo Admin principal.
2. Selecciona **Configuración > Sistema > Grid federation**.
3. Prueba la conexión usando el menú **Acciones** en la página de Grid federation o en la página de detalles de una conexión específica.

Menú de acciones

- a. Selecciona el botón de opción correspondiente a la conexión.
- b. Selecciona **Acciones > Probar**.

Página de detalles

- a. Selecciona un nombre de conexión para ver sus detalles.
- b. Selecciona **Probar conexión**.

4. Comprueba el estado de la conexión:

Estado de la conexión	Descripción
Conectado	Ambas redes están conectadas y se comunican con normalidad.
Error	La conexión está en estado de error. Por ejemplo, un certificado ha caducado o un valor de configuración ya no es válido.
Edición pendiente	Has editado la conexión en esta grid, pero la conexión sigue utilizando la configuración existente. Para completar la edición, sube el nuevo archivo de verificación a la otra grid.
Esperando para conectarte	Has configurado la conexión en esta grid, pero la conexión no se ha completado en la otra grid. Descarga el archivo de verificación de esta grid y súbelo a la otra grid.
Desconocido	La conexión se encuentra en un estado desconocido, posiblemente debido a un problema de red o a que un nodo está desconectado.

5. Si el estado de la conexión es **Error**, soluciona cualquier problema. Luego, selecciona **Probar conexión** otra vez para confirmar que el problema se ha solucionado.

Rotar certificados de conexión

Cada conexión de federación de redes utiliza cuatro certificados SSL generados automáticamente para proteger la conexión. Cuando los dos certificados de cada red se acercan a su fecha de caducidad, la alerta **Caducidad del certificado de federación de redes** te recuerda que debes renovarlos.



Si caducan los certificados de cualquiera de los extremos de la conexión, la conexión dejará de funcionar y las replicaciones quedarán pendientes hasta que se actualicen los certificados.

Pasos

1. Inicia sesión en Grid Manager desde el nodo Admin principal de cualquiera de las grids.
2. Selecciona **Configuración > Sistema > Grid federation**.
3. Desde cualquiera de las pestañas en la página de Grid federation, selecciona el nombre de la conexión para ver sus detalles.
4. Selecciona la pestaña **Certificados**.
5. Selecciona **Rotar certificados**.
6. Indica durante cuántos días deben ser válidos los nuevos certificados.
7. Introduce la contraseña de aprovisionamiento de la grid en la que has iniciado sesión.
8. Selecciona **Rotar certificados**.
9. Según sea necesario, repite estos pasos en la otra grid de la conexión.

En general, utiliza el mismo número de días para los certificados de ambos extremos de la conexión.

Eliminar una conexión de federación de grid

Puedes eliminar una conexión de federación de grids desde cualquiera de los grids en la conexión. Como se muestra en la figura, debes realizar los pasos previos en ambos grids para confirmar que la conexión no está siendo utilizada por ningún tenant en ninguno de los grids.



Antes de quitar una conexión, ten en cuenta lo siguiente:

- Al eliminar una conexión no se borran los elementos que ya se hayan copiado entre grids. Por ejemplo, los usuarios, grupos y objetos del tenant que existan en ambos grids no se borran de ninguno de los grids cuando se elimina el permiso del tenant. Si quieres borrar estos elementos, debes eliminarlos manualmente de ambos grids.
- Cuando eliminas una conexión, cualquier objeto pendiente de replicación (ingresado pero aún no replicado en la otra grid) tendrá su replicación fallida de forma permanente.

Desactivar la replicación para todos los buckets de los inquilinos

Pasos

1. Desde cualquiera de las dos grids, inicia sesión en el Grid Manager desde el nodo de administración principal.
2. Selecciona **Configuración > Sistema > Grid federation**.
3. Selecciona el nombre de la conexión para ver sus detalles.
4. En la pestaña **Inquilinos autorizados**, determina si la conexión está siendo utilizada por algún inquilino.
5. Si aparece algún inquilino en la lista, indica a todos los inquilinos que ["desactivar la replicación entre grids"](#) para todos sus buckets en ambos grids de la conexión.



No puedes eliminar el permiso **Usar conexión de federación entre grids** si algún bucket de un tenant tiene habilitada la replicación entre grids. Cada cuenta de tenant debe desactivar la replicación entre grids para sus buckets en ambos grids.

Quitar el permiso para cada tenant

Después de desactivar la replicación entre grids para todos los buckets de los inquilinos, elimina el permiso **Use grid federation permission** de todos los inquilinos en ambos grids.

Pasos

1. Selecciona **Configuración > Sistema > Grid federation**.
2. Selecciona el nombre de la conexión para ver sus detalles.
3. Para cada inquilino en la pestaña **Inquilinos permitidos**, quita el permiso **Usar conexión de federación de grid** de cada inquilino. Consulta "[Gestiona los inquilinos autorizados](#)".
4. Repite estos pasos para los inquilinos permitidos en la otra grid.

Eliminar conexión

Pasos

1. Cuando ningún inquilino de ninguna de las dos grids esté utilizando la conexión, selecciona **Eliminar**.
2. Revisa el mensaje de confirmación y selecciona **Remove**.
 - Si es posible eliminar la conexión, aparecerá un mensaje de éxito. La conexión de federación entre grids ya se ha eliminado de ambos grids.
 - Si no se puede eliminar la conexión (por ejemplo, porque todavía está en uso o hay un error de conexión), aparecerá un mensaje de error. Puedes hacer lo siguiente:
 - Soluciona el error (recomendado). Consulta "[Solucionar errores de federación de grid](#)".
 - Elimina la conexión a la fuerza. Consulta la siguiente sección.

Eliminar una conexión de federación de grid de forma forzada

Si es necesario, puedes forzar la eliminación de una conexión que no tenga el estado **Connected**.

La eliminación forzada solo elimina la conexión del grid local. Para eliminar por completo la conexión, realiza los mismos pasos en ambos grids.

Pasos

1. En el cuadro de diálogo de confirmación, selecciona **Forzar eliminación**.

Aparece un mensaje de éxito. Esta conexión de federación de grid ya no se puede utilizar. Sin embargo, es posible que los buckets de inquilino aún tengan habilitada la replicación entre grids y que algunas copias de objetos ya se hayan replicado entre los grids de la conexión.

2. Desde la otra grid en la conexión, inicia sesión en el Grid Manager desde el nodo de administración principal.
3. Selecciona **Configuración > Sistema > Grid federation**.
4. Selecciona el nombre de la conexión para ver sus detalles.
5. Selecciona **Eliminar y Sí**.

6. Selecciona **Eliminar forzosamente** para eliminar la conexión de este grid.

Administra los inquilinos permitidos para la federación de grid de StorageGRID

Puedes permitir que las cuentas de inquilino de S3 utilicen una conexión de federación de grid entre dos sistemas StorageGRID. Cuando se permite a los inquilinos usar una conexión, se requieren pasos especiales para editar los detalles del inquilino o para eliminar de forma permanente el permiso del inquilino para usar la conexión.

Antes de empezar

- Has iniciado sesión en el Grid Manager de cualquiera de las dos grids usando un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#) de la grid en la que has iniciado sesión.
- Tienes ["creaste una conexión de federación de grid"](#) entre dos grids.
- Has revisado los flujos de trabajo de ["clon de cuenta"](#) y ["replicación entre grids"](#).
- Como se requiere, ya has configurado el inicio de sesión único (SSO) o la federación de identidades para ambas grids en la conexión. Consulta ["¿Qué es un clon de cuenta?"](#).

Crear un inquilino autorizado

Si quieres permitir que una cuenta de inquilino nueva o existente use una conexión de federación de grid para la clonación de cuentas y la replicación entre grids, sigue las instrucciones generales para ["crear un nuevo cliente de S3"](#) o ["editar una cuenta de inquilino"](#) y ten en cuenta lo siguiente:

- Puedes crear el inquilino desde cualquiera de las dos cuadrículas de 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 creas o editas el inquilino para habilitar el permiso **Usar conexión de federación de grid** y luego lo guardas en el primer grid, se replica automáticamente un inquilino idéntico en el otro grid. El grid donde se replica el inquilino es el *grid de destino del inquilino*.
- Los inquilinos de ambos grids tendrán el mismo ID de cuenta de 20 dígitos, nombre, descripción, cuota y permisos. Opcionalmente, puedes usar el campo **Descripción** para ayudarte a identificar cuál es el inquilino de origen y cuál es el de destino. Por ejemplo, esta descripción de un inquilino creado en el Grid 1 también aparecerá para el inquilino replicado en el Grid 2: "Este inquilino se creó en el Grid 1."
- Por motivos de seguridad, la contraseña del usuario raíz no se copia en la grid de destino.



Antes de que un usuario raíz local pueda iniciar sesión en el inquilino replicado en la grid de destino, un administrador de esa grid debe ["cambiar la contraseña del usuario raíz local"](#).

- Después de que el inquilino nuevo o editado esté disponible en ambas grids, los usuarios del inquilino pueden realizar estas operaciones:
 - Desde la grid de origen del tenant, crea grupos y usuarios locales, que se clonan automáticamente en la grid de destino del tenant. Consulta ["Clonar grupos de inquilinos y usuarios"](#).
 - Crea nuevas claves de acceso de S3, que opcionalmente pueden clonarse en la grid de destino del tenant. Consulta ["Clonar claves de acceso a S3 mediante la API"](#).
 - Crea buckets idénticos en ambos grids de la conexión y habilita la replicación entre grids en una dirección o en ambas. Consulta ["Gestiona la replicación entre grids"](#).

Ver un inquilino autorizado

Puedes consultar los detalles de un inquilino al que se le permite utilizar una conexión de federación de grid.

Pasos

1. Selecciona **Tenants**.
2. En la página Tenants, selecciona el nombre del tenant para ver la página de detalles del tenant.

Si esta es la grid de origen del tenant (es decir, si el tenant se creó en esta grid), aparecerá un mensaje para recordarte que el tenant se clonó en otra grid. Si editas o eliminas este tenant, los cambios no se sincronizarán con la otra grid.

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. De forma opcional, selecciona la pestaña **Grid federation** para "supervisar la conexión de la federación de grid".

Editar un inquilino autorizado

Si necesitas editar un inquilino que tenga el permiso **Usar conexión de federación de red**, sigue las instrucciones generales de "Editar una cuenta de inquilino" y ten en cuenta lo siguiente:

- Si un inquilino tiene el permiso **Usar conexión de federación de grid**, puedes editar los detalles del

inquilino desde cualquiera de los grids de la conexión. Sin embargo, los cambios que realices no se copiarán en el otro grid. Si quieres mantener sincronizados los detalles del inquilino entre los grids, debes realizar las mismas ediciones en ambos grids.

- No puedes quitar el permiso **Utilizar conexión de federación de grid** cuando estás editando un inquilino.
- No puedes seleccionar una conexión de federación de grid diferente cuando estás editando un inquilino.

Eliminar un inquilino autorizado

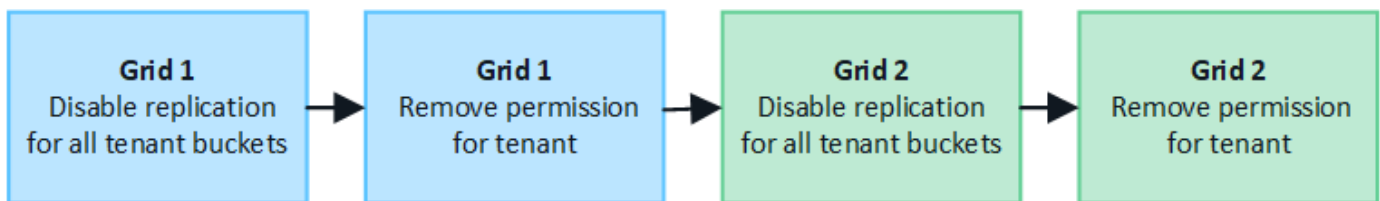
Si necesitas eliminar un inquilino que tiene el permiso **Use grid federation connection**, sigue las instrucciones generales para ["Eliminar una cuenta de inquilino"](#) y ten en cuenta lo siguiente:

- Antes de poder eliminar el inquilino original de la grid de origen, debes eliminar todos los buckets de la cuenta en la grid de origen.
- Antes de poder eliminar el inquilino clonado en la grid de destino, debes eliminar todos los buckets de la cuenta en la grid de destino.
- Si eliminas el inquilino original o el clonado, la cuenta ya no se podrá usar para la replicación entre grids.
- Si eliminas el tenant original de la grid de origen, cualquier grupo de tenant, usuario o clave que se haya clonado en la grid de destino no se verá afectado. Puedes eliminar el tenant clonado o permitir que gestione sus propios grupos, usuarios, claves de acceso y buckets.
- Si vas a eliminar el inquilino clonado en la grid de destino, se producirán errores de clonación si se añaden nuevos grupos o usuarios al inquilino original.

Para evitar estos errores, elimina el permiso del inquilino para usar la conexión de federación de grid antes de eliminar al inquilino de este grid.

Eliminar el permiso Usar conexión de federación de grid

Para impedir que un inquilino utilice una conexión de federación de grid, debes eliminar el permiso **Usar conexión de federación de grid**.



Antes de retirar a un inquilino el permiso para utilizar una conexión de federación de red, ten en cuenta lo siguiente:

- No puedes eliminar el permiso **Usar conexión de federación de redes** si alguno de los buckets del inquilino tiene habilitada la replicación entre grids. La cuenta del inquilino debe desactivar la replicación entre grids en todos sus buckets primero.
- Al eliminar el permiso **Usar conexión de federación entre grids**, no se elimina ningún elemento que ya se haya replicado entre grids. Por ejemplo, cualquier usuario, grupo y objeto del tenant que exista en ambos grids no se elimina de ninguno de los grids cuando se retira el permiso del tenant. Si quieres eliminar estos elementos, debes eliminarlos manualmente de ambos grids.
- Si deseas volver a habilitar este permiso con la misma conexión de federación de grid, elimina primero este tenant en el grid de destino; de lo contrario, volver a habilitar este permiso resultará en un error.



Al volver a habilitar el permiso **Usar conexión de federación de grid**, el grid local pasa a ser el grid de origen y se inicia la clonación en el grid remoto especificado por la conexión de federación de grid seleccionada. Si la cuenta de tenant ya existe en el grid remoto, la clonación dará lugar a un error de conflicto.

Antes de empezar

- Estás usando un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#) para ambas cuadrículas.

Desactivar la replicación para los buckets de los inquilinos

Como primer paso, desactiva la replicación entre grids para todos los buckets de los inquilinos.

Pasos

1. Desde cualquiera de las dos grids, inicia sesión en el Grid Manager desde el nodo de administración principal.
2. Selecciona **Configuración > Sistema > Grid federation**.
3. Selecciona el nombre de la conexión para ver sus detalles.
4. En la pestaña **Inquilinos autorizados**, comprueba si el inquilino está utilizando la conexión.
5. Si el inquilino aparece en la lista, indícale que ["desactivar la replicación entre grids"](#) para todos sus buckets en ambos grids de la conexión.



No puedes eliminar el permiso **Usar conexión de federación de grid** si alguno de los buckets del inquilino tiene habilitada la replicación entre grids. El inquilino debe deshabilitar la replicación entre grids para sus buckets en ambos grids.

Quitar permiso para el tenant

Después de desactivar la replicación entre grids para los buckets del inquilino, puedes eliminar el permiso del inquilino para usar la conexión de federación de grids.

Pasos

1. Inicia sesión en Grid Manager desde el nodo Admin principal.
2. Retira el permiso de la página Grid federation o de la página Tenants.

Página de federación de grid

- a. Selecciona **Configuración > Sistema > Grid federation**.
- b. Selecciona el nombre de la conexión para ver su página de detalles.
- c. En la pestaña **Inquilinos autorizados**, selecciona el botón de opción correspondiente al inquilino.
- d. Selecciona **Eliminar permiso**.

Página de inquilinos

- a. Selecciona **Tenants**.
- b. Selecciona el nombre del inquilino para mostrar la página de detalles.
- c. En la pestaña **Grid federation**, selecciona el botón de opción para la conexión.
- d. Selecciona **Eliminar permiso**.

3. Revisa las advertencias que aparecen en el cuadro de diálogo de confirmación y selecciona **Eliminar**.
 - Si se puede eliminar el permiso, vuelves a la página de detalles y se muestra un mensaje de éxito. Este tenant ya no puede usar la conexión de grid federation.
 - Si uno o más buckets de un tenant siguen teniendo activada la replicación entre grids, 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

Puedes hacer cualquiera de las siguientes cosas:

- (Recomendado.) Inicia sesión en Tenant Manager y desactiva la replicación para cada uno de los buckets del tenant. Consulta ["Gestiona la replicación entre grids"](#). Luego, repite los pasos para quitar el permiso **Use grid connection**.
- Elimina el permiso a la fuerza. Consulta la siguiente sección.

4. Ve a la otra grid y repite estos pasos para eliminar el permiso del mismo tenant en la otra grid.

Eliminar el permiso de forma forzada

Si es necesario, puedes forzar la retirada del permiso de un inquilino para utilizar una conexión de federación de grid, incluso si los buckets del inquilino tienen habilitada la replicación entre grids.

Antes de retirar por la fuerza el permiso de un inquilino, ten en cuenta las consideraciones generales para [retirar el permiso](#) así como estas consideraciones adicionales:

- Si eliminas el permiso **Usar conexión de federación de grid** por la fuerza, todos los objetos que estén pendientes de replicación en el otro grid (ingestados pero aún no replicados) se seguirán replicando. Para evitar que estos objetos en proceso lleguen al bucket de destino, también debes eliminar el permiso del tenant en el otro grid.

- Los objetos que se añadan al bucket de origen después de quitar el permiso **Use grid federation connection** nunca se replicarán en el bucket de destino.

Pasos

1. Inicia sesión en Grid Manager desde el nodo Admin principal.
2. Selecciona **Configuración > Sistema > Grid federation**.
3. Selecciona el nombre de la conexión para ver su página de detalles.
4. En la pestaña **Inquilinos autorizados**, selecciona el botón de opción correspondiente al inquilino.
5. Selecciona **Eliminar permiso**.
6. Lee las advertencias que aparecen en el cuadro de diálogo de confirmación y selecciona **Force remove**.

Aparece un mensaje de éxito. Este inquilino ya no puede utilizar la conexión de federación de grid.

7. Si es necesario, ve a la otra grid y repite estos pasos para eliminar de forma forzada el permiso de la misma cuenta de tenant en la otra grid. Por ejemplo, debes repetir estos pasos en la otra grid para evitar que los objetos en proceso lleguen al bucket de destino.

Soluciona errores de federación de grid en StorageGRID

Es posible que tengas que solucionar problemas relacionados con alertas y errores sobre las conexiones de federación de grid, la clonación de cuentas y la replicación entre grids.

Alertas y errores de conexión de la federación de grid

Es posible que recibas alertas o experimentes errores con tus conexiones de federación de grid.

Después de realizar cualquier cambio para resolver un problema de conexión, prueba la conexión para asegurarte de que el estado de la conexión vuelva a ser **Conectado**. Para obtener instrucciones, consulta ["Gestiona las conexiones de la federación de grid"](#).

Alerta de fallo en la conexión de la federación de grid

Problema

Se activó la alerta **Error de conexión a la federación Grid**.

Detalles

Esta alerta indica que la conexión de la federación de grid entre los grids no está funcionando.

Medidas recomendadas

1. Revisa la configuración de la página Grid Federation para ambas grids. Confirma que todos los valores sean correctos. Consulta ["Gestiona las conexiones de la federación de grid"](#).
2. Revisa los certificados utilizados para la conexión. Asegúrate de que no haya alertas de certificados de federación de grid caducados y de que los detalles de cada certificado sean válidos. Consulta las instrucciones para rotar los certificados de conexión en ["Gestiona las conexiones de la federación de grid"](#).
3. Confirma que todos los nodos de administración y de pasarela en ambas grids estén en línea y disponibles. Resuelve cualquier alerta que pueda estar afectando a estos nodos e inténtalo de nuevo.
4. Si proporcionaste un nombre de dominio completo (FQDN) para la grid local o remota, confirma que el servidor DNS esté en línea y disponible. Consulta ["¿Qué es la federación de grid?"](#) para ver los requisitos

de red, dirección IP y DNS.

Alerta sobre la caducidad del certificado de la federación de grid

Problema

Se activó la alerta **Caducidad del certificado de la federación de grid**.

Detalles

Esta alerta indica que uno o varios certificados de la federación de grid están a punto de caducar.

Medidas recomendadas

Consulta las instrucciones para la rotación de los certificados de conexión en "[Gestiona las conexiones de la federación de grid](#)".

Error al editar una conexión de federación de grid

Problema

Al editar una conexión de federación de grid, ves el siguiente mensaje de advertencia cuando seleccionas **Guardar y probar**: «No se pudo crear un archivo de configuración candidato en uno o más nodos».

Detalles

Al editar una conexión de federación de grid, StorageGRID intenta guardar un archivo de "configuración candidata" en todos los nodos de administración del primer grid. Aparece un mensaje de advertencia si este archivo no puede guardarse en todos los nodos de administración, por ejemplo, porque un nodo de administración está fuera de línea.

Medidas recomendadas

1. En la cuadrícula que estás utilizando para editar la conexión, selecciona **Nodos**.
2. Confirma que todos los nodos de administración de esa grid estén en línea.
3. Si hay algún nodo desconectado, vuelve a conectarlo e intenta editar la conexión de nuevo.

Errores al clonar cuentas

No puedo iniciar sesión en una cuenta de tenant clonada

Problema

No puedes iniciar sesión en una cuenta de inquilino clonada. El mensaje de error en la página de inicio de sesión de Tenant Manager es "Tus credenciales para esta cuenta no eran válidas. Por favor, inténtalo de nuevo."

Detalles

Por motivos de seguridad, cuando se clona una cuenta de inquilino desde la grid de origen del inquilino a la grid de destino del mismo, la contraseña que hayas establecido para el usuario raíz local del inquilino no se clona. Del mismo modo, cuando un inquilino crea usuarios locales en su grid de origen, las contraseñas de dichos usuarios locales no se clonan en la grid de destino.

Medidas recomendadas

Antes de que el usuario raíz pueda iniciar sesión en la grid de destino del tenant, un administrador de la grid debe primero "[cambiar la contraseña del usuario raíz local](#)" en la grid de destino.

Antes de que un usuario local clonado pueda iniciar sesión en la grid de destino del tenant, el usuario raíz del tenant clonado debe añadir una contraseña para el usuario en la grid de destino. Para obtener instrucciones,

consulta ["Gestiona usuarios"](#) en las instrucciones para usar el Tenant Manager.

Inquilino creado sin un clon

Problema

Ves el mensaje «Tenant created without a clone» después de crear un nuevo tenant con el permiso **Use grid federation connection**.

Detalles

Este problema puede producirse si se retrasan las actualizaciones del estado de la conexión, lo que podría hacer que una conexión defectuosa aparezca como **Connected**.

Medidas recomendadas

1. Revisa el motivo indicado en el mensaje de error y resuelve cualquier problema de red o de otro tipo que pueda estar impidiendo que la conexión funcione. Consulta [Alertas y errores de conexión de la federación de grid](#).
2. Sigue las instrucciones para probar una conexión a la federación de grid en ["Gestiona las conexiones de la federación de grid"](#) y confirma que el problema se ha solucionado.
3. Desde la grid de origen del tenant, selecciona **Tenants**.
4. Localiza la cuenta de inquilino que no se ha podido clonar.
5. Selecciona el nombre del inquilino para mostrar la página de detalles.
6. Selecciona **Retry account clone**.

The screenshot shows the 'Tenants > test' page. The tenant name 'test' is at the top. Below it, the Tenant ID is 0040 2213 8117 4859 6503, Protocol is S3, and Object count is 0. To the right, Quota utilization is shown as a dash, Logical space used as 0 bytes, and Quota as a dash. There are buttons for 'Sign in', 'Edit', and 'Actions'. A red error banner at the bottom states: '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'. A 'Retry account clone' button is located at the bottom of the error banner.

Si el error se ha solucionado, la cuenta del tenant ahora se clonará en la otra grid.

Alertas y errores de replicación entre grids

Último error mostrado para la conexión o el tenant

Problema

Cuando ["ver una conexión de federación de grid"](#) (o cuando ["gestionar los inquilinos permitidos"](#) para una conexión), notas un error en la columna **Último error** de la página de detalles de la conexión. Por ejemplo:

Grid 1 - Grid 2

Local hostname (this grid): 10.115.96.170
Port: 23000
Remote hostname (other grid): 10.115.96.175
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	2025-03-13 15:54:59 PDT 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. (logID 13371653720226059496) Check for errors	

Detalles

Para cada conexión de federación de redes, la columna **Último error** muestra el error más reciente que se haya producido, si lo hay, cuando se estaban replicando los datos de un inquilino a la otra red. Esta columna muestra solo el último error de replicación entre redes que se haya producido; los errores anteriores que pudieran haber ocurrido no se muestran. Un error en esta columna puede ocurrir por alguna de estas razones:

- No se encontró la versión del objeto de origen.
- No se encontró el bucket de origen.
- Se eliminó el bucket de destino.
- El bucket de destino fue recreado por una cuenta diferente.
- El bucket de destino tiene el control de versiones suspendido.
- El bucket de destino fue recreado por la misma cuenta, pero ahora no tiene versiones.
- El objeto de origen tiene una configuración de S3 Object Lock que no cumple con los parámetros de retención a nivel de inquilino del grid de destino.
- El objeto de origen tiene configuraciones de S3 Object Lock y S3 Object Lock está desactivado en el depósito de destino.

Medidas recomendadas

Si aparece un mensaje de error en la columna **Último error**, sigue estos pasos:

1. Revisa el texto del mensaje.
2. Realiza las acciones recomendadas. Por ejemplo, si se suspendió el control de versiones en el bucket de destino para la replicación entre grids, vuelve a habilitar el control de versiones para ese bucket.
3. Selecciona la conexión o la cuenta de inquilino de la tabla.
4. Selecciona **Borrar error**.
5. Selecciona **Sí** para borrar el mensaje y actualizar el estado del sistema.
6. Espera 5-6 minutos y luego ingiere un nuevo objeto en el bucket. Confirma que el mensaje de error no vuelva a aparecer.



Para asegurarte de que el mensaje de error se borre, espera al menos 5 minutos después de la marca de tiempo en el mensaje antes de ingresar un nuevo objeto.



Después de que soluciones el error, podría aparecer un nuevo **Último error** si se ingieren objetos en un bucket diferente que también tenga un error.

7. Para determinar si algún objeto no se pudo replicar debido al error del bucket, consulta ["Identifica y vuelve a intentar las operaciones de replicación que hayan fallado"](#).

Alerta de fallo permanente en la replicación entre grids

Problema

Se activó la alerta **Cross-grid replication permanent failure**.

Detalles

Esta alerta indica que los objetos de los inquilinos no se pueden replicar entre los buckets de dos grids debido a un motivo que requiere la intervención del usuario para resolverse. Esta alerta suele deberse a un cambio en el bucket de origen o en el de destino.

Medidas recomendadas

1. Inicia sesión en la grid donde se activó la alerta.
2. Ve a **Configuración > Sistema > Grid federation** y busca el nombre de la conexión que aparece en la alerta.
3. En la pestaña **Permitted tenants**, consulta la columna **Last error** para determinar qué cuentas de tenant presentan errores.
4. Para obtener más información sobre el fallo, consulta las instrucciones de ["Supervisa las conexiones de la federación de grid"](#) para revisar las métricas de replicación entre grids.
5. Para cada cuenta de inquilino afectada:
 - a. Consulta las instrucciones en ["Supervisa la actividad de los inquilinos"](#) para comprobar que el inquilino no ha superado su cuota en la grid de destino para la replicación entre grids.
 - b. Según sea necesario, aumenta la cuota del inquilino en la red de destino para permitir que se guarden nuevos objetos.
6. Para cada inquilino afectado, inicia sesión en Tenant Manager en ambas grids, para que puedas comparar la lista de buckets.
7. Para cada bucket que tenga habilitada la replicación entre redes, confirma lo siguiente:
 - Existe un bucket correspondiente para el mismo tenant en la otra grid (hay que utilizar el nombre exacto).
 - En ambos buckets está activado el control de versiones de objetos (el control de versiones no se puede suspender en ninguna de las dos grids).
 - Ninguno de los dos buckets se encuentra en el estado **Eliminación de objetos: solo lectura**.
8. Para confirmar que el problema se ha resuelto, consulta las instrucciones en ["Supervisa las conexiones de la federación de grid"](#) para revisar las métricas de replicación entre grids, o sigue estos pasos:
 - a. Vuelve a la página de la federación Grid.
 - b. Selecciona el inquilino afectado y selecciona **Borrar error** en la columna **Último error**.
 - c. Selecciona **Sí** para borrar el mensaje y actualizar el estado del sistema.

- d. Espera 5-6 minutos y luego ingiere un nuevo objeto en el bucket. Confirma que el mensaje de error no vuelva a aparecer.



Para asegurarte de que el mensaje de error se borre, espera al menos 5 minutos después de la marca de tiempo en el mensaje antes de ingresar un nuevo objeto.



La alerta puede tardar hasta un día en desaparecer una vez que se haya resuelto.

- a. Accede a ["Identifica y vuelve a intentar las operaciones de replicación que hayan fallado"](#) para identificar cualquier objeto o marcador de eliminación que no se haya replicado en la otra grid y volver a intentar la replicación si es necesario.

Alerta de recurso de replicación entre grids no disponible

Problema

Se activó la alerta **Cross-grid replication resource unavailable**.

Detalles

Esta alerta indica que las solicitudes de replicación entre grids están pendientes porque un recurso no está disponible. Por ejemplo, podría haber un error de red.

Medidas recomendadas

1. Supervisa la alerta para comprobar si el problema se resuelve por sí solo.
2. Si el problema persiste, determina si alguna de las grids tiene una alerta de **Grid federation connection failure** para la misma conexión o una alerta de **Unable to communicate with node** para un nodo. Esta alerta podría resolverse cuando soluciones esas alertas.
3. Para obtener más información sobre el fallo, consulta las instrucciones de ["Supervisa las conexiones de la federación de grid"](#) para revisar las métricas de replicación entre grids.
4. Si no puedes resolver la alerta, ponte en contacto con soporte técnico.

La replicación entre grids continuará con normalidad una vez que se resuelva el problema.

Identifica y vuelve a intentar las operaciones de replicación fallidas de StorageGRID

Después de resolver la alerta **Cross-grid replication permanent failure**, debes comprobar si hay algún objeto o marcador de eliminación que no se haya replicado en la otra grid. Luego puedes volver a ingresar estos objetos o usar la Grid Management API para volver a intentar la replicación.

La alerta **«Fallo permanente en la replicación entre redes»** indica que los objetos del inquilino no se pueden replicar entre los buckets de dos redes por un motivo que requiere la intervención del usuario para resolverse. Esta alerta suele deberse a un cambio en el bucket de origen o en el de destino. Para obtener más información, consulta ["Solucionar errores de federación de grid"](#).

Determina si algún objeto no se replicó

Para determinar si hay algún objeto o marcador de eliminación que no se haya replicado en la otra grid, puedes buscar en el registro de auditoría los mensajes **"CGRR (Solicitud de replicación entre grids)"**. Este mensaje se añade al registro cuando StorageGRID no consigue replicar un objeto, un objeto multiparte o un marcador de eliminación al bucket de destino.

Puedes usar la ["herramienta audit-explain"](#) para traducir los resultados a un formato más fácil de leer.

Antes de empezar

- Tienes permiso de acceso root.
- Tienes el archivo `Passwords.txt`.
- Conoces la dirección IP del nodo de administración principal.

Pasos

1. Inicia sesión en el nodo de administración principal:
 - a. Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Quando inicias sesión como root, el indicador cambia de \$ a #.

2. Busca mensajes CGRR en el archivo `audit.log` y usa la herramienta `audit-explain` para dar formato a los resultados.

Por ejemplo, este comando busca con «grep» 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 tendrán un aspecto similar al de este ejemplo, que contiene entradas correspondientes a seis mensajes CGRR. En el ejemplo, todas las solicitudes de replicación entre grids devolvieron un error general porque no se pudo replicar el objeto. Los tres primeros errores son de operaciones de "replicate object", y los tres últimos errores son de operaciones de "replicate delete marker".

```

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 grids CGRR	El nombre de la solicitud
inquilino	El ID de cuenta del inquilino
conexión	El identificador de la conexión de la federación de grid
operación	El tipo de operación de replicación que se estaba intentando realizar: • replicar objeto • replicar marcador de eliminación • replicar objeto multiparte
bucket	El nombre del bucket
objeto	El nombre del objeto
versión	El identificador de versión del objeto

Campo	Descripción
error	El tipo de error. Si la replicación entre grids falló, el error es «Error general».

Reintentar las replicaciones fallidas

Después de generar una lista de los objetos y marcadores de eliminación que no se replicaron en el bucket de destino y resolver los problemas subyacentes, puedes volver a intentar la replicación de dos maneras:

- Vuelve a introducir cada objeto en el bucket de origen.
- Utiliza la API privada de gestión de la grid, tal y como se describe.

Pasos

1. En la parte superior del Grid Manager, selecciona el icono de ayuda y selecciona **API documentation**.
2. Selecciona **Ir a la documentación privada de la API**.



Los puntos finales de la API de StorageGRID marcados como «Privados» están sujetos a cambios sin previo aviso. Los puntos finales privados de StorageGRID también ignoran la versión de la API de la solicitud.

3. En la sección **cross-grid-replication-advanced**, selecciona el siguiente endpoint:

```
POST /private/cross-grid-replication-retry-failed
```

4. Selecciona **Pruébalo**.
5. En el cuadro de texto **body**, reemplaza la entrada de ejemplo de **versionID** por un identificador de versión del audit.log que corresponda a una solicitud de replicación entre grids que haya fallado.

Asegúrate de mantener las comillas dobles alrededor de la cadena.

6. Selecciona **Ejecutar**.
7. Comprueba que el código de respuesta del servidor sea **204**, lo que indica que el objeto o el marcador de eliminación se ha marcado como pendiente para la replicación entre grids hacia el otro grid.



«Pendiente» significa que la solicitud de replicación entre grids se ha añadido a la cola interna para su procesamiento.

Supervisar los reintentos de replicación

Debes supervisar las operaciones de reintento de replicación para asegurarte de que se completan.



Puede que la replicación de un objeto o de un marcador de eliminación en la otra grid tarde varias horas o incluso más.

Puedes supervisar las operaciones de reintento de dos formas:

- Utiliza una solicitud S3 **"HeadObject"** o **"GetObject"**. La respuesta incluye el encabezado de respuesta específico de StorageGRID `x-ntap-sg-cgr-replication-status`, que tendrá uno de los siguientes

valores:

Grid	Estado de la replicación
Fuente	• FINALIZADO: La replicación se realizó con éxito. • PENDIENTE: El objeto aún no se ha replicado. • ERROR: La replicación falló debido a un error permanente. Un usuario debe solucionar el error.
Destino	RÉPLICA : El objeto fue replicado desde la cuadrícula de origen.

- Utiliza la API privada de gestión de la grid, tal y como se describe.

Pasos

1. En la sección **cross-grid-replication-advanced** de la documentación de la API privada, selecciona el siguiente endpoint:

```
GET /private/cross-grid-replication-object-status/{id}
```

2. Selecciona **Pruébalo**.
3. En la sección de Parámetros, introduce el ID de versión que usaste en la solicitud `cross-grid-replication-retry-failed`.
4. Selecciona **Ejecutar**.
5. Comprueba que el código de respuesta del servidor sea **200**.
6. Comprueba el estado de la replicación, que será uno de los siguientes:
 - **PENDIENTE**: El objeto aún no se ha replicado.
 - **FINALIZADO**: La replicación se realizó con éxito.
 - **FALLO**: La replicación falló debido a un error permanente. Un usuario debe solucionar el error.

Gestiona la seguridad

Administra la seguridad en StorageGRID

Puedes configurar diversos parámetros de seguridad desde Grid Manager para ayudar a proteger tu sistema StorageGRID.

Gestionar el cifrado

StorageGRID ofrece varias opciones para cifrar datos. Debes ["revisar los métodos de cifrado disponibles"](#) para determinar cuáles se ajustan a tus requisitos de protección de datos.

Gestiona certificados

Puedes ["configurar y gestionar los certificados del servidor"](#) usar para las conexiones HTTP o los certificados de cliente que se emplean para autenticar la identidad de un cliente o usuario ante el servidor.

Configura servidores de gestión de claves

El uso de un "servidor de gestión de claves" te permite proteger los datos de StorageGRID incluso si se retira un dispositivo del centro de datos. Una vez cifrados los volúmenes del dispositivo, no podrás acceder a ningún dato del mismo a menos que el nodo pueda comunicarse con el KMS.



Para utilizar la gestión de claves de cifrado, debes activar la opción **Cifrado de nodos** para cada appliance durante la instalación, antes de que el appliance se añada a la grid.

Gestiona la configuración del proxy

Si usas los servicios de plataforma de S3 o Cloud Storage Pools, puedes configurar un "servidor proxy de almacenamiento" entre los nodos de almacenamiento y los endpoints de S3 externos. Si envías paquetes de AutoSupport a través de HTTPS o HTTP, puedes configurar un "servidor proxy de administración" entre los nodos de administración y el soporte técnico.

Controla los cortafuegos

Para mejorar la seguridad de tu sistema, puedes controlar el acceso a los nodos de administración de StorageGRID abriendo o cerrando puertos específicos en "cortafuegos externo". También puedes controlar el acceso de red a cada nodo configurando su "cortafuegos interno". Puedes impedir el acceso en todos los puertos excepto aquellos necesarios para tu implementación.

Revisa los métodos de cifrado de StorageGRID

StorageGRID ofrece varias opciones para cifrar datos. Debes revisar los métodos disponibles para determinar cuáles se ajustan a tus requisitos de protección de datos.

La tabla ofrece un resumen a grandes rasgos de los métodos de cifrado disponibles en StorageGRID.

Opción de cifrado	Cómo funciona	Aplica a
Servidor de gestión de claves (KMS) en Grid Manager	Tú "configurar un servidor de gestión de claves" para el sitio de StorageGRID y "activar el cifrado de nodos para el dispositivo". Luego, un nodo del dispositivo se conecta al KMS para solicitar una clave de cifrado de claves (KEK). Esta clave cifra y descifra la clave de cifrado de datos (DEK) en cada volumen.	Nodos de appliance que tienen activada la opción Cifrado de nodo durante la instalación. Todos los datos del appliance están protegidos contra la pérdida física o la retirada del centro de datos. Nota: La gestión de claves de cifrado mediante un KMS solo es compatible con los Storage Nodes y los servicios appliances.

Opción de cifrado	Cómo funciona	Aplica a
Página de cifrado de unidades en el instalador de StorageGRID Appliance	Si el dispositivo contiene unidades que admiten cifrado por hardware, puedes establecer una frase de contraseña para la unidad durante la instalación. Cuando estableces una frase de contraseña para la unidad, es imposible que alguien recupere datos válidos de las unidades que se hayan retirado del sistema, a menos que conozca la frase de contraseña. Antes de iniciar la instalación, ve a Configure Hardware > Drive Encryption para establecer una frase de contraseña para la unidad que se aplique a todas las unidades con autocifrado gestionadas por StorageGRID en un nodo.	Dispositivos que incorporan unidades con cifrado automático. Todos los datos en las unidades protegidas están protegidos contra la pérdida física o la extracción del centro de datos. El cifrado de unidades no se aplica a las unidades gestionadas por SANtricity. Si tienes un dispositivo de almacenamiento con unidades de autocifrado y controladoras SANtricity, puedes habilitar la seguridad de las unidades en SANtricity.
Seguridad de las unidades en SANtricity System Manager	Si la función Drive Security está habilitada para tu dispositivo StorageGRID, puedes 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.	Appliances de almacenamiento que tienen unidades con cifrado de disco completo (FDE) o unidades de autocifrado. Todos los datos de las unidades protegidas están protegidos contra la pérdida física o la extracción del centro de datos. No se puede usar con algunos appliances de almacenamiento ni con ningún appliance de servicios.
Cifrado de objetos almacenados	Activa la opción "Cifrado de objetos almacenados" en Grid Manager. Cuando está activada, cualquier objeto nuevo que no esté cifrado a nivel de bucket o a nivel de objeto se cifra durante la ingesta.	Datos de objetos S3 recién importados. Los objetos almacenados actualmente no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados.

Opción de cifrado	Cómo funciona	Aplica a
Cifrado de buckets de S3	Envías una solicitud PutBucketEncryption para habilitar el cifrado para el bucket. Cualquier objeto nuevo que no esté cifrado a nivel de objeto se cifrará durante la ingesta.	Solo datos de objetos S3 recién ingeridos. Debes especificar el cifrado para el bucket. Los objetos existentes del bucket no están cifrados. Los metadatos de los objetos y otros datos confidenciales no están cifrados. "Operaciones en cubos"
Cifrado del lado del servidor (SSE) de objetos S3	Envías una solicitud S3 para almacenar un objeto e incluyes el encabezado de solicitud x-amz-server-side-encryption.	Solo datos de objetos S3 recién ingeridos. Se debe especificar el cifrado para el objeto. Los metadatos del objeto y otros datos confidenciales no están cifrados. StorageGRID gestiona las claves. "Utiliza el cifrado del lado del servidor"
Cifrado del lado del servidor de objetos S3 con claves proporcionadas por el cliente (SSE-C)	Envías una solicitud S3 para almacenar un objeto e incluyes 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 del objeto y otros datos confidenciales no están cifrados. Las claves se gestionan fuera de StorageGRID. "Utiliza el cifrado del lado del servidor"

Opción de cifrado	Cómo funciona	Aplica a
Cifrado de volúmenes externos o almacenes de datos	Tú usas un método de cifrado externo a StorageGRID para cifrar un volumen o un almacén de datos completo, si tu plataforma de implementación lo admite.	Todos los datos de los objetos, los metadatos y los datos de configuración del sistema, partiendo de la base de que todos los volúmenes o datastores están cifrados. Un método de cifrado externo permite un control más estricto sobre los algoritmos y las claves de cifrado. Se puede combinar con los demás métodos enumerados.
Cifrado de objetos fuera de StorageGRID	Tú usas un método de cifrado fuera de StorageGRID para cifrar los datos y metadatos de los objetos antes de que se incorporen a StorageGRID.	Solo datos y metadatos de objetos (los datos de configuración del sistema no están cifrados). Un método de cifrado externo permite un control más estricto sobre los algoritmos y las claves de cifrado. Se puede combinar con los demás métodos enumerados. "Amazon Simple Storage Service - Guía del usuario: protección de datos mediante el cifrado del lado del cliente"

Utiliza varios métodos de cifrado

En función de tus necesidades, puedes utilizar más de un método de cifrado a la vez. Por ejemplo:

- Puedes utilizar un KMS para proteger los nodos de los dispositivos y también usar la función de seguridad de unidades en SANtricity System Manager para "doble cifrar" los datos en las unidades con cifrado automático de esos mismos dispositivos.
- Puedes utilizar un KMS para proteger los datos en los nodos del dispositivo y también usar la opción de cifrado de objetos almacenados para cifrar todos los objetos cuando se ingieren.

Si solo una pequeña parte de tus objetos requiere cifrado, plantéate controlar el cifrado a nivel de bucket o de objeto individual. Habilitar varios niveles de cifrado tiene un coste adicional de rendimiento.

Información relacionada

["Infórmate sobre las opciones de cifrado con certificación FIPS"](#)

Gestiona certificados

Administra certificados de seguridad en StorageGRID

Los certificados de seguridad son pequeños archivos de datos que se usan para crear conexiones seguras y confiables entre los componentes de StorageGRID y entre los

componentes de StorageGRID y los sistemas externos.

StorageGRID utiliza dos tipos de certificados de seguridad:

- **Los certificados de servidor** son necesarios cuando usas conexiones HTTPS. Los certificados de servidor se usan para establecer conexiones seguras entre clientes y servidores, autenticando la identidad de un servidor ante sus clientes y proporcionando una vía de comunicación segura para los datos. El servidor y el cliente tienen cada uno una copia del certificado.
- **Los certificados de cliente** autentican la identidad de un cliente o usuario ante el servidor, lo que proporciona una autenticación más segura que las contraseñas por sí 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 compara la firma del servidor con la firma que figura en su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión con el servidor utilizando la misma clave pública.

StorageGRID funciona como el servidor para algunas conexiones (como el endpoint del equilibrador de carga) o como el cliente para otras conexiones (como el servicio de replicación de CloudMirror).

Certificado CA predeterminado de Grid

StorageGRID tiene una autoridad de certificación (CA) integrada que genera un certificado de CA de Grid interno durante la instalación del sistema. El certificado de CA de Grid se usa, de forma predeterminada, para proteger el tráfico interno de StorageGRID. Una autoridad de certificación (CA) externa puede emitir certificados personalizados que cumplan plenamente con las políticas de seguridad de la información de tu organización.

Utiliza el certificado CA de Grid para entornos que no sean de producción. Para producción, utiliza certificados personalizados firmados por una autoridad de certificación externa. Se admiten las 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 al servidor.
- Todos los certificados personalizados deben cumplir con la ["Directrices para el refuerzo del sistema para certificados de servidor"](#).
- StorageGRID admite la agrupación de certificados de una autoridad de certificación (CA) en un único archivo (lo que se conoce como paquete de certificados de CA).



StorageGRID también incluye certificados de CA del sistema operativo que son idénticos en todas las grids. En entornos de producción, asegúrate de especificar un certificado personalizado firmado por una autoridad de certificación externa en lugar del certificado de CA del sistema operativo.

Las variantes de los tipos de certificados de servidor y de cliente se implementan de varias maneras. Debes tener listos todos los certificados necesarios para tu configuración específica de StorageGRID antes de configurar el sistema.

Accede a los certificados de seguridad

Puedes acceder a la información sobre todos los certificados de StorageGRID en un único lugar, junto con enlaces al flujo de trabajo de configuración de cada certificado.

Pasos

1. En Grid Manager, selecciona **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. Selecciona una pestaña en la página Certificados para obtener información sobre cada categoría de certificado y acceder a la configuración de los certificados. Puedes acceder a una pestaña si tienes el "permiso correspondiente".
 - **Global:** Garantiza el acceso a StorageGRID desde navegadores web y clientes de API externos.
 - **Grid CA:** Protege el tráfico interno de StorageGRID.
 - **Cliente:** Protege las conexiones entre los clientes externos y la base de datos Prometheus de StorageGRID.
 - **Puntos de conexión del equilibrador de carga:** Protege las conexiones entre los clientes de S3 y el equilibrador de carga de StorageGRID.
 - **Inquilinos:** Garantiza la seguridad de las conexiones con los servidores de federación de identidades o desde los endpoints de los servicios de la plataforma hasta los recursos de almacenamiento S3.
 - **Otros:** Protege las conexiones a StorageGRID que requieren certificados específicos.

A continuación se describe cada pestaña, con enlaces a información adicional sobre los certificados.

Global

Los certificados globales protegen el acceso a StorageGRID desde navegadores web y clientes externos de la API de S3. Durante la instalación, la autoridad de certificación de StorageGRID genera inicialmente dos certificados globales. La práctica recomendada para un entorno de producción es utilizar certificados personalizados firmados por una autoridad de certificación externa.

- [Certificado de interfaz de gestión](#): Protege las conexiones de los navegadores web de los clientes a las interfaces de gestión de StorageGRID.
- [Certificado de la API de S3](#): Protege las conexiones de la API del cliente con los nodos de almacenamiento, los nodos de administración y los nodos de puerta de enlace, que las aplicaciones cliente de S3 utilizan para cargar y descargar datos de objetos.

La información sobre los certificados globales que están instalados incluye:

- **Nombre**: Nombre del certificado con un enlace para gestionar el certificado.
- **Descripción**
- **Tipo**: personalizado o predeterminado. + Siempre debes usar un certificado personalizado para mejorar la seguridad de la grid.
- **Fecha de caducidad**: si usas el certificado predeterminado, no se muestra ninguna fecha de caducidad.

Puedes:

- Sustituye los certificados predeterminados por certificados personalizados firmados por una autoridad de certificación externa para mejorar la seguridad del grid:
 - ["Sustituye el certificado predeterminado de la interfaz de gestión generado por StorageGRID"](#) se utiliza para las conexiones de Grid Manager y Tenant Manager.
 - ["Sustituye el certificado de la API de S3"](#) se usa para las conexiones del Storage Node y del endpoint del equilibrador de carga (opcional).
- ["Restaurar el certificado predeterminado de la interfaz de gestión"](#).
- ["Restablece el certificado predeterminado de la API de S3"](#).
- ["Utiliza un script para generar un nuevo certificado autofirmado de la interfaz de gestión"](#).
- Copia o descarga el ["certificado de interfaz de gestión"](#) o ["Certificado de la API de S3"](#).

CA de Grid

El [Certificado 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 caducidad del certificado y el contenido del certificado.

Puedes ["copiar o descargar el certificado de Grid CA"](#), pero no puedes cambiarlo.

Cliente

[Certificados de cliente](#), generados por una autoridad de certificación externa, protegen las conexiones entre las herramientas de monitorización externas y la base de datos StorageGRID Prometheus.

La tabla de certificados contiene una fila para cada certificado de cliente configurado e indica si el

certificado puede usarse para acceder a la base de datos de Prometheus, junto con la fecha de caducidad del certificado.

Puedes:

- ["Sube o genera un nuevo certificado de cliente."](#)
- Selecciona el nombre de un certificado para ver los detalles del certificado, donde puedes:
 - ["Cambia el nombre del certificado de cliente."](#)
 - ["Configura el permiso de acceso a Prometheus."](#)
 - ["Sube y sustituye el certificado de cliente."](#)
 - ["Copia o descarga el certificado de cliente."](#)
 - ["Elimina el certificado de cliente."](#)
- Selecciona **Acciones** para ["editar"](#), ["adjuntar"](#) o ["eliminar"](#) rápidamente un certificado de cliente. Puedes seleccionar hasta 10 certificados de cliente y eliminarlos de una sola vez usando **Acciones > Eliminar**.

Puntos de conexión del equilibrador de carga

[Certificados de los endpoints del balanceador de carga](#) protege las conexiones entre los clientes S3 y el servicio de equilibrador de carga de StorageGRID en los nodos de puerta de enlace y los nodos de administración.

La tabla de puntos de conexión del equilibrador de carga contiene una fila para cada punto de conexión configurado e indica si se está utilizando el certificado global de la API S3 o un certificado personalizado del punto de conexión del equilibrador de carga para dicho punto de conexión. También se muestra la fecha de caducidad de cada certificado.



Los cambios en el certificado de un endpoint pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Puedes:

- ["Ver un punto de conexión del equilibrador de carga"](#), incluidos los datos de su certificado.
- ["Especifica un certificado de endpoint del equilibrador de carga para FabricPool."](#)
- ["Utiliza el certificado global de la API de S3"](#) en lugar de generar un nuevo certificado para el endpoint del balanceador de carga.

Inquilinos

Los usuarios pueden utilizar [certificados del servidor de federación de identidades](#) o [certificados de los endpoints de servicio de la plataforma](#) para asegurar 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 los servicios de la plataforma.

Puedes:

- ["Selecciona un nombre de inquilino para iniciar sesión en el Tenant Manager"](#)
- ["Selecciona el nombre de un inquilino para ver los detalles de la federación de identidades del inquilino"](#)
- ["Selecciona un nombre de cliente para ver los detalles de los servicios de la plataforma de ese"](#)

cliente"

- "Especifica un certificado de endpoint de servicio de plataforma durante la creación del endpoint"

Otros

StorageGRID utiliza otros certificados de seguridad para fines específicos. Estos certificados se enumeran según su nombre funcional. Otros certificados de seguridad incluyen:

- [Certificados de Cloud Storage Pool](#)
- [Certificados de notificación por correo electrónico](#)
- [Certificados del servidor syslog externo](#)
- [Certificados de conexión de la federación de grid](#)
- [Certificados de federación de identidades](#)
- [Certificados del servidor de gestión de claves \(KMS\)](#)
- [Certificados de inicio de sesión único](#)

La información indica el tipo de certificado que utiliza una función y las fechas de caducidad de los certificados del servidor y del cliente, según corresponda. Si seleccionas el nombre de una función, se abre una pestaña del navegador donde puedes ver y editar los detalles del certificado.



Solo podrás ver y acceder a la información de otros certificados si dispones del ["permiso correspondiente"](#).

Puedes:

- ["Especifica un certificado de Cloud Storage Pool para S3, C2S S3 o Azure"](#)
- ["Especifica un certificado para las notificaciones de alerta por correo electrónico"](#)
- ["Usa un certificado para un servidor syslog externo"](#)
- ["Rotar los certificados de conexión de la federación de grid"](#)
- ["Ver y editar un certificado de federación de identidades"](#)
- ["Sube los certificados del servidor y del cliente del servidor de gestión de claves \(KMS\)"](#)
- ["Especificar manualmente un certificado de SSO para una relación de confianza de parte confiable"](#)

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 de los clientes y la interfaz de gestión de StorageGRID, permitiendo que los usuarios accedan a Grid Manager y Tenant Manager sin avisos de seguridad. Este certificado también autentica las conexiones a la Grid Management API y a la Tenant Management API. Puedes utilizar el certificado predeterminado creado durante la instalación o subir un certificado personalizado.	Configuración > Seguridad > Certificados , selecciona la pestaña Global y luego selecciona Management interface certificate	"Configura los certificados de la interfaz de gestión"

Certificado de la API de S3

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica las conexiones seguras de los clientes S3 a un nodo de almacenamiento y a los puntos de conexión del equilibrador de carga (opcional).	Configuración > Seguridad > Certificados , selecciona la pestaña Global y luego selecciona S3 API certificate	"Configura los certificados de la API de S3"

Certificado CA de Grid

Consulta el [Descripción predeterminada del certificado CA de la grid](#).

Certificado de cliente de administrador

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Cliente	Instalado en cada cliente, permitiendo que StorageGRID autentique el acceso de clientes externos. • Permite a los clientes externos autorizados acceder a la base de datos de StorageGRID Prometheus. • Permite supervisar de forma segura StorageGRID mediante herramientas externas.	Configuración > Seguridad > Certificados y luego selecciona la pestaña Cliente	"Configurar certificados de cliente"

Certificado del endpoint del balanceador de carga

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los clientes de S3 y el servicio StorageGRID Load Balancer en los nodos de puerta de enlace y los nodos de administración. Puedes cargar o generar un certificado del equilibrador de carga cuando configuras un punto de conexión del equilibrador de carga. Las aplicaciones cliente usan el certificado del equilibrador de carga al conectarse a StorageGRID para guardar y recuperar datos de objetos. También puedes utilizar una versión personalizada del certificado global Certificado de la API de S3 para autenticar las conexiones al servicio de equilibrador de carga. Si se utiliza el certificado global para autenticar las conexiones del equilibrador de carga, no necesitas cargar ni generar un certificado independiente para cada endpoint del equilibrador de carga. Nota: El certificado utilizado para la autenticación del equilibrador de carga es el que más se utiliza durante el funcionamiento normal de StorageGRID.	Configuración > Red > Puntos de conexión del equilibrador de carga	• "Configura los puntos de conexión del equilibrador de carga" • "Crear un punto de conexión del equilibrador de carga para FabricPool"

Certificado del endpoint de Cloud Storage Pool

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión desde un StorageGRID Cloud Storage Pool 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 alertas por correo electrónico

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autentica la conexión entre un servidor de correo electrónico SMTP y StorageGRID que se usa para las notificaciones de alertas. • Si la comunicación con el servidor SMTP requiere Transport Layer Security (TLS), debes especificar el certificado de la autoridad de certificación (CA) del servidor de correo electrónico. • Especifica un certificado de cliente solo si el servidor de correo electrónico SMTP requiere certificados de cliente para la autenticación.	Alertas > Email setup	"Configura notificaciones por correo electrónico para las alertas"

Certificado del 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 las conexiones TCP, RELP/TCP y UDP a un servidor syslog externo.	Configuración > Supervisión > Servidor de auditoría y syslog	"Utiliza un servidor syslog externo"

Certificado de conexión de Grid federation

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autentica y cifra la información enviada entre el sistema StorageGRID actual y otra grid en una conexión de federación de grids.	Configuración > Sistema > Federación de redes	• "Crear conexiones de federación de grid" • "Rotar los certificados de conexión"

Certificado de federación de identidades

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre StorageGRID y un proveedor de identidades externo, como Active Directory, OpenLDAP u Oracle Directory Server. Se utiliza para la federación de identidades, lo que permite que un sistema externo gestione los grupos de administradores y los usuarios.	Configuración > Control de acceso > Federación de identidades	"Usa la federación de identidades"

Certificado del servidor de gestión de claves (KMS)

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor y cliente	Autentica la conexión entre StorageGRID y un servidor externo de gestión de claves (KMS), que proporciona claves de cifrado a los nodos del dispositivo StorageGRID.	Configuración > Seguridad > Servidor de gestión de claves	" Agregar servidor de gestión de claves (KMS) "

Certificado del endpoint de los servicios de plataforma

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión desde el servicio de la plataforma StorageGRID a un recurso de almacenamiento S3.	Tenant Manager > STORAGE (S3) > Puntos de conexión de los servicios de la plataforma	" Crear un endpoint de servicios de plataforma " " Editar el endpoint de los servicios de plataforma "

Certificado de inicio de sesión único (SSO)

Tipo de certificado	Descripción	Ubicación de navegación	Detalles
Servidor	Autentica la conexión entre los servicios de federación de identidades, como Active Directory Federation Services (AD FS) y StorageGRID, que se utilizan para las solicitudes de inicio de sesión único (SSO).	Configuración > Control de acceso > Inicio de sesión único	" Configura el inicio de sesión único "

Ejemplos de certificados

Ejemplo 1: servicio de equilibrado de carga

En este ejemplo, StorageGRID actúa como servidor.

1. Configuras un punto final del equilibrador de carga y subes o generas un certificado de servidor en StorageGRID.
2. Configuras una conexión de cliente S3 al endpoint del balanceador de carga y subes el mismo certificado al cliente.
3. Cuando el cliente desea guardar o recuperar datos, se conecta al punto de acceso del equilibrador 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 compara la firma del servidor con la firma que figura en su copia del certificado. Si las firmas coinciden, el cliente inicia una sesión usando la misma clave pública.
6. El cliente envía datos de objetos a StorageGRID.

Ejemplo 2: Servidor externo de gestión de claves (KMS)

En este ejemplo, StorageGRID actúa como cliente.

1. Mediante un software externo de servidor de gestión de claves (KMS), configuras StorageGRID como cliente KMS y obtienes un certificado de servidor firmado por una autoridad de certificación (CA), un certificado público de cliente y la clave privada correspondiente a dicho certificado de cliente.
2. Usando el Grid Manager, configuras un servidor KMS y subes los certificados del servidor y del cliente, además de la clave privada del cliente.
3. Cuando un nodo de StorageGRID necesita una clave de cifrado, envía 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 compatibles en StorageGRID

El sistema StorageGRID admite certificados personalizados cifrados con RSA o ECDSA (Elliptic Curve Digital Signature Algorithm).



El tipo de cifrado de la política de seguridad debe coincidir con el tipo de certificado del servidor. Por ejemplo, los cifrados RSA requieren certificados RSA y los cifrados ECDSA requieren certificados ECDSA. Consulta ["Gestiona certificados de seguridad"](#). Si configuras una política de seguridad personalizada que no sea compatible con el certificado del servidor, puedes ["volver temporalmente a la política de seguridad predeterminada"](#).

Para obtener más información sobre cómo StorageGRID protege las conexiones de los clientes, consulta ["Seguridad para los clientes de S3"](#).

Configura certificados de la interfaz de gestión en StorageGRID

Puedes sustituir el certificado predeterminado de la interfaz de gestión por un único certificado personalizado que permita a los usuarios acceder a Grid Manager y a Tenant Manager sin que aparezcan advertencias de seguridad. También puedes volver al certificado predeterminado de la interfaz de gestión o generar uno nuevo.

Acerca de esta tarea

De forma predeterminada, cada nodo de administración recibe un certificado firmado por la CA del grid. Puedes sustituir estos certificados firmados por la CA por un único certificado de interfaz de gestión personalizado común y su clave privada correspondiente.

Como se usa un único certificado de interfaz de gestión personalizado para todos los nodos de administración, debes especificar el certificado como un certificado comodín o multidominio si los clientes necesitan verificar el nombre de host al conectarse a Grid Manager y Tenant Manager. Define el certificado personalizado de manera que coincida con todos los nodos de administración del grid.

Debes completar la configuración en el servidor y, dependiendo de la autoridad de certificación (CA) raíz que utilices, es posible que los usuarios también tengan que instalar el certificado de la CA de Grid en el navegador web que vayan a utilizar para acceder al Grid Manager y al Tenant Manager.



Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor caducado, se activa la alerta **Caducidad del certificado de servidor para la interfaz de gestión** cuando dicho certificado está a punto de caducar. Cuando lo necesites, puedes ver cuándo caduca el certificado actual seleccionando **Configuración > Seguridad > Certificados** y revisando la fecha de caducidad del certificado de la interfaz de gestión en la pestaña Global.



Si accedes al Grid Manager o al Tenant Manager utilizando un nombre de dominio en lugar de una dirección IP, el navegador muestra un error de certificado sin opción de ignorarlo si se da alguna de las siguientes situaciones:

- El certificado de tu interfaz de gestión personalizada caduca.
- Tú [Volver de un certificado personalizado de la interfaz de gestión al certificado predeterminado del servidor](#).

Agrega un certificado personalizado para la interfaz de gestión

Para añadir un certificado personalizado para la interfaz de gestión, puedes proporcionar tu propio certificado o generar uno usando Grid Manager.

Pasos

1. Selecciona **Configuración > Seguridad > Certificados**.
2. En la pestaña **Global**, selecciona **Certificado de la interfaz de gestión**.
3. Selecciona **Usar certificado personalizado**.
4. Sube o genera el certificado.

Subir certificado

Sube los archivos de certificados del servidor necesarios.

a. Selecciona **Cargar certificado**.

b. Sube los archivos de certificados del servidor necesarios:

- **Certificado del servidor:** el archivo del certificado personalizado del servidor (codificado en formato PEM).
- **Clave privada del certificado:** El archivo de la clave privada del certificado del servidor personalizado (.key).



Las claves privadas EC deben ser de 224 bits o más. Las claves privadas RSA deben ser de 2048 bits o más.

- **Paquete de 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 certificados de CA codificados en formato PEM, concatenados en el orden de la cadena de certificados.

c. Despliega **Detalles del certificado** para ver los metadatos de cada certificado que subiste. Si subiste un paquete de CA opcional, cada certificado se muestra en su propia pestaña.

- Selecciona **Descargar certificado** para guardar el archivo del certificado o selecciona **Descargar paquete de CA** para guardar el paquete de certificados.

Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión .pem.

Por ejemplo: storagegrid_certificate.pem

- Selecciona **Copiar certificado PEM** o **Copiar paquete de CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

d. Selecciona **Guardar**. + El certificado de la interfaz de gestión personalizada se utiliza para todas las nuevas conexiones posteriores a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

Generar certificado

Genera los archivos del certificado del servidor.



La mejor práctica para un entorno de producción es usar un certificado de interfaz de gestión personalizado firmado por una autoridad de certificación externa.

a. Selecciona **Generar certificado**.

b. Indica la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o más dominios completos para incluir en el certificado. Usa un * como comodín para representar varios nombres de dominio.

Campo	Descripción
IP	Una o varias direcciones IP para incluir en el certificado.
Asunto (opcional)	Nombre del sujeto X.509 o nombre distintivo (DN) del titular del certificado. Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la primera dirección IP como nombre común (CN) del sujeto.
Días de validez	Número de días después de la creación en los que caduca el certificado.
Agregar extensiones de uso de clave	Si seleccionas esta opción (predeterminada y recomendada), se añaden al certificado generado las extensiones de uso de clave y uso ampliado de clave. Estas extensiones definen la finalidad de la clave incluida en el certificado. Nota: Deja esta casilla marcada a menos que tengas problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.

c. Selecciona **Generar**.

d. Selecciona **Detalles del certificado** para ver los metadatos del certificado generado.

- Selecciona **Descargar certificado** para guardar el archivo del certificado.

Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

e. Selecciona **Guardar**. + El certificado de la interfaz de gestión personalizada se utiliza para todas las nuevas conexiones posteriores a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

5. Actualiza la página para asegurarte de que el navegador web esté actualizado.



Después de subir o generar un nuevo certificado, espera hasta un día para que se borren las alertas relacionadas con la caducidad del certificado.

6. Después de que añades un certificado personalizado de la interfaz de gestión, la página de certificado de la interfaz de gestión muestra información detallada sobre los certificados que están en uso. + Puedes descargar o copiar el certificado PEM según lo necesites.

Restaurar el certificado predeterminado de la interfaz de gestión

Puedes volver a utilizar el certificado predeterminado de la interfaz de administración para las conexiones a Grid Manager y Tenant Manager.

Pasos

1. Selecciona **Configuración > Seguridad > Certificados**.
2. En la pestaña **Global**, selecciona **Certificado de la interfaz de gestión**.
3. Selecciona **Usar certificado predeterminado**.

Cuando restauras el certificado predeterminado de la interfaz de gestión, los archivos de certificado de servidor personalizados que configuraste se eliminan y no se pueden recuperar del sistema. El certificado predeterminado de la interfaz de gestión se utiliza para todas las nuevas conexiones de cliente posteriores.

4. Actualiza la página para asegurarte de que el navegador web esté actualizado.

Utiliza un script para generar un nuevo certificado autofirmado de la interfaz de gestión

Si se requiere una validación estricta del nombre de host, puedes utilizar un script para generar el certificado de la interfaz de gestión.

Antes de empezar

- Tienes ["permisos de acceso específicos"](#).
- Tienes el archivo `Passwords.txt`.

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. Obtén el nombre de dominio completo (FQDN) de cada Admin Node.
2. Inicia sesión en el nodo de administración principal:
 - a. Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

3. Configura StorageGRID con un nuevo certificado autofirmado.

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- En el caso de `--domains`, utiliza caracteres comodín para representar los nombres de dominio completos de todos los nodos de administración. Por ejemplo, `*.ui.storagegrid.example.com` utiliza el carácter comodín `*` para representar `admin1.ui.storagegrid.example.com` y `admin2.ui.storagegrid.example.com`.

- Establece `--type` en `management` para configurar el certificado de la interfaz de gestión, que usan Grid Manager y Tenant Manager.
- Por defecto, los certificados generados tienen una validez de un año (365 días) y deben volver a generarse antes de que caduquen. Puedes usar el argumento `--days` para cambiar el periodo de validez predeterminado.



El periodo de validez de un certificado comienza cuando se ejecuta `make-certificate`. Debes asegurarte de que el cliente de gestión 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
```

El resultado contiene el certificado público que necesita tu cliente de la API de gestión.

4. Selecciona y copia el certificado.

Incluye las etiquetas `BEGIN` y `END` en tu selección.

5. Cierra sesión en la línea de comandos. `$ exit`

6. Confirma que el certificado se configuró:

- Accede al Grid Manager.
- Selecciona **Configuración > Seguridad > Certificados**
- En la pestaña **Global**, selecciona **Certificado de la interfaz de gestión**.

7. Configura tu cliente de gestión para que use el certificado público que copiaste. Incluye las etiquetas `BEGIN` y `END`.

Descarga o copia el certificado de la interfaz de administración

Puedes guardar o copiar el contenido del certificado de la interfaz de administración para utilizarlo en otro lugar.

Pasos

1. Selecciona **Configuración > Seguridad > Certificados**.
2. En la pestaña **Global**, selecciona **Certificado de la interfaz de gestión**.
3. Selecciona la pestaña **Servidor** o **Paquete de CA** y luego descarga o copia el certificado.

Descargar el archivo de certificado o el paquete de CA

Descarga el certificado o el paquete de CA .pem. Si utilizas un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

- a. Selecciona **Descargar certificado** o **Descargar paquete de CA**.

Si estás descargando un paquete de CA, todos los certificados de las pestañas secundarias del paquete de CA se descargan en un único archivo.

- b. Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión .pem.

Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado o paquete PEM de CA

Copia el texto del certificado para pegarlo en otro lugar. Si utilizas un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

- a. Selecciona **Copiar certificado PEM** o **Copiar CA bundle PEM**.

Si estás copiando un paquete de CA, todos los certificados de las pestañas secundarias del paquete de CA se copian juntos.

- b. Pega el certificado copiado en un editor de texto.
- c. Guarda el archivo de texto con la extensión .pem.

Por ejemplo: `storagegrid_certificate.pem`

Configura certificados de la API S3 en StorageGRID

Puedes sustituir o restaurar el certificado de servidor que se utiliza para las conexiones de los clientes S3 a los nodos de almacenamiento o a los endpoints del balanceador de carga. El certificado de servidor personalizado de sustitución es específico de tu organización.



Hemos eliminado los detalles de Swift de esta versión del sitio de documentación. Consulta ["StorageGRID 11.8: configura los certificados de las API de S3 y Swift"](#).

Acerca de esta tarea

De forma predeterminada, a cada nodo de almacenamiento se le asigna un certificado de servidor X.509 firmado por la CA de la grid. Estos certificados firmados por la CA pueden sustituirse por un único certificado de servidor personalizado común y la clave privada correspondiente.

Se utiliza un único certificado de servidor personalizado para todos los nodos de almacenamiento, por lo que debes especificar el certificado como certificado comodín o multidominio si los clientes necesitan verificar el nombre de host al conectarse al endpoint de almacenamiento. Define el certificado personalizado de manera que coincida con todos los nodos de almacenamiento en el grid.

Después de completar la configuración en el servidor, es posible que también tengas que instalar el certificado

de la CA de Grid en el cliente de la API de S3 que vayas a usar para acceder al sistema, dependiendo de la autoridad de certificación (CA) raíz que estés usando.



Para asegurarte de que las operaciones no se interrumpan por un fallo en el certificado del servidor, la alerta **Vencimiento del certificado de servidor global para la API de S3** se activa cuando el certificado de servidor raíz está a punto de caducar. Si lo necesitas, puedes ver cuándo caduca el certificado actual seleccionando **Configuración > Seguridad > Certificados** y consultando la fecha de caducidad del certificado de la API de S3 en la pestaña Global.

Puedes subir o generar un certificado de API de S3 personalizado.

Agrega un certificado personalizado de la API de S3

Pasos

1. Selecciona **Configuración > Seguridad > Certificados**.
2. En la pestaña **Global**, selecciona **S3 API certificate**.
3. Selecciona **Usar certificado personalizado**.
4. Sube o genera el certificado.

Subir certificado

Sube los archivos de certificados del servidor necesarios.

a. Selecciona **Cargar certificado**.

b. Sube los archivos de certificados del servidor necesarios:

- **Certificado del servidor:** el archivo del certificado personalizado del servidor (codificado en formato PEM).
- **Clave privada del certificado:** El archivo de la clave privada del certificado del servidor personalizado (.key).



Las claves privadas EC deben ser de 224 bits o más. Las claves privadas RSA deben ser de 2048 bits o más.

- **Paquete de 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 certificados de CA codificados en formato PEM, concatenados en el orden de la cadena de certificados.

c. Selecciona los detalles del certificado para ver los metadatos y el PEM de cada certificado personalizado de la API de S3 que hayas subido. Si subiste un paquete de CA opcional, cada certificado se muestra en su propia pestaña.

- Selecciona **Descargar certificado** para guardar el archivo del certificado o selecciona **Descargar paquete de CA** para guardar el paquete de certificados.

Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión .pem.

Por ejemplo: storagegrid_certificate.pem

- Selecciona **Copiar certificado PEM** o **Copiar paquete de CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

d. Selecciona **Guardar**.

El certificado de servidor personalizado se usa para las siguientes nuevas conexiones de clientes S3.

Generar certificado

Genera los archivos del certificado del servidor.

a. Selecciona **Generar certificado**.

b. Indica la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o más dominios completos para incluir en el certificado. Usa un * como comodín para representar varios nombres de dominio.
IP	Una o varias direcciones IP para incluir en el certificado.

Campo	Descripción
Asunto (opcional)	Nombre del sujeto X.509 o nombre distintivo (DN) del titular del certificado. Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la primera dirección IP como nombre común (CN) del sujeto.
Días de validez	Número de días después de la creación en los que caduca el certificado.
Agregar extensiones de uso de clave	Si seleccionas esta opción (predeterminada y recomendada), se añaden al certificado generado las extensiones de uso de clave y uso ampliado de clave. Estas extensiones definen la finalidad de la clave incluida en el certificado. Nota: Deja esta casilla marcada a menos que tengas problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.

c. Selecciona **Generar**.

d. Selecciona **Detalles del certificado** para mostrar los metadatos y el PEM del certificado personalizado de la API de S3 que se generó.

- Selecciona **Descargar certificado** para guardar el archivo del certificado.

Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

e. Selecciona **Guardar**.

El certificado de servidor personalizado se usa para las siguientes nuevas conexiones de clientes S3.

5. Selecciona una pestaña para mostrar los metadatos del certificado predeterminado del servidor StorageGRID, de un certificado firmado por una autoridad de certificación (CA) que se haya cargado o de un certificado personalizado que se haya generado.



Después de subir o generar un nuevo certificado, espera hasta un día para que se borren las alertas relacionadas con la caducidad del certificado.

6. Actualiza la página para asegurarte de que el navegador web esté actualizado.

7. Después de añadir un certificado de la API de S3 personalizado, la página del certificado de la API de S3 muestra información detallada sobre el certificado de la API de S3 personalizado que está en uso. +
Puedes descargar o copiar el PEM del certificado según sea necesario.

Restablece el certificado predeterminado de la API de S3

Puedes volver a utilizar el certificado predeterminado de la API de S3 para las conexiones de los clientes de S3 a los nodos de almacenamiento. Sin embargo, no puedes utilizar el certificado predeterminado de la API de S3 para un endpoint de un load balancer.

Pasos

1. Selecciona **Configuración > Seguridad > Certificados**.
2. En la pestaña **Global**, selecciona **S3 API certificate**.
3. Selecciona **Usar certificado predeterminado**.

Al restaurar la versión predeterminada del certificado global de la API de S3, los archivos de certificados de servidor personalizados que hayas configurado se eliminan y no pueden recuperarse del sistema. El certificado predeterminado de la API de S3 se usará para las siguientes nuevas conexiones de clientes S3 a Storage Nodes.

4. Selecciona **OK** para confirmar la advertencia y restablecer el certificado predeterminado de la API de S3.

Si tienes permiso de acceso Root y se ha utilizado un certificado personalizado de la API de S3 para las conexiones al endpoint del balanceador de carga, se muestra una lista de endpoints del balanceador de carga a los que ya no podrás acceder usando el certificado predeterminado de la API de S3. Ve a ["Configura los puntos de conexión del equilibrador de carga"](#) para editar o eliminar los endpoints afectados.

5. Actualiza la página para asegurarte de que el navegador web esté actualizado.

Descarga o copia el certificado de la API de S3

Puedes guardar o copiar el contenido del certificado de la API de S3 para utilizarlo en otro lugar.

Pasos

1. Selecciona **Configuración > Seguridad > Certificados**.
2. En la pestaña **Global**, selecciona **S3 API certificate**.
3. Selecciona la pestaña **Servidor** o **Paquete de CA** y luego descarga o copia el certificado.

Descargar el archivo de certificado o el paquete de CA

Descarga el certificado o el paquete de CA .pem. Si utilizas un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Selecciona **Descargar certificado** o **Descargar paquete de CA**.

Si estás descargando un paquete de CA, todos los certificados de las pestañas secundarias del paquete de CA se descargan en un único archivo.

b. Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión .pem.

Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado o paquete PEM de CA

Copia el texto del certificado para pegarlo en otro lugar. Si utilizas un paquete de CA opcional, cada certificado del paquete se muestra en su propia subpestaña.

a. Selecciona **Copiar certificado PEM** o **Copiar CA bundle PEM**.

Si estás copiando un paquete de CA, todos los certificados de las pestañas secundarias del paquete de CA se copian juntos.

b. Pega el certificado copiado en un editor de texto.

c. Guarda el archivo de texto con la extensión .pem.

Por ejemplo: `storagegrid_certificate.pem`

Información relacionada

- ["Usa la API de REST de S3"](#)
- ["Configura los nombres de dominio de los endpoints S3"](#)

Copia el certificado StorageGRID Grid CA

StorageGRID utiliza una autoridad de certificación (CA) interna para proteger el tráfico interno. Este certificado no cambia aunque subas tus propios certificados.

Antes de empezar

- Has 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 de la CA del sistema StorageGRID.

Pasos

1. Selecciona **Configuración > Seguridad > Certificados** y luego selecciona la pestaña **Grid CA**.

2. En la sección **Certificado PEM**, descarga o copia el certificado.

Descargar el archivo del certificado

Descarga el archivo de certificado .pem.

- Selecciona **Descargar certificado**.
- Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión .pem.

Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado PEM

Copia el texto del certificado para pegarlo en otro sitio.

- Selecciona **Copiar certificado PEM**.
- Pega el certificado copiado en un editor de texto.
- Guarda el archivo de texto con la extensión .pem.

Por ejemplo: `storagegrid_certificate.pem`

Configura los certificados de StorageGRID para FabricPool

Para los clientes S3 que realizan una validación estricta de nombres de host y no admiten desactivarla, como los clientes ONTAP que usan FabricPool, puedes generar o cargar un certificado de servidor al configurar el endpoint del equilibrador de carga.

Antes de empezar

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

Acerca de esta tarea

Cuando creas un endpoint de equilibrador de carga, puedes generar un certificado de servidor autofirmado o subir un certificado firmado por una autoridad de certificación (CA) conocida. En entornos de producción, deberías usar 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 de tipo man-in-the-middle.

Los siguientes pasos ofrecen directrices generales para los clientes de S3 que utilizan FabricPool. Para obtener información y procedimientos más detallados, consulta ["Configura StorageGRID para FabricPool"](#).

Pasos

- Si lo deseas, configura un grupo de alta disponibilidad (HA) para que lo use FabricPool.
- Crea un punto de conexión del equilibrador de carga de S3 para que lo use FabricPool.

Al crear un punto final de equilibrador de carga HTTPS, se te pedirá que subas tu certificado de servidor, la clave privada del certificado y, opcionalmente, el paquete de la autoridad de certificación (CA bundle).

3. Adjunta StorageGRID como un nivel de cloud en ONTAP.

Especifica el puerto del extremo del balanceador de carga y el nombre de dominio completo utilizado en el certificado de CA que cargaste. A continuación, proporciona el certificado de CA.



Si una CA intermedia emitió el certificado de StorageGRID, debes proporcionar el certificado de la CA intermedia. Si la CA raíz emitió directamente el certificado de StorageGRID, debes proporcionar el certificado de la CA raíz.

Configura certificados de cliente en StorageGRID

Los certificados de cliente permiten a los clientes externos autorizados acceder a la base de datos de StorageGRID Prometheus, lo que ofrece una forma segura para que las herramientas externas supervisen StorageGRID.

Si necesitas acceder a StorageGRID usando una herramienta de monitoreo externa, debes cargar o generar un certificado de cliente usando Grid Manager y copiar la información del certificado en la herramienta externa.

Consulta ["Gestiona certificados de seguridad"](#) y ["Configura certificados de servidor personalizados"](#).



Para garantizar que las operaciones no se vean interrumpidas por un certificado de servidor caducado, se activa la alerta **Caducidad de los certificados de cliente configurados en la página Certificados** cuando este certificado de servidor está a punto de caducar. Según sea necesario, puedes ver cuándo caduca el certificado actual seleccionando **Configuración > Seguridad > Certificados** y consultando la fecha de caducidad del certificado de cliente en la pestaña Cliente.



Si utilizas un servidor de gestión de claves (KMS) para proteger los datos en nodos de dispositivos configurados de forma especial, consulta la información específica sobre ["subir un certificado de cliente KMS"](#).

Antes de empezar

- Tienes permiso de acceso root.
- Has 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 Admin Node.
 - Si has configurado el certificado de la interfaz de gestión de StorageGRID, tienes la CA, el certificado de cliente y la clave privada que se usaron para configurar el certificado de la interfaz de gestión.
 - Para cargar tu propio certificado, la clave privada del certificado está disponible en tu ordenador local.
 - La clave privada debe haberse guardado o anotado en el momento de su creación. Si no tienes la clave privada original, debes crear una nueva.
- Para editar un certificado de cliente:
 - Tienes la dirección IP o el nombre de dominio del Admin Node.
 - Para cargar tu propio certificado o un certificado nuevo, la clave privada, el certificado de cliente y la CA (si se utiliza) están disponibles en tu ordenador local.

Agregar certificados de cliente

Para añadir el certificado de cliente, sigue uno de estos procedimientos:

- [El certificado de la interfaz de gestión ya está configurado](#)
- [Certificado de cliente emitido por una CA](#)
- [Certificado generado desde Grid Manager](#)

El certificado de la interfaz de gestión ya está configurado

Sigue este procedimiento para añadir un certificado de cliente si ya se ha configurado un certificado de interfaz de gestión utilizando una CA, un certificado de cliente y una clave privada proporcionados por el cliente.

Pasos

1. En el Grid Manager, selecciona **Configuración > Seguridad > Certificados** y luego selecciona la pestaña **Cliente**.
2. Selecciona **Add**.
3. Introduce un nombre para el certificado.
4. Para acceder a las métricas de Prometheus mediante tu herramienta de monitorización externa, selecciona **Allow prometheus**.
5. Selecciona **Continuar**.
6. En el paso **Adjuntar certificados**, sube el certificado de la interfaz de gestión.
 - a. Selecciona **Cargar certificado**.
 - b. Selecciona **Examinar** y elige el archivo del certificado de la interfaz de gestión (.pem).
 - Selecciona **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el certificado PEM.
 - Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
 - c. Selecciona **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la pestaña Cliente.

7. [Configura una herramienta de supervisión externa](#), como Grafana.

Certificado de cliente emitido por una CA

Sigue este procedimiento para añadir un certificado de cliente de administrador si no se ha configurado ningún certificado de interfaz de gestión y tienes previsto añadir un certificado de cliente para Prometheus que utilice un certificado de cliente y una clave privada emitidos por una autoridad de certificación (CA).

Pasos

1. Sigue los pasos para ["configurar un certificado de la interfaz de gestión"](#).
2. En el Grid Manager, selecciona **Configuración > Seguridad > Certificados** y luego selecciona la pestaña **Cliente**.
3. Selecciona **Add**.
4. Introduce un nombre para el certificado.

5. Para acceder a las métricas de Prometheus mediante tu herramienta de monitorización externa, selecciona **Allow prometheus**.
6. Selecciona **Continuar**.
7. En el paso **Adjuntar certificados**, sube los archivos del certificado de cliente, la clave privada y el paquete de la CA:
 - a. Selecciona **Cargar certificado**.
 - b. Selecciona **Examinar** y elige los archivos del certificado de cliente, la clave privada y el paquete de CA (.pem).
 - Selecciona **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el certificado PEM.
 - Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
 - c. Selecciona **Crear** para guardar el certificado en Grid Manager.

Los nuevos certificados aparecen en la pestaña Cliente.

8. [Configura una herramienta de supervisión externa](#), como Grafana.

Certificado generado desde Grid Manager

Sigue este procedimiento para añadir un certificado de cliente de administrador si no se ha configurado ningún certificado de interfaz de gestión y tienes previsto añadir un certificado de cliente para Prometheus que utiliza la función de generar certificados en Grid Manager.

Pasos

1. En el Grid Manager, selecciona **Configuración > Seguridad > Certificados** y luego selecciona la pestaña **Cliente**.
2. Selecciona **Add**.
3. Introduce un nombre para el certificado.
4. Para acceder a las métricas de Prometheus mediante tu herramienta de monitorización externa, selecciona **Allow prometheus**.
5. Selecciona **Continuar**.
6. En el paso **Adjuntar certificados**, selecciona **Generar certificado**.
7. Indica la información del certificado:
 - **Sujeto** (opcional): sujeto X.509 o nombre distintivo (DN) del titular del certificado.
 - **Días de validez**: el número de días durante los que el certificado generado es válido, a partir del momento en que se genera.
 - **Agregar extensiones de uso de clave**: Si seleccionas esta opción (predeterminada y recomendada), se añaden al certificado generado las extensiones de uso de clave y de uso de clave ampliado.

Estas extensiones definen la finalidad de la clave incluida en el certificado.



Deja esta casilla marcada a menos que tengas problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.

8. Selecciona **Generar**.

9. Selecciona **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el certificado PEM.



No podrás ver la clave privada del certificado después de cerrar el cuadro de diálogo. Copia o descarga la clave en una ubicación segura.

- Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
- Selecciona **Descargar certificado** para guardar el archivo del certificado.

Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Selecciona **Copiar clave privada** para copiar la clave privada del certificado y pegarla en otro lugar.
- Selecciona **Descargar clave privada** para guardar la clave privada en un archivo.

Indica el nombre del archivo de la clave privada y la ubicación de descarga.

10. Selecciona **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la pestaña Cliente.

11. En el Grid Manager, selecciona **Configuración > Seguridad > Certificados** y luego selecciona la pestaña **Global**.
12. Selecciona **Management Interface certificate**.
13. Selecciona **Usar certificado personalizado**.
14. Sube los archivos `certificate.pem` y `private_key.pem` del paso [Datos del certificado de cliente](#). No es necesario subir el paquete de CA.
- a. Selecciona **Cargar certificado** y luego selecciona **Continuar**.
 - b. Sube cada archivo de certificado (`.pem`).
 - c. Selecciona **Guardar** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la página de certificados de la interfaz de administración.

15. [Configura una herramienta de supervisión externa](#), como Grafana.

Configura una herramienta de supervisión externa

Pasos

1. Configura los siguientes ajustes en tu herramienta de monitorización externa, como Grafana.
 - a. **Nombre:** Introduce un nombre para la conexión.

StorageGRID no requiere esta información, pero debes introducir un nombre para comprobar la conexión.
 - b. **URL:** introduce el nombre de dominio o la dirección IP del nodo de administración. Especifica HTTPS y el puerto 9091.

Por ejemplo: `https://admin-node.example.com:9091`

c. Activa **Autenticación de cliente TLS y Con certificado de CA**.

d. En «Detalles de autenticación TLS/SSL», copia y pega: +

- El certificado CA de la interfaz de gestión a **CA Cert**
- El certificado de cliente en **Client Cert**
- La clave privada de **Client Key**

e. **ServerName**: introduce 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 gestión.

2. Guarda y prueba el certificado y la clave privada que copiaste de StorageGRID o de un archivo local.

Ahora puedes acceder a las métricas de Prometheus desde StorageGRID con tu herramienta de monitorización externa.

Para obtener información sobre las métricas, consulta ["Instrucciones para monitorear StorageGRID"](#).

Editar certificados de cliente

Puedes editar el certificado de cliente de un administrador para cambiar su nombre, habilitar o deshabilitar el acceso a Prometheus, o subir un nuevo certificado cuando el actual haya caducado.

Pasos

1. Selecciona **Configuración > Seguridad > Certificados** y luego selecciona la pestaña **Cliente**.

En la tabla se indican las fechas de caducidad de los certificados y los permisos de acceso a Prometheus. Si un certificado está a punto de caducar o ya ha caducado, aparece un mensaje en la tabla y se activa una alerta.

2. Selecciona el certificado que deseas editar.

3. Selecciona **Editar** y luego selecciona **Editar nombre y permisos**

4. Introduce un nombre para el certificado.

5. Para acceder a las métricas de Prometheus mediante tu herramienta de monitorización externa, selecciona **Allow prometheus**.

6. Selecciona **Continuar** para guardar el certificado en Grid Manager.

El certificado actualizado aparece en la pestaña Cliente.

Adjuntar nuevo certificado de cliente

Puedes subir un nuevo certificado cuando el actual haya caducado.

Pasos

1. Selecciona **Configuración > Seguridad > Certificados** y luego selecciona la pestaña **Cliente**.

En la tabla se indican las fechas de caducidad de los certificados y los permisos de acceso a Prometheus. Si un certificado está a punto de caducar o ya ha caducado, aparece un mensaje en la tabla y se activa una alerta.

2. Selecciona el certificado que deseas editar.
3. Selecciona **Editar** y luego selecciona una opción de edición.

Subir certificado

Copia el texto del certificado para pegarlo en otro sitio.

- a. Selecciona **Cargar certificado** y luego selecciona **Continuar**.
- b. Sube el nombre del certificado de cliente (.pem).

Selecciona **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el certificado PEM.

- Selecciona **Descargar certificado** para guardar el archivo del certificado.

Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión .pem.

Por ejemplo: storagegrid_certificate.pem

- Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
- c. Selecciona **Crear** para guardar el certificado en Grid Manager.

El certificado actualizado aparece en la pestaña Cliente.

Generar certificado

Genera el texto del certificado para pegarlo en otro sitio.

- a. Selecciona **Generar certificado**.
- b. Indica la información del certificado:

- **Sujeto** (opcional): sujeto X.509 o nombre distintivo (DN) del titular del certificado.
- **Días de validez**: el número de días durante los que el certificado generado es válido, a partir del momento en que se genera.
- **Agregar extensiones de uso de clave**: Si seleccionas esta opción (predeterminada y recomendada), se añaden al certificado generado las extensiones de uso de clave y de uso de clave ampliado.

Estas extensiones definen la finalidad de la clave incluida en el certificado.



Deja esta casilla marcada a menos que tengas problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.

- c. Selecciona **Generar**.
- d. Selecciona **Detalles del certificado de cliente** para mostrar los metadatos del certificado y el certificado PEM.



No podrás ver la clave privada del certificado después de cerrar el cuadro de diálogo. Copia o descarga la clave en una ubicación segura.

- Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

- Selecciona **Descargar certificado** para guardar el archivo del certificado.

Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Selecciona **Copiar clave privada** para copiar la clave privada del certificado y pegarla en otro lugar.
- Selecciona **Descargar clave privada** para guardar la clave privada en un archivo.

Indica el nombre del archivo de la clave privada y la ubicación de descarga.

e. Selecciona **Crear** para guardar el certificado en Grid Manager.

El nuevo certificado aparece en la pestaña Cliente.

Descargar o copiar certificados de cliente

Puedes descargar o copiar un certificado de cliente para utilizarlo en otro lugar.

Pasos

1. Selecciona **Configuración > Seguridad > Certificados** y luego selecciona la pestaña **Cliente**.
2. Selecciona el certificado que quieras copiar o descargar.
3. Descarga o copia el certificado.

Descargar el archivo del certificado

Descarga el archivo de certificado `.pem`.

- a. Selecciona **Descargar certificado**.
- b. Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

Copiar certificado

Copia el texto del certificado para pegarlo en otro sitio.

- a. Selecciona **Copiar certificado PEM**.
- b. Pega el certificado copiado en un editor de texto.
- c. Guarda el archivo de texto con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

Eliminar certificados de cliente

Si ya no necesitas un certificado de cliente de administrador, puedes eliminarlo.

Pasos

1. Selecciona **Configuración > Seguridad > Certificados** y luego selecciona la pestaña **Cliente**.
2. Selecciona el certificado que deseas eliminar.
3. Selecciona **Eliminar** y luego confirma.



Para eliminar hasta 10 certificados, selecciona cada certificado que quieras eliminar en la pestaña Cliente y luego selecciona **Acciones > Eliminar**.

Después de que se elimina un certificado, los clientes que usaban ese certificado deben especificar un nuevo certificado de cliente para acceder a la base de datos de StorageGRID Prometheus.

Configura los ajustes de seguridad

Administra la política TLS y SSH en StorageGRID

La política de TLS y SSH determina qué protocolos y algoritmos de cifrado se utilizan para establecer conexiones TLS seguras con las aplicaciones cliente y conexiones SSH seguras con los servicios internos de StorageGRID.

La política de seguridad controla cómo TLS y SSH cifran los datos en tránsito. En general, utiliza la política «Compatibilidad moderna» (predeterminada), a menos que tu sistema deba cumplir con Common Criteria o que necesites usar otros cifrados.



Algunos servicios de StorageGRID no se han actualizado para usar los cifrados en estas políticas.

Antes de empezar

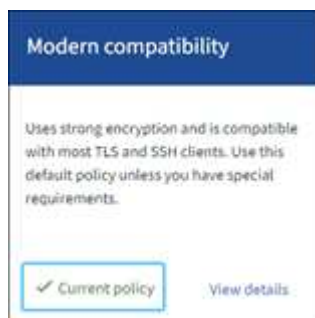
- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).

Selecciona una política de seguridad

Pasos

1. Selecciona **Configuración > Seguridad > Ajustes de seguridad**.

La pestaña **Políticas de TLS y SSH** muestra las políticas disponibles. La política activa actualmente se identifica con una marca de verificación verde en el mosaico de la política.



2. Consulta las pestañas para conocer las políticas disponibles.

Compatibilidad moderna (predeterminada)

Usa la política predeterminada si necesitas un cifrado robusto y no tienes requisitos especiales. Esta política es compatible con la mayoría de los clientes TLS y SSH.

Compatibilidad con versiones anteriores

Utiliza la política de compatibilidad Legacy si necesitas opciones de compatibilidad adicionales para clientes más antiguos. Las opciones adicionales de esta política pueden hacer que sea menos segura que la política de compatibilidad Modern.

Criterios Comunes

Utiliza la política de Common Criteria si necesitas la certificación de Common Criteria.

FIPS estricto

Usa la política estricta de FIPS si necesitas la certificación Common Criteria y tienes que usar el módulo NetApp Cryptographic Security Module (NCSM) 3.0.8 o el módulo NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 para las conexiones de clientes externos con los endpoints del equilibrador de carga, Tenant Manager y Grid Manager. El uso de esta política podría reducir el rendimiento.

El módulo NCSM 3.0.8 y el módulo NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 se usan en las siguientes operaciones:

- NCSM

- Conexiones TLS entre los siguientes servicios: ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw y cache-svc
- Conexiones TLS entre los clientes y el servicio nginx-gw (puntos finales del equilibrador de carga)
- Conexiones TLS entre los clientes y el servicio LDR
- Cifrado del contenido de objetos para SSE-S3, SSE-C y la configuración de cifrado de objetos almacenados
- Conexiones SSH

Para obtener más información, consulta el NIST Cryptographic Algorithm Validation Program "[Certificado n.º 4838](#)".

- NetApp Módulo Kernel Crypto API de StorageGRID

El módulo NetApp StorageGRID Kernel Crypto API solo está presente en plataformas de máquinas virtuales (VM) y dispositivos StorageGRID.

- Recolección de entropía
- Cifrado de nodos

Para obtener más información, consulta el Programa de Validación de Algoritmos Criptográficos de NIST "[Certificados del n.º A6242 al n.º A6257](#)" y "[Certificado de Entropy n.º E223](#)".

Nota: Después de seleccionar esta política, "[realizar un reinicio progresivo](#)" en todos los nodos para activar el NCSM. Usa **Mantenimiento > Reinicio progresivo** para iniciar y monitorear los reinicios.

Personalizado

Crea una política personalizada si necesitas aplicar tus propios cifrados.

Opcionalmente, si tu StorageGRID tiene requisitos de criptografía FIPS 140, activa la función de modo FIPS para usar el módulo NCSM 3.0.8 y el módulo NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64:

- Establece el parámetro `fipsMode` en `true`.
- Cuando se te solicite, "[realizar un reinicio progresivo](#)" en todos los nodos para activar los módulos de criptografía. Usa **Mantenimiento > Reinicio progresivo** para iniciar y supervisar los reinicios.
- Selecciona **Soporte > Diagnóstico** para ver las versiones activas de los módulos FIPS.

- Para ver los detalles sobre los cifrados, protocolos y algoritmos de cada política, selecciona **Ver detalles**.
- Para cambiar la política actual, selecciona **Usar política**.

Aparece una marca de verificación verde junto a **Current policy** en el mosaico de la política.

Crear una política de seguridad personalizada

Puedes crear una política personalizada si necesitas aplicar tus propios cifrados.

Pasos

- En la ficha de la política que más se parezca a la política personalizada que quieres crear, selecciona **Ver detalles**.
- Selecciona **Copiar al portapapeles** y luego selecciona **Cancelar**.



- En el mosaico **Política personalizada**, selecciona **Configurar y usar**.
- Pega el JSON que copiaste y haz los cambios que sean necesarios.
- Selecciona **Usar política**.

Aparece una marca de verificación verde junto a **Política actual** en el mosaico **Política personalizada**.

- Si lo deseas, selecciona **Editar configuración** para realizar más cambios en la nueva política personalizada.

Volver temporalmente a la política de seguridad predeterminada

Si has configurado una política de seguridad personalizada, puede que no puedas iniciar sesión en Grid Manager si la política TLS configurada es incompatible con ["certificado de servidor configurado"](#).

Puedes volver temporalmente a la política de seguridad predeterminada.

Pasos

1. Inicia sesión en un nodo de administración:
 - a. Introduce el siguiente comando: `ssh admin@Admin_Node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

2. Ejecuta el siguiente comando:

```
restore-default-cipher-configurations
```

3. Desde un navegador web, accede al Grid Manager en el mismo nodo de administración.
4. Sigue los pasos de [Selecciona una política de seguridad](#) para volver a configurar la política.

Configura la red StorageGRID y la seguridad de objetos

Puedes configurar la seguridad de la red y de los objetos para cifrar los objetos almacenados, impedir determinadas solicitudes S3 o permitir que las conexiones de los clientes a los Storage Nodes utilicen HTTP en lugar de HTTPS.

Cifrado de objetos almacenados

El cifrado de objetos almacenados permite cifrar todos los datos de los objetos a medida que se importan a través de S3. De forma predeterminada, los objetos almacenados no están cifrados, pero puedes optar por cifrarlos utilizando el algoritmo de cifrado AES-128 o AES-256. Al habilitar esta configuración, todos los objetos recién importados se cifran, pero no se produce ningún cambio en los objetos ya almacenados. Si deshabilitas el cifrado, los objetos que ya están cifrados permanecen así, pero los objetos recién importados no se cifran.

La configuración de cifrado de objetos almacenados solo se aplica a los objetos de S3 que no hayan sido cifrados mediante el cifrado a nivel de bucket o a nivel de objeto.

Para obtener más información sobre los métodos de cifrado de StorageGRID, consulta ["Revisa los métodos de cifrado de StorageGRID"](#).

Impedir que el cliente realice modificaciones

Impedir la modificación por parte del cliente es una configuración válida para todo el sistema. Cuando se selecciona la opción **Impedir la modificación por parte del cliente**, se rechazan las siguientes solicitudes.

API de REST de S3

- DeleteBucket solicitudes
- Cualquier solicitud para modificar los datos de un objeto existente, los metadatos definidos por el usuario o el etiquetado de objetos S3

Habilita HTTP para las conexiones del nodo de almacenamiento

De forma predeterminada, las aplicaciones cliente utilizan el protocolo de red HTTPS para cualquier conexión directa con los nodos de almacenamiento. Si lo deseas, puedes habilitar HTTP para estas conexiones, por ejemplo, al realizar pruebas en una red que no sea de producción.

Utiliza HTTP para las conexiones con los nodos de almacenamiento únicamente si los clientes S3 necesitan establecer conexiones HTTP directamente con los nodos de almacenamiento. No necesitas usar esta opción para los clientes que solo usan conexiones HTTPS o para los clientes que se conectan al servicio de Load Balancer (porque puedes ["configurar cada endpoint del balanceador de carga"](#) usar tanto HTTP como HTTPS).

Consulta ["Resumen: direcciones IP y puertos para las conexiones de los clientes"](#) para saber qué puertos usan los clientes S3 al conectarse a los nodos de almacenamiento mediante HTTP o HTTPS.

Selecciona opciones

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes permiso de acceso root.

Pasos

1. Selecciona **Configuración > Seguridad > Ajustes de seguridad**.
2. Selecciona la pestaña **Red y objetos**.
3. Para el cifrado de objetos almacenados, utiliza la configuración **Ninguna** (predeterminada) si no quieres que los objetos almacenados se cifren, o selecciona **AES-128** o **AES-256** para cifrar los objetos almacenados.
4. Si lo deseas, selecciona **Impedir la modificación por parte del cliente** si quieres evitar que los clientes de S3 realicen solicitudes específicas.



Si modificas esta configuración, la nueva configuración tardará aproximadamente un minuto en aplicarse. El valor configurado se almacena en caché para mejorar el rendimiento y la escalabilidad.

5. Opcionalmente, selecciona **Habilitar HTTP para las conexiones a los nodos de almacenamiento** si los clientes se conectan directamente a los nodos de almacenamiento y quieres usar conexiones HTTP.



Ten cuidado al habilitar HTTP en una red de producción porque las solicitudes se enviarán sin cifrar.

6. Selecciona **Guardar**.

Cambiar la configuración de seguridad de la interfaz StorageGRID

La configuración de seguridad de la interfaz te permite controlar si se cierra la sesión de

los usuarios cuando permanecen inactivos durante más del tiempo especificado y si se incluye un seguimiento de la pila en las respuestas de error de la API.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["Permiso de acceso raíz"](#).

Acerca de esta tarea

La página **Configuración de seguridad** incluye los parámetros **Tiempo de espera por inactividad del navegador** y **Rastreo de pila de la Management API**.

Tiempo de espera por inactividad del navegador

Indica cuánto tiempo puede estar inactivo el navegador de un usuario antes de que se cierre su sesión. El valor predeterminado es de 15 minutos.

El tiempo de espera por inactividad del navegador también se controla mediante lo siguiente:

- Un temporizador independiente de StorageGRID, no configurable, que se incluye por motivos de seguridad del sistema. El token de autenticación de cada usuario caduca 16 horas después de que el usuario inicia sesión. Cuando caduca la autenticación de un usuario, ese usuario se desconecta automáticamente, incluso si el tiempo de espera por inactividad del navegador está desactivado o no se ha alcanzado el valor para el tiempo de espera del navegador. Para renovar el token, el usuario debe volver a iniciar sesión.
- Configuración del tiempo de espera para el proveedor de identidad, suponiendo que el inicio de sesión único (SSO) esté habilitado para StorageGRID.

Si el SSO está habilitado y se agota el tiempo de espera del navegador de un usuario, el usuario debe volver a introducir sus credenciales de SSO para acceder de nuevo a StorageGRID. Consulta ["Cómo funciona el SSO"](#).

Traza de la pila de la Management API

Controla si se devuelve un seguimiento de la pila en las respuestas de error de la API de Grid Manager y Tenant Manager.

Esta opción está desactivada por defecto, pero es posible que quieras activar esta funcionalidad en un entorno de prueba. En general, deberías dejar desactivado el seguimiento de la pila en los entornos de producción para evitar revelar detalles internos del software cuando ocurren errores en la API.

Pasos

1. Selecciona **Configuración > Seguridad > Ajustes de seguridad**.
2. Selecciona la pestaña **Interfaz**.
3. Para cambiar la configuración del tiempo de espera de inactividad del navegador:
 - a. Despliega el acordeón.
 - b. Para cambiar el tiempo de espera, especifica un valor comprendido entre 60 segundos y 7 días. El tiempo de espera predeterminado es de 15 minutos.
 - c. Para desactivar esta función, desmarca la casilla.
 - d. Selecciona **Guardar**.

La nueva configuración no afecta a los usuarios que ya hayan iniciado sesión. Los usuarios deben

volver a iniciar sesión o actualizar su navegador para que la nueva configuración del tiempo de espera surta efecto.

4. Para cambiar la configuración del seguimiento de la pila de la Management API:

- a. Despliega el acordeón.
- b. Marca la casilla de verificación para devolver un seguimiento de la pila en las respuestas de error de la API de Grid Manager y Tenant Manager.



Mantén desactivada la traza de pila en los entornos de producción para evitar revelar detalles internos del software cuando ocurran errores en la API.

- c. Selecciona **Guardar**.

Administra el acceso SSH externo en StorageGRID

Gestiona el acceso SSH para el tráfico entrante en el grid bloqueando o permitiendo el acceso externo. Gestionar el acceso externo por SSH no afecta al tráfico entre nodos en el grid.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["Permiso de acceso raíz"](#).

Acerca de esta tarea

Para mejorar la seguridad del sistema, el acceso SSH externo está bloqueado de forma predeterminada. Si necesitas realizar tareas que requieran acceso SSH entrante, como la resolución de problemas, permite temporalmente el acceso externo. Cuando hayas terminado la tarea, bloquea el acceso externo.

Pasos

1. Selecciona **Configuración > Seguridad > Ajustes de seguridad**.
2. Selecciona la pestaña **Bloquear SSH**.
3. Utiliza la opción **Bloquear el acceso SSH entrante** para gestionar el acceso SSH externo:
 - a. Marca la casilla para bloquear el acceso (predeterminado).
 - b. Desmarca la casilla para permitir el acceso.



Requiere acceso en el puerto 22 entre el portátil de servicio y todos los demás nodos de grid. Elimina el acceso en el puerto 22 cuando completes la tarea de mantenimiento.

4. Selecciona **Guardar**.

Configura servidores de gestión de claves

Conoce los servidores de gestión de claves en StorageGRID

Un servidor de gestión de claves (KMS) es un sistema externo de terceros que proporciona claves de cifrado a los nodos de los dispositivos StorageGRID en el sitio de StorageGRID asociado mediante el Protocolo de Interoperabilidad de Gestión de Claves (KMIP).

StorageGRID solo admite determinados servidores de gestión de claves. Para obtener una lista de los productos y versiones compatibles, usa la ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Puedes usar uno o varios servidores de gestión de claves para gestionar las claves de cifrado de los nodos de cualquier dispositivo StorageGRID que tenga habilitada la opción **Node Encryption** durante la instalación. Usar servidores de gestión de claves con estos nodos de dispositivo te permite proteger tus datos incluso si se retira un dispositivo del centro de datos. Después de que los volúmenes del dispositivo estén cifrados, no puedes acceder a ningún dato en el dispositivo a menos que el nodo pueda comunicarse con el KMS.

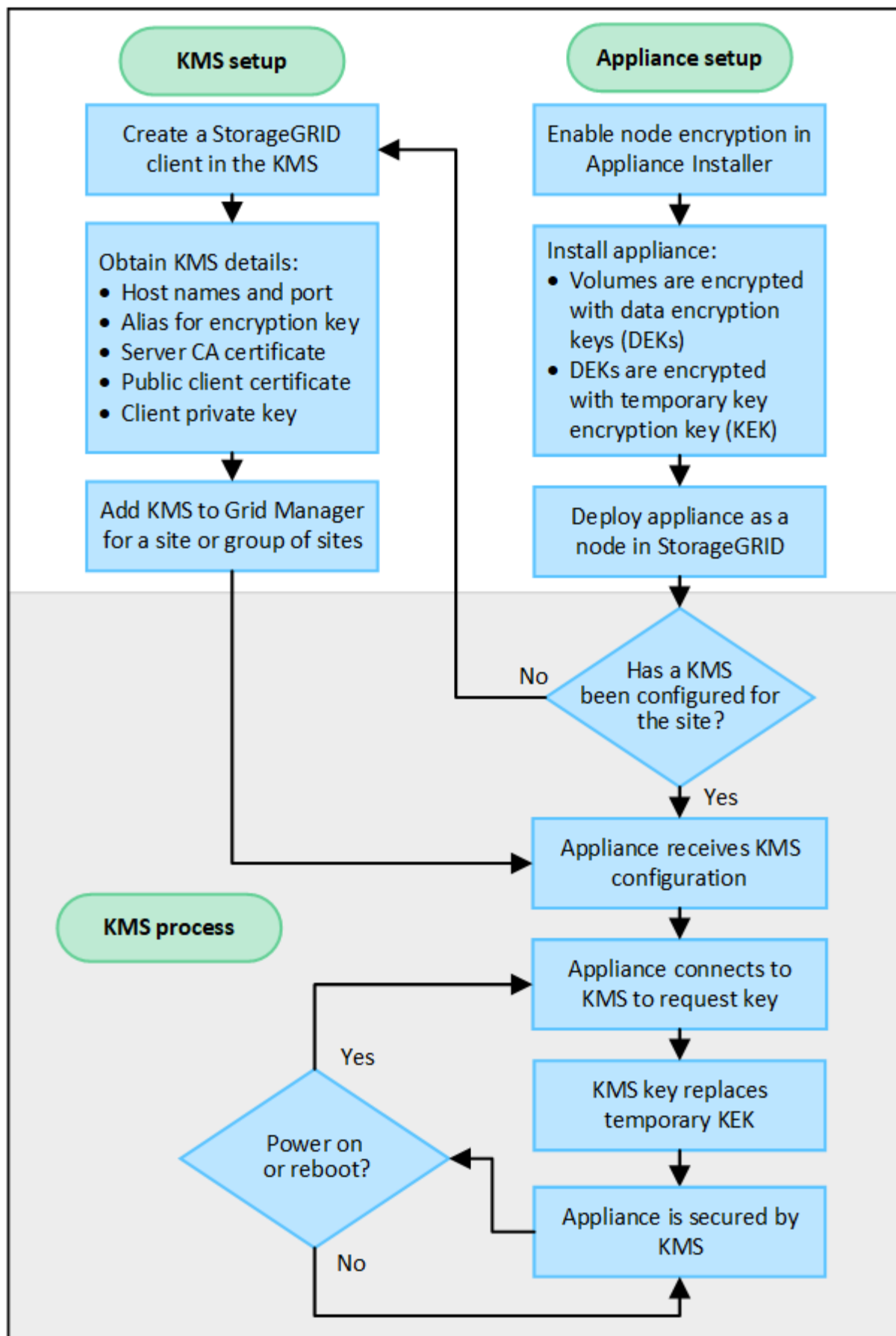


StorageGRID no crea ni gestiona las claves externas utilizadas para cifrar y descifrar los nodos del appliance. Si tienes pensado utilizar un servidor de gestión de claves externo para proteger los datos de StorageGRID, debes comprender cómo configurar ese servidor y cómo gestionar las claves de cifrado. Realizar las tareas de gestión de claves queda fuera del alcance de estas instrucciones. Si necesitas ayuda, consulta la documentación de tu servidor de gestión de claves o ponte en contacto con el soporte técnico.

Configuración del servidor de gestión de claves StorageGRID y de los dispositivos

Antes de que puedas usar un servidor de gestión de claves (KMS) para proteger los datos de StorageGRID en los nodos del dispositivo, debes completar dos tareas de configuración: configurar uno o más servidores KMS y habilitar el cifrado de los nodos del dispositivo. Cuando estas dos tareas de configuración estén completas, el proceso de gestión de claves ocurre automáticamente.

El diagrama de flujo muestra los pasos a grandes rasgos para usar un KMS y proteger los datos de StorageGRID en los nodos de los dispositivos.



El diagrama de flujo muestra que la configuración de KMS y la configuración del dispositivo se realizan en

paralelo; sin embargo, puedes configurar los servidores de gestión de claves antes o después de habilitar el cifrado de nodos para los nuevos nodos del dispositivo, en función de tus necesidades.

Configura el servidor de gestión de claves (KMS)

La configuración de un servidor de gestión de claves incluye los siguientes pasos a grandes rasgos.

Paso	Consulta
Accede al software KMS y añade un cliente de StorageGRID a cada KMS o KMS cluster.	"Configura StorageGRID como cliente en el KMS"
Obtén la información necesaria para el cliente de StorageGRID en el KMS.	"Configura StorageGRID como cliente en el KMS"
Agrega el KMS al Grid Manager, asígnalo a un solo sitio o a un grupo predeterminado de sitios, sube los certificados requeridos y guarda la configuración del KMS.	"Agrega un servidor de gestión de claves (KMS)"

Configura el appliance

La configuración de un nodo de dispositivo para su uso con KMS incluye los siguientes pasos a grandes rasgos.

1. Durante la fase de configuración del hardware de la instalación del dispositivo, utiliza el StorageGRID Appliance Installer para activar la opción **Node Encryption** del dispositivo.



No puedes activar la opción **Cifrado de nodos** después de añadir un appliance a la grid, y no puedes usar la gestión externa de claves para appliances que no tengan activado el cifrado de nodos.

2. Ejecuta el StorageGRID Appliance Installer. Durante la instalación, se asigna una clave de cifrado de datos (DEK) aleatoria a cada volumen del dispositivo, de la siguiente manera:
 - Las DEK se usan para cifrar los datos de cada volumen. Estas claves se generan mediante el cifrado de disco Linux Unified Key Setup (LUKS) en el SO del appliance y no se pueden cambiar.
 - Cada DEK individual se cifra mediante una clave maestra de cifrado (KEK). La KEK inicial es una clave temporal que cifra las DEK hasta que el dispositivo pueda conectarse al KMS.
3. Agrega el nodo del dispositivo a StorageGRID.

Consulta ["Habilitar el cifrado de nodos"](#) para más detalles.

Proceso de cifrado con gestión de claves (ocurre automáticamente)

El cifrado con gestión de claves incluye los siguientes pasos a grandes rasgos que se llevan a cabo de forma automática.

1. Al instalar en la red un dispositivo que tiene activado el cifrado de nodos, StorageGRID comprueba 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 del KMS.

- Si aún no se ha configurado un KMS para el sitio, los datos del appliance seguirán cifrándose mediante la KEK temporal hasta que configures un KMS para el sitio y el appliance 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 sustituye a 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, no debes considerar que los volúmenes del dispositivo estén protegidos frente a su retirada del centro de datos hasta que la clave de cifrado de KMS sustituya a la clave temporal.

- 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 sobrevive a una pérdida de alimentación o a un reinicio.

Requisitos y consideraciones del servidor de gestión de claves StorageGRID

Antes de configurar un servidor externo de gestión de claves (KMS), debes conocer las consideraciones y los requisitos.

¿Qué versión de KMIP es compatible?

StorageGRID es compatible con la versión 1.4 de KMIP.

["Especificación del Protocolo de Interoperabilidad para la Gestión de Claves versión 1.4"](#)

¿Cuáles son las consideraciones de red?

La configuración del cortafuegos de red debe permitir que cada nodo del dispositivo se comuniquen a través del puerto utilizado para las comunicaciones del Protocolo de Interoperabilidad de Gestión de Claves (KMIP). El puerto KMIP predeterminado es 5696.

Debes asegurarte de que cada nodo de dispositivo que utilice el cifrado de nodos tenga acceso de red al KMS o al clúster de KMS que configuraste 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 clúster de KMS, según lo que admita el KMS y qué ["Política de TLS y SSH"](#) estés utilizando.

StorageGRID negocia el protocolo y el cifrado (TLS 1.2) o el conjunto de cifrados (TLS 1.3) con el KMS al establecer la conexión. Para ver qué versiones de protocolo y cifrados o conjuntos de cifrado están disponibles, revisa la sección `tlsOutbound` de la política activa de TLS y SSH del grid (**Configuration > Security Security settings**).

¿Qué dispositivos son compatibles?

Puedes utilizar un servidor de gestión de claves (KMS) para gestionar las claves de cifrado de cualquier dispositivo StorageGRID de tu grid que tenga activada la opción **Node Encryption**. Esta opción solo se puede activar durante la etapa de configuración del hardware de la instalación del dispositivo usando el StorageGRID Appliance Installer.



No puedes activar el cifrado de nodos después de añadir un dispositivo a la grid, y no puedes usar la gestión externa de claves para los dispositivos que no tienen activado el cifrado de nodos.

Puedes utilizar el KMS configurado para los dispositivos StorageGRID y los nodos de los dispositivos.

No puedes utilizar el KMS configurado para nodos basados en software (que no sean dispositivos), entre los que se incluyen los siguientes:

- Nodos implementados como máquinas virtuales (VM)
- Nodos implementados en motores de contenedores en hosts Linux

Los nodos implementados en estas otras plataformas pueden usar el cifrado fuera de StorageGRID a nivel de almacén de datos o de disco.

¿Cuándo debo configurar los servidores de gestión de claves?

En una nueva instalación, lo habitual es configurar uno o varios servidores de gestión de claves en Grid Manager antes de crear inquilinos. Este orden garantiza que los nodos estén protegidos antes de que se almacene cualquier dato de objeto en ellos.

Puedes configurar los servidores de gestión de claves en Grid Manager antes o después de instalar los nodos del appliance.

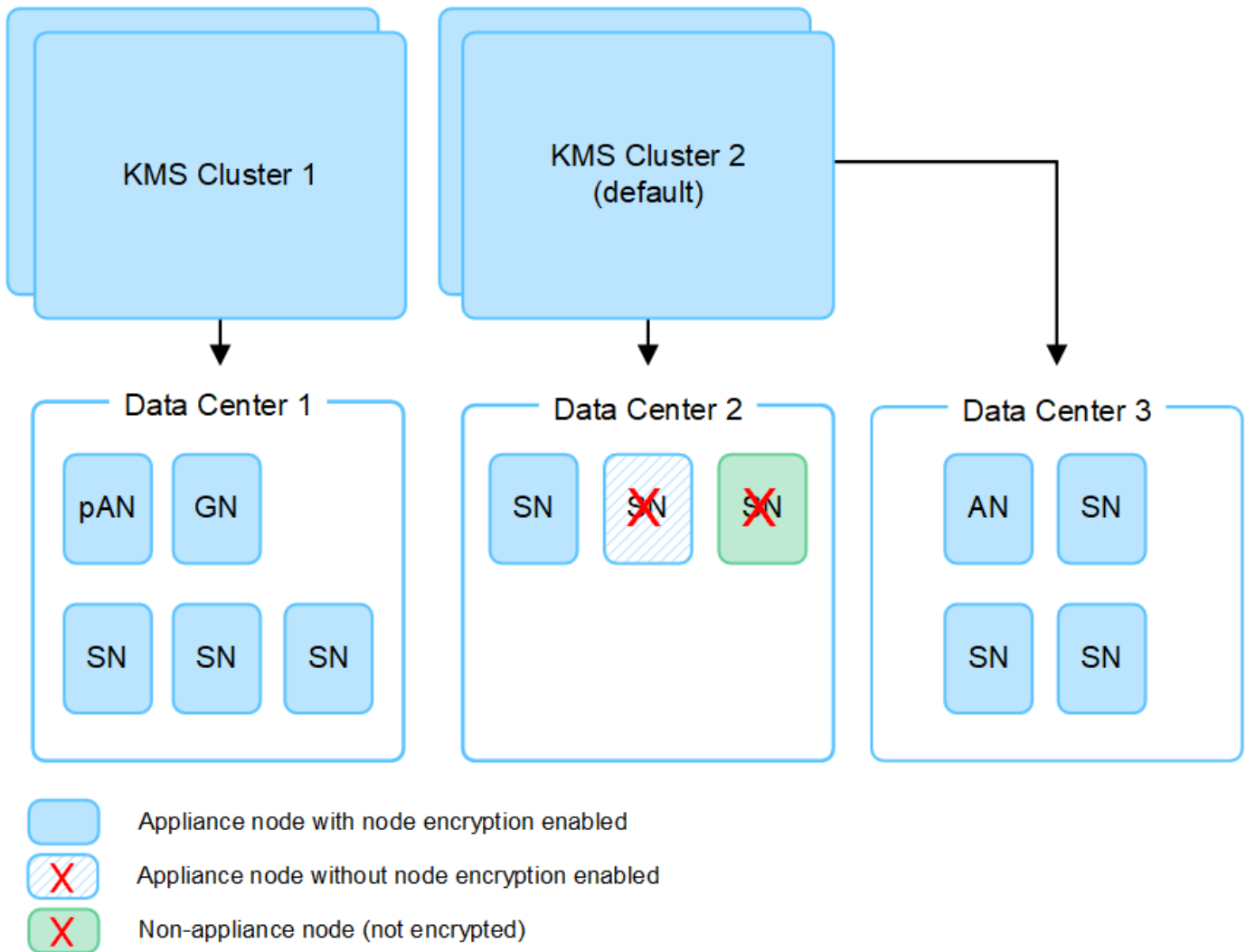
¿Cuántos servidores de gestión de claves necesito?

Puedes configurar uno o varios servidores de gestión de claves externos para proporcionar claves de cifrado a los nodos de appliance en tu sistema StorageGRID. Cada KMS proporciona una única clave de cifrado a los nodos de appliance de StorageGRID en un solo sitio o en un grupo de sitios.

StorageGRID admite el uso de clústeres de KMS. Cada clúster de KMS contiene varios servidores de gestión de claves replicados que comparten los ajustes de configuración y las claves de cifrado. Se recomienda usar clústeres de KMS para la gestión de claves, ya que mejora las capacidades de conmutación por error de una configuración de alta disponibilidad.

Por ejemplo, supón que tu sistema StorageGRID tiene tres centros de datos. Podrías configurar un clúster KMS para proporcionar una clave a todos los nodos de los dispositivos en el Data Center 1 y un segundo clúster KMS para proporcionar una clave a todos los nodos de los dispositivos en los demás sitios. Cuando añades el segundo clúster KMS, puedes configurar un KMS predeterminado para Data Center 2 y Data Center 3.

Ten en cuenta que no puedes utilizar un KMS para nodos que no sean de appliance ni para ningún nodo de appliance que no tuviera activada la configuración **Cifrado de nodo** durante la instalación.



¿Qué ocurre cuando se rota una clave?

Como práctica recomendada de seguridad, deberías **"rotar la clave de cifrado"** periódicamente que usa cada KMS configurado.

Cuando la nueva versión de la clave esté disponible:

- Se distribuye automáticamente a los nodos de los dispositivos cifrados en el sitio o sitios asociados con el KMS. La distribución debería ocurrir dentro de una hora desde que se rota la clave.
- Si el nodo del dispositivo cifrado está desconectado cuando se distribuye la nueva versión de la clave, el nodo recibirá la nueva clave en cuanto se reinicie.
- Si por cualquier motivo la nueva versión de la clave no se puede usar para cifrar los volúmenes del dispositivo, se activará la alerta **Error en la rotación de la clave de cifrado de KMS** para el nodo del dispositivo. Es posible que necesites ponerte en contacto con el soporte técnico para obtener ayuda para resolver esta alerta.

¿Puedo volver a utilizar un nodo de appliance después de que haya sido cifrado?

Si necesitas instalar un dispositivo cifrado en otro sistema StorageGRID, primero debes decomisionar el nodo de grid para mover los datos de objetos a otro nodo. Después, puedes usar el StorageGRID Appliance Installer para **"borrar la configuración de KMS"**. Al borrar la configuración de KMS, se desactiva el ajuste **Node**

Encryption y se elimina la asociación entre el nodo del dispositivo y la configuración de KMS para el sitio de StorageGRID.



Sin acceso a la clave de cifrado KMS, cualquier dato que permanezca en el dispositivo ya no se podrá acceder y quedará bloqueado de forma permanente.

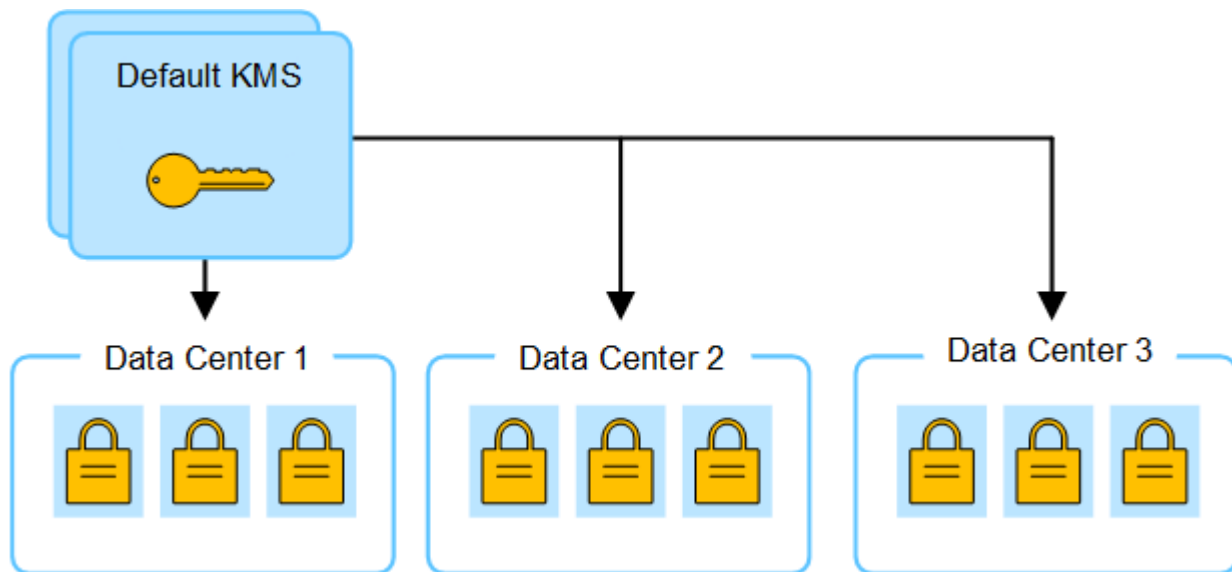
Consideraciones para cambiar el KMS de un sitio StorageGRID

Cada servidor de gestión de claves (KMS) o clúster de KMS proporciona una clave de cifrado a todos los nodos del appliance en una única sede o en un grupo de sedes. Si necesitas cambiar qué KMS se utiliza para una sede, es posible que tengas que copiar la clave de cifrado de un KMS a otro.

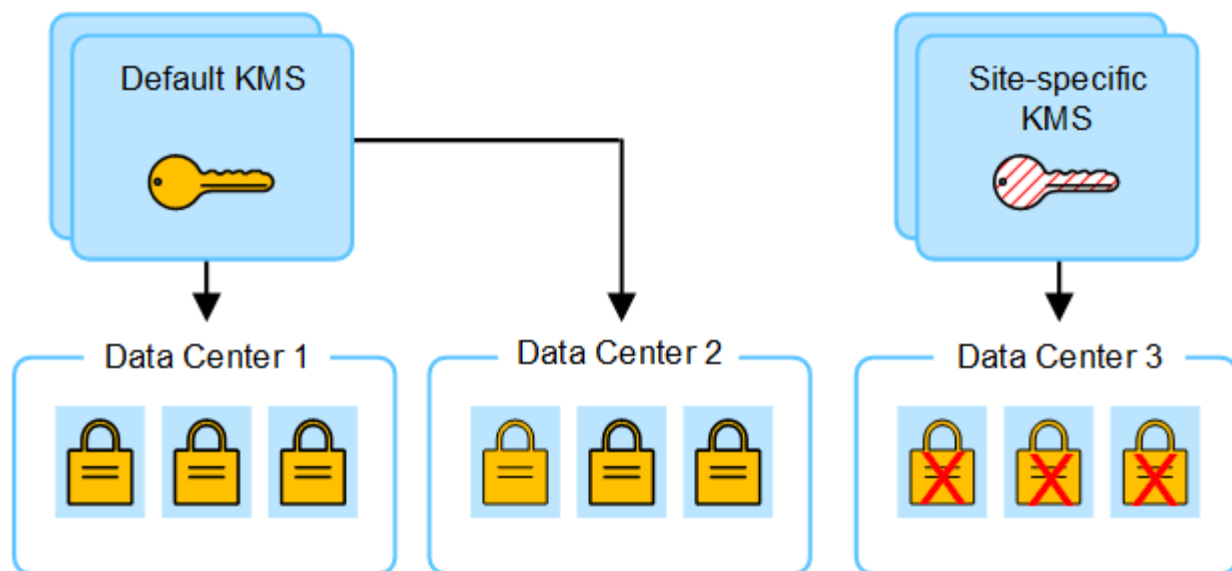
Si cambias el KMS utilizado para un sitio, debes asegurarte de que los nodos del dispositivo previamente cifrados en ese sitio puedan descifrarse usando la clave almacenada en el nuevo KMS. En algunos casos, podrías necesitar copiar la versión actual de la clave de cifrado del KMS original al nuevo KMS. Debes asegurarte de que el KMS tenga la clave correcta para descifrar los nodos del dispositivo cifrados en el sitio.

Por ejemplo:

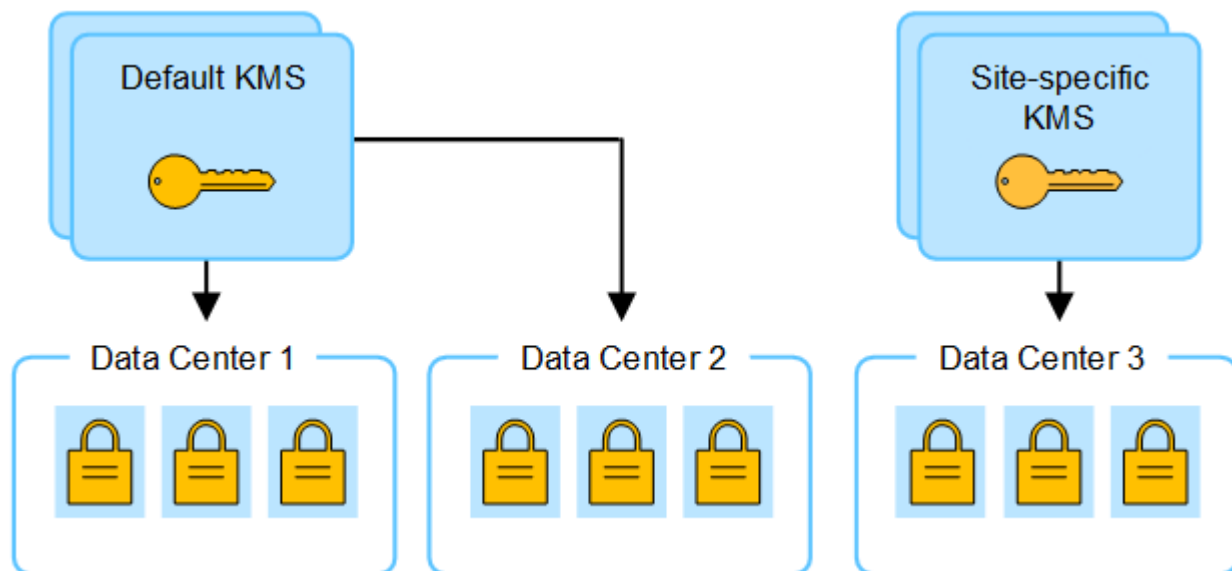
1. Inicialmente configuras un KMS predeterminado que se aplica a todos los sitios que no tienen un KMS dedicado.
2. Cuando se guarda el KMS, todos los nodos de appliance que tienen habilitada la configuración **Cifrado de nodos** se conectan al KMS y solicitan la clave de cifrado. Esta clave se utiliza para cifrar los nodos de appliance en todos los sitios. Esta misma clave también se debe utilizar para descifrar esos appliances.



3. Decides añadir un KMS específico para un sitio (el Data Center 3 de la figura). Sin embargo, porque los nodos del appliance ya están cifrados, ocurre un error de validación cuando intentas guardar la configuración para el KMS específico del sitio. El error ocurre porque el KMS específico del sitio no tiene la clave correcta para descifrar los nodos de ese sitio.



4. Para solucionar el problema, copias la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. (Técnicamente, copias la clave original a una nueva clave con el mismo alias. La clave original pasa a ser una versión anterior de la nueva clave.) El KMS específico del sitio ahora tiene la clave correcta para descifrar los nodos del dispositivo en Data Center 3, así que puede guardarse en StorageGRID.



Casos de uso para cambiar el KMS que se utiliza en un sitio

La tabla resume los pasos necesarios para los casos más comunes al cambiar el KMS de un sitio.

Caso de uso para cambiar el KMS de un sitio	Pasos necesarios
Tienes una o varias entradas de KMS específicas de cada sitio y quieres usar una de ellas como KMS predeterminado.	Edita el KMS específico del sitio. En el campo Gestiona claves para, selecciona Sitios no gestionados por otro KMS (KMS predeterminado). El KMS específico del sitio se usará ahora como el KMS predeterminado. Se aplicará a cualquier sitio que no tenga un KMS dedicado. "Editar un servidor de gestión de claves (KMS)"
Tienes un KMS predeterminado y añades un nuevo sitio en una ampliación. No quieres utilizar el KMS predeterminado para el nuevo sitio.	1. Si los nodos de los dispositivos de la nueva ubicación ya han sido cifrados mediante el KMS predeterminado, utiliza el software del KMS para copiar la versión actual de la clave de cifrado del KMS predeterminado a un nuevo KMS. 2. Usando el Grid Manager, añade el nuevo KMS y selecciona el sitio. "Agrega un servidor de gestión de claves (KMS)"
Quieres que el KMS de un sitio use un servidor diferente.	1. Si los nodos de los dispositivos de la sede ya han sido cifrados por el KMS existente, utiliza el software del KMS para copiar la versión actual de la clave de cifrado del KMS existente al nuevo KMS. 2. Mediante el Grid Manager, edita la configuración actual de KMS e introduce el nuevo nombre de host o la nueva dirección IP. "Agrega un servidor de gestión de claves (KMS)"

Configura StorageGRID como cliente en el KMS

Debes configurar StorageGRID como cliente para cada servidor externo de gestión de claves o clúster KMS antes de poder añadir el KMS a StorageGRID.



Estas instrucciones se aplican a Thales CipherTrust Manager y Hashicorp Vault. Para ver la lista de productos y versiones compatibles, usa el ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Pasos

1. Desde el software KMS, crea un cliente StorageGRID para cada KMS o clúster de KMS que planeas usar.

Cada KMS gestiona una única clave de cifrado para los nodos de los dispositivos StorageGRID de un único sitio o de un grupo de sitios.

2. Crea una clave utilizando uno de los dos métodos siguientes:
 - Utiliza la página de gestión de claves de tu producto KMS. Crea una clave de cifrado AES para cada KMS o clúster de KMS.

La clave de cifrado debe tener 2,048 bits o más y debe ser exportable.

- Haz que StorageGRID cree la clave. Se te pedirá cuando pruebes y guardes después de ["carga de certificados de cliente"](#).

3. Anota la siguiente información para cada KMS o clúster de KMS.

Necesitarás esta información cuando añadas el KMS a StorageGRID:

- Nombre de host o dirección IP de cada servidor.
- Puerto KMIP utilizado por el KMS.
- Alias de la clave de cifrado en el KMS.

4. Para cada KMS o clúster de KMS, obtén un certificado de servidor firmado por una autoridad de certificación (CA) o un paquete de certificados que contenga cada uno de los archivos de certificados de CA codificados en formato 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 usar el formato X.509 codificado en Base-64 Privacy Enhanced Mail (PEM).
- El campo «Nombre alternativo del sujeto» (SAN) de cada certificado de servidor debe incluir el nombre de dominio completo (FQDN) o la dirección IP a la que StorageGRID se conectará.



Al configurar el KMS en StorageGRID, debes introducir los mismos FQDN o direcciones IP en el campo **Hostname**.

- El certificado del servidor debe coincidir con el certificado utilizado por la interfaz KMIP del KMS, que suele utilizar el puerto 5696.

5. Obtén el certificado público de cliente emitido para StorageGRID por el KMS externo y la clave privada para el certificado de cliente.

El certificado de cliente permite a StorageGRID autenticarse ante el KMS.

Agrega un servidor de gestión de claves en StorageGRID

Usas el asistente de StorageGRID Key Management Server para añadir cada KMS o clúster KMS.

Antes de empezar

- Has revisado la "[Consideraciones y requisitos para usar un servidor de gestión de claves](#)".
- Tienes "[configuraste StorageGRID como cliente en el KMS](#)" y dispones de la información necesaria para cada KMS o clúster de KMS.
- Has iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tienes el "[Permiso de acceso raíz](#)".

Acerca de esta tarea

Si es posible, configura cualquier servidor de gestión de claves específico de un sitio antes de configurar un KMS predeterminado que se aplique a todos los sitios no gestionados por otro KMS. Si creas primero el KMS predeterminado, todos los dispositivos cifrados por nodo de la grid se cifrarán mediante el KMS predeterminado. Si quieres crear un KMS específico de un sitio más adelante, primero debes copiar la versión actual de la clave de cifrado del KMS predeterminado al nuevo KMS. Consulta "[Aspectos a tener en cuenta al cambiar el KMS de un sitio](#)" para más detalles.

Paso 1: detalles de KMS

En el paso 1 (Datos del KMS) del asistente para añadir un servidor de gestión de claves, tú proporcionas los datos del KMS o del clúster de KMS.

Pasos

1. Selecciona **Configuración > Seguridad > Servidor de gestión de claves**.

Aparece la página del servidor de gestión de claves con la pestaña Detalles de configuración seleccionada.

2. Selecciona **Crear**.

Aparece el paso 1 (detalles del KMS) del asistente Add a Key Management Server.

3. Introduce la siguiente información para el KMS y el cliente de StorageGRID que configuraste en ese KMS.

Campo	Descripción
Nombre de la KMS	Un nombre descriptivo que te ayude a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de la clave	El alias exacto de la clave para el cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. Nota: Si aún no has creado una clave usando tu producto KMS, se te pedirá que StorageGRID cree la clave.
Gestiona las claves de	El sitio de StorageGRID que se asociará a este KMS. Si es posible, deberías configurar cualquier servidor de gestión de claves específico del sitio antes de configurar un KMS predeterminado que se aplique a todos los sitios no gestionados por otro KMS. • Selecciona una sede si este KMS va a gestionar las claves de cifrado de los nodos del appliance en una sede concreta. • Selecciona Sitios no gestionados 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 añadas en ampliaciones posteriores. Nota: Se producirá un error de validación al guardar la configuración de KMS si seleccionas un sitio que fue cifrado previamente por el KMS predeterminado pero no proporcionaste 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 Gestión de Claves (KMIP). El valor predeterminado es 5696, que es el puerto estándar de KMIP.

Campo	Descripción
Nombre de host	El nombre de dominio completo o la dirección IP del KMS. Nota: El campo «Nombre alternativo del sujeto» (SAN) del certificado del servidor debe incluir el nombre de dominio completo (FQDN) o la dirección IP que introduzcas aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

- Si estás configurando un clúster KMS, selecciona **Add another hostname** para añadir un nombre de host para cada servidor del clúster.
- Selecciona **Continuar**.

Paso 2: Subir el certificado del servidor

En el paso 2 (Cargar certificado del servidor) del asistente Añadir un servidor de gestión de claves, subes el certificado del servidor (o el paquete de certificados) para el KMS. El certificado del servidor permite que el KMS externo se autentique ante StorageGRID.

Pasos

- En el **Paso 2 (Cargar el certificado del servidor)**, busca la ubicación donde guardaste el certificado del servidor o el paquete de certificados.
- Sube el archivo del certificado.

Aparecen los metadatos del certificado del servidor.



Si has subido un paquete de certificados, los metadatos de cada certificado aparecen en su propia pestaña.

- Selecciona **Continuar**.

Paso 3: Carga los certificados de cliente

En el paso 3 (Subir certificados de cliente) del asistente Agregar un servidor de gestión de claves, subes 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

- En el **Paso 3 (Cargar certificados de cliente)**, busca la ubicación del certificado de cliente.
- Sube el archivo del certificado de cliente.

Aparecen los metadatos del certificado de cliente.

- Busca la ubicación de la clave privada del certificado de cliente.
- Sube el archivo de la clave privada.
- Selecciona **Probar y guardar**.

Si una clave no existe, se te pedirá que StorageGRID cree una.

Se comprueban las conexiones entre el servidor de gestión de claves y los nodos del dispositivo. Si todas las conexiones son válidas y se encuentra la clave correcta en el KMS, el nuevo servidor de gestión de

claves se añade a la tabla en la página Key Management Server.



Inmediatamente después de añadir un KMS, el estado del certificado en la página Key Management Server aparece como Unknown. StorageGRID puede tardar hasta 30 minutos en obtener el estado real de cada certificado. Debes actualizar tu navegador web para ver el estado actual.

6. Si aparece un mensaje de error al seleccionar **Probar y guardar**, revisa los detalles del mensaje y luego selecciona **OK**.

Por ejemplo, es posible que recibas un error 422: entidad no procesable si falla una prueba de conexión.

7. Si necesitas guardar la configuración actual sin comprobar la conexión externa, selecciona **Force save**.



Al seleccionar **Force save**, se guarda la configuración del KMS, pero no se comprueba la conexión externa desde cada appliance a ese KMS. Si hay algún problema con la configuración, podrías no poder reiniciar los nodos de appliance que tengan habilitado el cifrado de nodos en el sitio afectado. Podrías perder el acceso a tus datos hasta que se resuelvan los problemas.

8. Revisa el mensaje de confirmación y selecciona **OK** si estás seguro de que quieres guardar la configuración de forma forzada.

La configuración del KMS se guarda, pero no se prueba la conexión con el KMS.

Administra un servidor de gestión de claves en StorageGRID

Gestionar un servidor de gestión de claves (KMS) implica ver o editar detalles, gestionar certificados, ver los nodos cifrados y eliminar un KMS cuando ya no lo necesites.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["permiso de acceso necesario"](#).

Ver detalles de KMS

Puedes consultar información sobre cada servidor de gestión de claves (KMS) en tu sistema StorageGRID, incluidos los detalles de las claves y el estado actual de los certificados del servidor y del cliente.

Pasos

1. Selecciona **Configuración > Seguridad > Servidor de gestión de claves**.

Aparece la página del servidor de gestión de claves y muestra la siguiente información:

- La pestaña Detalles de configuración muestra cualquier servidor de gestión de claves que esté configurado.
 - La pestaña «Nodos cifrados» muestra cualquier nodo que tenga activado el cifrado de nodos.
2. Para ver los detalles de un KMS específico y realizar operaciones en él, selecciona el nombre del KMS. La página de detalles del KMS muestra la siguiente información:

Campo	Descripción
Gestiona las claves de	El sitio de StorageGRID asociado al KMS. Este campo muestra el nombre de un sitio específico de StorageGRID o sitios no gestionados por otro KMS (KMS predeterminado) .
Nombre de host	El dominio completo o la dirección IP del KMS. Si hay un clúster de dos servidores de gestión de claves, se muestra el nombre de dominio completo o la dirección IP de ambos servidores. Si hay más de dos servidores de gestión de claves en un clúster, se muestra el nombre de dominio completo o la dirección IP del primer KMS, junto con el número de servidores de gestión de claves adicionales que hay en el clúster. Por ejemplo: 10.10.10.10 and 10.10.10.11 o 10.10.10.10 and 2 others. Para ver todos los nombres de host de un clúster, selecciona un KMS y selecciona Editar o Acciones > Editar .

3. Selecciona una pestaña en la página de detalles del KMS para ver la siguiente información:

Pestaña	Campo	Descripción
Datos clave	Nombre de la clave	El alias de clave para el cliente de StorageGRID en el KMS.
UID clave	El identificador único de la última versión de la clave.	Última modificación
La fecha y la hora de la última versión de la clave.	Certificado de servidor	Metadatos
Los metadatos del certificado, como el número de serie, la fecha y la hora de caducidad, y el PEM del certificado.	Certificado PEM	El contenido del archivo PEM (privacy enhanced mail) para el certificado.
Certificado de cliente	Metadatos	Los metadatos del certificado, como el número de serie, la fecha y la hora de caducidad, y el PEM del certificado.

4. Con la frecuencia que exijan las políticas de seguridad de tu organización, selecciona **Rotar clave** o utiliza el software KMS para crear una nueva versión de la clave.

Cuando la rotación de claves se realiza correctamente, se actualizan los campos Key UID y Last modified.

Si renuevas la clave de cifrado mediante el software KMS, hazlo pasando de la última versión utilizada de la clave a una nueva versión de la misma clave. No la renueves por una clave completamente diferente.



Nunca intentes rotar una clave cambiando el nombre de la clave (alias) en el KMS. StorageGRID requiere que todas las versiones de clave utilizadas anteriormente (así como las futuras) sean accesibles desde el KMS con el mismo alias de clave. Si cambias el alias de la clave de un KMS configurado, es posible que StorageGRID no pueda descifrar tus datos.

Gestiona certificados

Soluciona rápidamente cualquier problema con los certificados de servidor o de cliente. Si es posible, reemplaza los certificados antes de que caduquen.



Debes resolver cualquier problema relacionado con los certificados lo antes posible para mantener el acceso a los datos.

Pasos

1. Selecciona **Configuración > Seguridad > Servidor de gestión de claves**.
2. En la tabla, fíjate en el valor de caducidad del certificado de cada KMS.
3. Si la fecha de caducidad del certificado de cualquier KMS es Unknown, espera hasta 30 minutos y luego actualiza tu navegador web.
4. Si en la columna «Caducidad del certificado» se indica que un certificado ha caducado o está a punto de caducar, selecciona el KMS para ir a la página de detalles del KMS.
 - a. Selecciona **Server certificate** y comprueba el valor del campo "Expires on".
 - b. Para sustituir el certificado, selecciona **Editar certificado** para subir un certificado nuevo.
 - c. Repite estos pasos secundarios y selecciona **Certificado de cliente** en lugar de **Certificado de servidor**.
5. Cuando se activen las alertas **Caducidad del certificado de la CA de KMS**, **Caducidad del certificado de cliente de KMS** y **Caducidad del certificado de servidor de KMS**, toma nota de la descripción de cada alerta y realiza las acciones recomendadas.

StorageGRID puede tardar hasta 30 minutos en obtener las actualizaciones de la caducidad del certificado. Actualiza tu navegador web para ver los valores actuales.



Si aparece el mensaje «**El estado del certificado del servidor es desconocido**», asegúrate de que tu KMS permita obtener un certificado de servidor sin requerir un certificado de cliente.

Ver nodos cifrados

Puedes consultar la información sobre los nodos de los dispositivos de tu sistema StorageGRID que tienen activada la opción **Cifrado de nodos**.

Pasos

1. Selecciona **Configuración > Seguridad > Servidor de gestión de claves**.

Aparece la página «Servidor de gestión de claves». La pestaña «Detalles de configuración» muestra los

servidores de gestión de claves que se hayan configurado.

2. En la parte superior de la página, selecciona la pestaña **Nodos cifrados**.

La pestaña «Nodos cifrados» muestra los nodos del dispositivo en tu sistema StorageGRID que tienen activada la opción **Cifrado de nodos**.

3. Revisa la información en la tabla para cada nodo de dispositivo.

Columna	Descripción
Nombre de nodo	El nombre del nodo del dispositivo.
Tipo de nodo	El tipo de nodo: Storage, Admin o Gateway.
Sitio	El nombre del sitio de StorageGRID en el que está instalado el nodo.
Nombre de la KMS	El nombre descriptivo del KMS utilizado para el nodo. Si no aparece ningún KMS en la lista, selecciona la pestaña Detalles de configuración para añadir un KMS. "Agrega un servidor de gestión de claves (KMS)"
UID clave	El ID único de la clave de cifrado que se utiliza para cifrar y descifrar datos en el nodo del dispositivo. Para ver el UID completo de una clave, selecciona el texto. Un guión (--) indica que se desconoce el UID de la clave, posiblemente porque hay un problema de conexión entre el nodo del appliance 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. Puede tardar varios minutos en actualizarse el estado de la conexión después de los cambios en la configuración del KMS. Nota: Actualiza tu navegador web para ver los nuevos valores.

4. Si en la columna Estado aparece un problema relacionado con el KMS, resuélvelo de inmediato.

Durante el funcionamiento normal de KMS, el estado será **Conectado a KMS**. Si un nodo se desconecta de la grid, se muestra el estado de conexión del nodo (Administratively Down o Unknown).

Otros mensajes de estado corresponden a alertas de StorageGRID con los mismos nombres:

- No se ha podido cargar la configuración de KMS
- Error de conectividad con KMS
- No se ha encontrado el nombre de la clave de cifrado de KMS
- Error en la rotación de la clave de cifrado de KMS
- La clave KMS no pudo descifrar el volumen de un dispositivo

- KMS no está configurado

Lleva a cabo las acciones recomendadas para estas alertas.



Debes resolver cualquier problema de inmediato para garantizar que tus datos estén totalmente protegidos.

Editar un KMS

Es posible que tengas que modificar la configuración de un servidor de gestión de claves, por ejemplo, si un certificado está a punto de caducar.

Antes de empezar

- Si planeas actualizar el sitio seleccionado para un KMS, has revisado "[Consideraciones para cambiar el KMS de un sitio](#)".
- Has iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tienes el "[Permiso de acceso raíz](#)".

Pasos

1. Selecciona **Configuración > Seguridad > Servidor de gestión de claves**.

Aparece la página «Key management server» y muestra todos los key management servers que se han configurado.

2. Selecciona el KMS que quieras editar y selecciona **Acciones > Editar**.

También puedes editar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Editar** en la página de detalles del KMS.

3. Opcionalmente, actualiza los detalles en **Step 1 (KMS details)** del asistente Edit a Key Management Server.

Campo	Descripción
Nombre de la KMS	Un nombre descriptivo que te ayude a identificar este KMS. Debe tener entre 1 y 64 caracteres.
Nombre de la clave	El alias exacto de la clave para el cliente StorageGRID en el KMS. Debe tener entre 1 y 255 caracteres. Solo necesitas modificar el nombre de la clave en casos excepcionales. Por ejemplo, debes modificar el nombre de la clave si se cambia el nombre del alias en el KMS o si todas las versiones de la clave anterior se han copiado al historial de versiones del nuevo alias.

Campo	Descripción
Gestiona las claves de	Si estás editando un KMS específico de un sitio y aún no tienes un KMS predeterminado, puedes seleccionar opcionalmente Sitios no gestionados por otro KMS (KMS predeterminado). Esta selección convierte un KMS específico de un sitio en el KMS predeterminado, que se aplicará a todos los sitios que no tengan un KMS dedicado y a cualquier sitio añadido en una expansión. Nota: Si estás editando un KMS específico de un sitio, no puedes seleccionar otro sitio. Si estás editando el KMS predeterminado, no puedes seleccionar un sitio específico.
Puerto	El puerto que utiliza el servidor KMS para las comunicaciones del Protocolo de Interoperabilidad de Gestión de Claves (KMIP). El valor predeterminado es 5696, que es el puerto estándar de KMIP.
Nombre de host	El nombre de dominio completo o la dirección IP del KMS. Nota: El campo «Nombre alternativo del sujeto» (SAN) del certificado del servidor debe incluir el nombre de dominio completo (FQDN) o la dirección IP que introduzcas aquí. De lo contrario, StorageGRID no podrá conectarse al KMS ni a todos los servidores de un clúster KMS.

4. Si estás configurando un clúster KMS, selecciona **Add another hostname** para añadir un nombre de host para cada servidor del clúster.

5. Selecciona **Continuar**.

Aparece el paso 2 (Cargar el certificado del servidor) del asistente Edit a Key Management Server.

6. Si necesitas sustituir el certificado del servidor, selecciona **Examinar** y sube el nuevo archivo.

7. Selecciona **Continuar**.

Aparece el paso 3 (Cargar certificados de cliente) del asistente Edit a Key Management Server.

8. Si necesitas sustituir el certificado de cliente y la clave privada del certificado de cliente, selecciona **Examinar** y sube los nuevos archivos.

9. Selecciona **Probar y guardar**.

Se prueban las conexiones entre el servidor de gestión de claves y todos los nodos de appliance con cifrado de nodos en los sitios afectados. Si todas las conexiones de los nodos son válidas y se encuentra la clave correcta en el KMS, el servidor de gestión de claves se añade a la tabla de la página Key Management Server.

10. Si aparece un mensaje de error, revisa los detalles del mensaje y selecciona **OK**.

Por ejemplo, es posible que recibas un error 422: entidad no procesable si el sitio que has seleccionado para este KMS ya está gestionado por otro KMS, o si ha fallado una prueba de conexión.

11. Si necesitas guardar la configuración actual antes de solucionar los errores de conexión, selecciona **Force save**.



Al seleccionar **Force save**, se guarda la configuración del KMS, pero no se comprueba la conexión externa desde cada appliance a ese KMS. Si hay algún problema con la configuración, podrías no poder reiniciar los nodos de appliance que tengan habilitado el cifrado de nodos en el sitio afectado. Podrías perder el acceso a tus datos hasta que se resuelvan los problemas.

La configuración de KMS se ha guardado.

12. Revisa el mensaje de confirmación y selecciona **OK** si estás seguro de que quieres guardar la configuración de forma forzada.

La configuración del KMS se guarda, pero no se prueba la conexión con el KMS.

Eliminar un servidor de gestión de claves (KMS)

Es posible que, en algunos casos, desees eliminar un servidor de gestión de claves. Por ejemplo, es posible que desees eliminar un KMS específico de un sitio si has decomisionado dicho sitio.

Antes de empezar

- Has revisado la "[Consideraciones y requisitos para usar un servidor de gestión de claves](#)".
- Has iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tienes el "[Permiso de acceso raíz](#)".

Acerca de esta tarea

Puedes eliminar un KMS en estos casos:

- Puedes eliminar un KMS específico de un sitio si dicho sitio ha sido decomisionado o si el sitio no incluye ningún nodo de dispositivo con el cifrado de nodos activado.
- Puedes eliminar el KMS predeterminado si ya existe un KMS específico para cada sitio que tenga nodos de appliance con el cifrado de nodos habilitado.

Pasos

1. Selecciona **Configuración > Seguridad > Servidor de gestión de claves**.

Aparece la página «Key management server» y muestra todos los key management servers que se han configurado.

2. Selecciona el KMS que quieras eliminar y selecciona **Actions > Remove**.

También puedes eliminar un KMS seleccionando el nombre del KMS en la tabla y seleccionando **Eliminar** en la página de detalles del KMS.

3. Confirma que lo siguiente es cierto:
 - Estás eliminando un KMS específico de un sitio que no tiene ningún nodo de dispositivo con el cifrado de nodos activado.
 - Estás eliminando el KMS predeterminado, pero ya existe un KMS específico para cada sitio con cifrado de nodos.
4. Selecciona **Sí**.

Se ha eliminado la configuración de KMS.

Gestiona la configuración del proxy

Configura un proxy de almacenamiento StorageGRID

Si estás utilizando servicios de plataforma o Cloud Storage Pools, puedes configurar un proxy no transparente entre los nodos de almacenamiento y los endpoints de S3 externos. Por ejemplo, es posible que necesites un proxy no transparente para permitir que los mensajes de los servicios de plataforma se envíen a endpoints externos, como un endpoint en internet.



La configuración del proxy de almacenamiento no se aplica a los endpoints de los servicios de la plataforma Kafka.

Antes de empezar

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

Acerca de esta tarea

Puedes configurar los parámetros de un único proxy de almacenamiento.

Pasos

1. Selecciona **Configuración > Seguridad > Proxy settings**.
2. En la pestaña **Almacenamiento**, marca la casilla **Habilitar proxy de almacenamiento**.
3. Selecciona el protocolo para el proxy de almacenamiento.
4. Introduce el nombre de host o la dirección IP del servidor proxy.
5. Opcionalmente, introduce el puerto que se usa para conectarte al servidor proxy.

Deja este campo en blanco para utilizar el puerto predeterminado del protocolo: 80 para HTTP o 1080 para SOCKS5.

6. Selecciona **Guardar**.

Después de guardar el proxy de almacenamiento, puedes configurar y probar nuevos endpoints para los servicios de plataforma o Cloud Storage Pools.



Los cambios en el proxy pueden tardar hasta 10 minutos en surtir efecto.

7. Comprueba la configuración de tu servidor proxy para asegurarte de que los mensajes relacionados con los servicios de la plataforma de StorageGRID no se bloqueen.
8. Si necesitas desactivar un proxy de almacenamiento, desmarca la casilla de selección y selecciona **Guardar**.

Configura los ajustes del proxy de administración en StorageGRID

Si envías paquetes AutoSupport usando HTTP o HTTPS, puedes configurar un proxy no transparente entre los nodos de administración y el soporte técnico (AutoSupport).

Para obtener más información sobre AutoSupport, consulta ["Configura AutoSupport"](#).

Antes de empezar

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

Acerca de esta tarea

Puedes configurar los ajustes de un único proxy de administrador.

Pasos

1. Selecciona **Configuración > Seguridad > Proxy settings**.

Aparece la página «Configuración del proxy». De forma predeterminada, la opción «Almacenamiento» está seleccionada en el menú de pestañas.

2. Selecciona la pestaña **Admin**.
3. Marca la casilla **Habilitar proxy de administrador**.
4. Introduce el nombre de host o la dirección IP del servidor proxy.
5. Introduce el puerto que se utiliza para conectarte al servidor proxy.
6. Si lo deseas, introduce un nombre de usuario y una contraseña para el servidor proxy.

Deja estos campos en blanco si tu servidor proxy no requiere un nombre de usuario o una contraseña.

7. Selecciona una de las siguientes:

- Si deseas proteger la conexión con el proxy de administración, selecciona **Verificar certificado del proxy**. Sube 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 la ruta de actualización en la página de actualización de StorageGRID no funcionarán si se verifica un certificado de proxy.

Después de que subas el paquete de CA, aparecen sus metadatos.

- Si no deseas validar los certificados al comunicarte con el servidor proxy de administración, selecciona **No verificar el certificado del proxy**.

8. Selecciona **Guardar**.

Una vez guardado el proxy de administración, se configura el servidor proxy entre los nodos de administración y soporte técnico.



Los cambios en el proxy pueden tardar hasta 10 minutos en surtir efecto.

9. Si necesitas desactivar el proxy de administrador, desmarca la casilla **Habilitar proxy de administrador** y luego selecciona **Guardar**.

Controla los cortafuegos

Controla el acceso a StorageGRID en un firewall externo

Puedes abrir o cerrar puertos específicos en el firewall externo.

Puedes controlar el acceso a las interfaces de usuario y a las API en los Admin Nodes de StorageGRID abriendo o cerrando puertos específicos en el firewall externo. Por ejemplo, es posible que quieras evitar que los inquilinos puedan conectarse al Grid Manager en el firewall, además de utilizar otros métodos para controlar el acceso al sistema.

Si quieres configurar el firewall interno de StorageGRID, consulta ["Configura el cortafuegos interno"](#).

Puerto	Descripción	Si el puerto está abierto...
443	Puerto HTTPS predeterminado para los nodos de administración	Los navegadores web y los clientes de la API de gestión pueden acceder al Grid Manager, a la Grid Management API, al Tenant Manager y a la Tenant Management API. Nota: El puerto 443 también se utiliza para parte del tráfico interno.
8443	Puerto restringido de Grid Manager en los nodos de administración	• Los navegadores web y los clientes de la API de gestión pueden acceder al Grid Manager y a la Grid Management API mediante HTTPS. • Los navegadores web y los clientes de la API de gestión no pueden acceder al Tenant Manager ni a la Tenant Management API. • Se rechazarán las solicitudes de contenido interno.
9443	Puerto restringido de Tenant Manager en los nodos de administración	• Los navegadores web y los clientes de la API de gestión pueden acceder al Tenant Manager y a la Tenant Management API mediante HTTPS. • Los navegadores web y los clientes de la API de gestión no pueden acceder al Grid Manager ni a la Grid Management API. • Se rechazarán las solicitudes de contenido interno.



El inicio de sesión único (SSO) no está disponible en los puertos restringidos de Grid Manager o Tenant Manager. Debes utilizar el puerto HTTPS predeterminado (443) si quieres que los usuarios se autenticuen con el inicio de sesión único.

Información relacionada

- ["Inicia sesión en Grid Manager"](#)
- ["Crear cuenta de inquilino"](#)
- ["Comunicaciones externas"](#)

Administra los controles internos de firewall en StorageGRID

StorageGRID incluye un cortafuegos interno en cada nodo que mejora la seguridad de tu grid al permitirte controlar el acceso de red al nodo. Usa el cortafuegos para evitar el acceso de red en todos los puertos excepto en los necesarios para tu implementación

específica de grid. Los cambios de configuración que hagas en la página de control del cortafuegos se aplican a cada nodo.

Utiliza las tres pestañas de la página de control del cortafuegos para personalizar el acceso que necesitas para tu grid.

- **Lista de direcciones con privilegios:** utiliza esta pestaña para permitir el acceso seleccionado a los puertos cerrados. Puedes añadir direcciones IP o subredes en notación CIDR que puedan acceder a los puertos cerrados mediante la pestaña Gestionar acceso externo.
- **Gestionar el acceso externo:** Usa esta pestaña para cerrar los puertos que están abiertos por defecto o volver a abrir los puertos que se cerraron anteriormente.
- **Red de clientes no fiables:** Usa esta pestaña para especificar si un nodo confía en el tráfico entrante de la red de clientes.

La configuración de esta pestaña prevalece sobre la de la pestaña Gestionar acceso externo.

- Un nodo con una red de clientes no fiable solo aceptará conexiones en los puertos de los puntos finales del equilibrador de carga configurados en dicho nodo (puntos finales globales, de interfaz de nodo y vinculados al tipo de nodo).
- Los puertos de los puntos finales del equilibrador de carga *son los únicos puertos abiertos* en las redes de clientes no confiables, independientemente de la configuración de la pestaña Manage external networks.
- Cuando se consideran de confianza, se puede acceder a todos los puertos abiertos en la pestaña Gestionar acceso externo, así como a cualquier endpoint del equilibrador de carga abierto en la Client Network.



La configuración que realices en una pestaña puede afectar a los cambios de acceso que realices en otra pestaña. Asegúrate de comprobar la configuración de todas las pestañas para garantizar que tu red funcione tal y como esperas.

Para configurar los controles del cortafuegos interno, consulta ["Configura los controles del cortafuegos"](#).

Para obtener más información sobre los firewalls externos y la seguridad de la red, consulta ["Controla el acceso en el cortafuegos externo"](#).

Pestañas Lista de direcciones privilegiadas y Gestionar el acceso externo

La pestaña Privileged address list te permite registrar una o más direcciones IP para permitirles el acceso a los puertos de la grid que están cerrados. La pestaña Manage external access te permite cerrar el acceso externo a los puertos externos seleccionados o a todos los puertos externos abiertos (los puertos externos son aquellos a los que pueden acceder los nodos que no pertenecen a la grid de forma predeterminada). A menudo puedes utilizar estas dos pestañas juntas para personalizar el acceso exacto a la red que necesitas permitir para tu grid.



Las direcciones IP privilegiadas no tienen acceso al puerto interno de grid de forma predeterminada.

Ejemplo 1: usa un servidor de enlace para tareas de mantenimiento

Supón que quieres usar un jump host (un host con seguridad reforzada) para la administración de la red. Podrías seguir estos pasos generales:

1. Utiliza la pestaña «Lista de direcciones privilegiadas» para añadir la dirección IP del jump host.
2. Utiliza la pestaña «Manage external access» para bloquear todos los puertos.



Añade la dirección IP privilegiada antes de bloquear los puertos 443 y 8443. Cualquier usuario que esté conectado actualmente a un puerto bloqueado, incluido tú, perderá el acceso a Grid Manager a menos que su dirección IP se haya añadido a la lista de direcciones privilegiadas.

Después de guardar tu configuración, todos los puertos externos del Admin Node de tu grid se bloquearán para todos los hosts, excepto para el jump host. Luego puedes usar el jump host para realizar tareas de mantenimiento en tu grid de forma más segura.

Ejemplo 2: bloquear los puertos sensibles

Supongamos que quieres bloquear los puertos sensibles y el servicio en ese puerto. Podrías seguir estos pasos generales:

1. Utiliza la pestaña «Lista de direcciones con privilegios» para conceder acceso únicamente a los hosts que necesitan acceso al servicio.
2. Utiliza la pestaña «Manage external access» para bloquear todos los puertos.



Añade la dirección IP privilegiada antes de bloquear el acceso a cualquier puerto asignado para acceder a Grid Manager y Tenant Manager (los puertos preestablecidos son 443 y 8443). Cualquier usuario que esté conectado actualmente a un puerto bloqueado, incluido tú, perderá el acceso a Grid Manager a menos que su dirección IP se haya añadido a la lista de direcciones privilegiadas.

Después de que guardes tu configuración, el puerto sensible y el servicio en ese puerto 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 desde qué interfaz provenga la solicitud.

Ejemplo 3: desactivar el acceso a los servicios que no se utilizan

A nivel de red, puedes desactivar algunos servicios que no tengas previsto utilizar. Por ejemplo, para bloquear el tráfico de clientes HTTP S3, usarías el interruptor de la pestaña Manage external access para bloquear el puerto 18084.

Pestaña Redes de clientes no fiables

Si utilizas una red de clientes, puedes ayudar a proteger StorageGRID de ataques hostiles aceptando el tráfico entrante de clientes solo en los endpoints configurados explícitamente.

De forma predeterminada, la red de clientes de cada nodo de grid es de *confianza*. Es decir, de forma predeterminada, StorageGRID confía en las conexiones entrantes a cada nodo de grid en todos los "puertos externos disponibles".

Puedes reducir la amenaza de ataques hostiles contra tu sistema StorageGRID especificando que la Client Network de cada nodo sea *untrusted*. Si la Client Network de un nodo es untrusted, el nodo solo acepta conexiones entrantes en los puertos configurados explícitamente como endpoints del load balancer. Consulta ["Configura los puntos de conexión del equilibrador de carga"](#) y ["Configura los controles del cortafuegos"](#).

Ejemplo 1: el nodo de puerta de enlace solo acepta solicitudes HTTPS S3

Supongamos que quieres que un nodo de puerta de enlace rechace todo el tráfico entrante en la red del cliente, excepto las solicitudes HTTPS S3. Para ello, deberías seguir estos pasos generales:

1. Desde la página ["Puntos de conexión del equilibrador de carga"](#), configura un endpoint del equilibrador de carga para S3 sobre HTTPS en el puerto 443.
2. En la página de control del cortafuegos, selecciona No fiable para indicar que la Client Network en el Gateway Node no es fiable.

Después de que guardes tu configuración, se rechaza todo el tráfico entrante en la red de clientes del Gateway Node, 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 plataforma S3

Supongamos que quieres habilitar el tráfico saliente de los servicios de la plataforma S3 desde un nodo de almacenamiento, pero quieres impedir cualquier conexión entrante a ese nodo de almacenamiento desde la red del cliente. Realizarías este paso general:

- En la pestaña Untrusted Client Networks de la página de control del Firewall, indica que la Client Network en el Storage Node no es de confianza.

Una vez que guardas tu configuración, el Storage Node ya no acepta tráfico entrante en la Client Network, pero sigue permitiendo las solicitudes salientes hacia los destinos de servicios de plataforma configurados.

Ejemplo 3: limitar el acceso a Grid Manager a una subred

Supongamos que quieres permitir el acceso a Grid Manager únicamente en una subred concreta. Realiza los siguientes pasos:

1. Conecta la red de clientes de tus nodos de administración a la subred.
2. Utiliza la pestaña Untrusted Client Network para configurar la Client Network como no fiable.
3. Cuando creas un punto de conexión del equilibrador de carga de la interfaz de gestión, introduce el puerto y selecciona la interfaz de gestión a la que accederá el puerto.
4. Selecciona **Sí** en «Red de cliente no fiable».
5. Utiliza la pestaña «Gestionar acceso externo» para bloquear todos los puertos externos (con o sin direcciones IP privilegiadas configuradas para los hosts fuera de esa subred).

Una vez que guardes tu configuración, solo los hosts de la subred que especificaste podrán acceder al Grid Manager. Todos los demás hosts quedarán bloqueados.

Configura el firewall interno de StorageGRID

Puedes configurar el firewall de StorageGRID para controlar el acceso de red a puertos específicos en tus nodos de StorageGRID.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).
- Has revisado la información en ["Gestiona los controles del cortafuegos"](#) y ["Directrices de redes"](#).

- Si deseas que un nodo de administración o un nodo de puerta de enlace acepte tráfico entrante únicamente en los puntos de conexión configurados explícitamente, has definido los puntos de conexión del equilibrador de carga.



Al modificar la configuración de la red de clientes, es posible que las conexiones de los clientes existentes fallen si no se han configurado los endpoints del equilibrador de carga.

Acerca de esta tarea

StorageGRID incluye un cortafuegos interno en cada nodo que te permite abrir o cerrar algunos de los puertos de los nodos de tu grid. Puedes usar las pestañas de control del cortafuegos para abrir o cerrar los puertos que están abiertos por defecto en la Grid Network, Admin Network y Client Network. También puedes crear una lista de direcciones IP privilegiadas que pueden acceder a los puertos del grid que estén cerrados. Si estás usando una Client Network, puedes especificar si un nodo confía en el tráfico entrante de la Client Network y puedes configurar el acceso a puertos específicos en la Client Network.

Limitar el número de puertos abiertos a direcciones IP fuera de tu grid a solo aquellos que sean absolutamente necesarios mejora la seguridad de tu grid. Usas la configuración de cada una de las tres pestañas de control del Firewall para asegurarte de que solo estén abiertos los puertos necesarios.

Para obtener más información sobre el uso de los controles del firewall, incluidos algunos ejemplos, consulta ["Gestiona los controles del cortafuegos"](#).

Para obtener más información sobre los firewalls externos y la seguridad de la red, consulta ["Controla el acceso en el cortafuegos externo"](#).

Accede a los controles del cortafuegos

Pasos

1. Selecciona **Configuración > Seguridad > Control del cortafuegos**.

Las tres pestañas de esta página se describen en ["Gestiona los controles del cortafuegos"](#).

2. Selecciona cualquier pestaña para configurar los controles del cortafuegos.

Puedes utilizar estas pestañas en cualquier orden. Las configuraciones que establezcas en una pestaña no limitan lo que puedes hacer en las demás; sin embargo, los cambios de configuración que realices en una pestaña podrían modificar el comportamiento de los puertos configurados en otras pestañas.

Lista de direcciones privilegiadas

La pestaña «Lista de direcciones privilegiadas» sirve para conceder a los hosts acceso a los puertos que están cerrados por defecto o que se han cerrado mediante la configuración de la pestaña «Manage external access».

Las direcciones IP y subredes con privilegios no tienen acceso al grid interno de forma predeterminada. Además, los endpoints del equilibrador de carga y los puertos adicionales que abras en la pestaña Lista de direcciones con privilegios seguirán estando accesibles aunque los bloques en la pestaña Administrar acceso externo.



La configuración de la pestaña «Lista de direcciones privilegiadas» no puede anular la configuración de la pestaña «Red de clientes no fiables».

Pasos

1. En la pestaña «Lista de direcciones privilegiadas», introduce la dirección o la subred IP a la que quieres conceder acceso a los puertos cerrados.
2. Si lo deseas, selecciona **Add another IP address or subnet in CIDR notation** para añadir clientes con privilegios adicionales.



Agrega la menor cantidad posible de direcciones a la lista de direcciones privilegiadas.

3. Si lo deseas, selecciona **Permitir que las direcciones IP con privilegios accedan a los puertos internos de StorageGRID**. Consulta ["Puertos internos de StorageGRID"](#).



Esta opción elimina algunas protecciones para los servicios internos. Si es posible, déjala desactivada.

4. Selecciona **Guardar**.

Gestiona el acceso externo

Cuando se cierra un puerto en la pestaña Gestionar acceso externo, el puerto no puede ser accedido por ninguna dirección IP que no sea de la grid, a menos que añadas la dirección IP a la lista de direcciones privilegiadas. Solo puedes cerrar los puertos que están abiertos por defecto, y solo puedes abrir los puertos que hayas cerrado.



La configuración de la pestaña Manage external access no puede anular la configuración de la pestaña Untrusted Client Network. Por ejemplo, si un nodo no es de confianza, el puerto SSH/22 se bloquea en la Client Network aunque esté abierto en la pestaña Manage external access. La configuración de la pestaña Untrusted Client Network anula los puertos cerrados (como 443, 8443, 9443) en la Client Network.

Pasos

1. Selecciona **Gestionar acceso externo**. La pestaña muestra una tabla con todos los puertos externos (puertos a los que pueden acceder por defecto los nodos que no forman parte del grid) de los nodos de tu grid.
2. Configura los puertos que quieras abrir y cerrar utilizando las siguientes opciones:
 - Utiliza el botón de activación junto a cada puerto para abrir o cerrar el puerto seleccionado.
 - Selecciona **Abrir todos los puertos mostrados** para abrir todos los puertos que aparecen en la tabla.
 - Selecciona **Cerrar todos los puertos mostrados** para cerrar todos los puertos que aparecen en la tabla.



Si cierras los puertos 443 u 8443 de Grid Manager, cualquier usuario que esté conectado en ese momento a un puerto bloqueado, incluido tú, perderá el acceso a Grid Manager a menos que su dirección IP se haya añadido a la lista de direcciones privilegiadas.



Utiliza la barra de desplazamiento situada a la derecha de la tabla para asegurarte de que has visto todos los puertos disponibles. Utiliza el campo de búsqueda para encontrar la configuración de cualquier puerto externo introduciendo un número de puerto. Puedes introducir un número de puerto parcial. Por ejemplo, si introduces **2**, se mostrarán todos los puertos que tengan la cadena "2" como parte de su nombre.

3. Selecciona **Guardar**

Red de clientes no fiables

Si la red de cliente de un nodo no es de confianza, el nodo solo acepta tráfico entrante en los puertos configurados como puntos finales del equilibrador de carga y, opcionalmente, en los puertos adicionales que selecciones en esta pestaña. También puedes utilizar esta pestaña para especificar la configuración predeterminada para los nuevos nodos añadidos en una ampliación.



Las conexiones de los clientes existentes podrían fallar si no se han configurado los endpoints del equilibrador de carga.

Los cambios de configuración que realices en la pestaña **Red de clientes no fiables** anulan los ajustes de la pestaña **Manage external access**.

Pasos

1. Selecciona **Red de cliente no fiable**.
2. En la sección «Establecer valor predeterminado para nuevos nodos», especifica cuál debe ser la configuración predeterminada cuando se añadan nuevos nodos a la grid en un procedimiento de ampliación.
 - **De confianza** (por defecto): Cuando se añade un nodo en una ampliación, su Client Network es de confianza.
 - **No fiable**: Cuando se añade un nodo en una ampliación, su red de cliente no es fiable.

Si lo necesitas, puedes volver a esta pestaña para cambiar la configuración de un nodo nuevo concreto.



Esta configuración no afecta a los nodos existentes en tu sistema StorageGRID.

3. Utiliza las siguientes opciones para seleccionar los nodos que solo deben permitir conexiones de clientes en los puntos finales del equilibrador de carga configurados explícitamente o en puertos adicionales seleccionados:
 - Selecciona **Marcar como no fiable los nodos mostrados** para añadir todos los nodos que aparecen en la tabla a la lista de Red de clientes no fiables.
 - Selecciona **Confiar en los nodos mostrados** para eliminar todos los nodos que aparecen en la tabla de la lista de Untrusted Client Network.
 - Utiliza el botón de alternancia situado junto a cada nodo para configurar la red del cliente como de confianza o no de confianza para el nodo seleccionado.

Por ejemplo, puedes seleccionar **No confiar en los nodos mostrados** para añadir todos los nodos a la lista de Untrusted Client Network y luego usar el botón de alternancia junto a un nodo individual para añadir ese nodo a la lista de Trusted Client Network.



Utiliza la barra de desplazamiento situada a la derecha de la tabla para asegurarte de que has visto todos los nodos disponibles. Utiliza el campo de búsqueda para encontrar la configuración de cualquier nodo introduciendo el nombre de nodo. Puedes introducir un nombre parcial. Por ejemplo, si introduces **GW**, se mostrarán todos los nodos que tengan la cadena "GW" como parte de su nombre.

4. Selecciona **Guardar**.

La nueva configuración del cortafuegos se aplica y se hace efectiva de forma inmediata. Las conexiones de los clientes existentes podrían fallar si no se han configurado los endpoints del balanceador de carga.

Gestiona inquilinos

Cuentas de tenant en StorageGRID

Una cuenta de inquilino te permite utilizar la API de REST del Servicio de Almacenamiento Sencillo (S3) para almacenar y recuperar objetos en un sistema StorageGRID.



Se han eliminado los detalles sobre Swift de esta versión del sitio de documentación. Consulta ["StorageGRID 11.8: administra inquilinos"](#).

Como administrador de la grid, creas y gestionas las cuentas de inquilino que los clientes de S3 usan para almacenar y recuperar objetos.

Cada cuenta de inquilino cuenta con grupos federados o locales, usuarios, buckets de S3 y objetos.

Puedes usar las cuentas de inquilino para segregar los objetos almacenados por diferentes entidades. Por ejemplo, puedes usar varias cuentas de inquilino para cualquiera de estos casos de uso:

- **Caso de uso empresarial:** Si administras un sistema StorageGRID en una aplicación empresarial, es posible que desees segregar el almacenamiento de objetos de la red según los distintos departamentos de tu organización. En este caso, podrías crear cuentas de inquilino para el departamento de Marketing, el departamento de Customer Support, el departamento de Human Resources, etc.



Si utilizas el protocolo de cliente S3, puedes emplear los buckets de S3 y las políticas de bucket para segregar los objetos entre los departamentos de una empresa. No necesitas usar cuentas de inquilino. Consulta las instrucciones para implementar ["Buckets de S3 y políticas de bucket"](#) para más información.

- **Caso de uso de proveedor de servicios:** Si administras un sistema StorageGRID como proveedor de servicios, puedes segregar el almacenamiento de objetos del grid por las diferentes entidades que alquilarán el almacenamiento en tu grid. En este caso, crearías cuentas de inquilino para Company A, Company B, Company C, y así sucesivamente.

Para más información, consulta ["Utiliza una cuenta de inquilino"](#).

¿Cómo creo una cuenta de inquilino?

Utiliza el Grid manager para crear una cuenta de inquilino. Al crear una cuenta de inquilino, debes especificar la siguiente información:

- Información básica, incluido el nombre del inquilino, el tipo de cliente (S3) y la cuota de almacenamiento opcional.
- Permisos de la cuenta de inquilino, como si la cuenta de inquilino puede usar los servicios de la plataforma S3, configurar su propia fuente de identidad, usar S3 Select o usar una conexión de federación de grid.
- El acceso a raíz inicial para el inquilino, en función de si el sistema StorageGRID utiliza grupos y usuarios locales, federación de identidades o inicio de sesión único (SSO).

Además, puedes activar la configuración de S3 Object Lock para el sistema StorageGRID si las cuentas de inquilino de S3 deben cumplir con los requisitos normativos. Cuando S3 Object Lock está activado, todas las cuentas de inquilino de S3 pueden crear y gestionar buckets conformes.

¿Para qué sirve Tenant Manager?

Después de crear la cuenta de inquilino, los usuarios del inquilino pueden iniciar sesión en el Tenant Manager para realizar tareas como las siguientes:

- Configura la federación de identidades (a menos que la fuente de identidades se comparta con la grid)
- Gestiona grupos y usuarios
- Utiliza la federación de grid para la clonación de cuentas y la replicación entre grid
- Gestiona claves de acceso de S3
- Crear y gestionar buckets de S3
- Usa los servicios de la plataforma S3
- Usa S3 Select
- Supervisa el uso del almacenamiento



Aunque los usuarios inquilinos de S3 pueden crear y gestionar claves de acceso y buckets de S3 con el Tenant Manager, deben usar una aplicación cliente de S3 para cargar y gestionar objetos. Consulta ["Usa la API de REST de S3"](#) para más detalles.

Crear una cuenta de inquilino de StorageGRID

Debes crear al menos una cuenta de inquilino para controlar el acceso al almacenamiento en tu sistema StorageGRID.

Los pasos para crear una cuenta de inquilino varían en función de si ["federación de identidades"](#) y ["inicio de sesión único"](#) están configurados y de si la cuenta de Grid Manager que usas para crear la cuenta de inquilino pertenece a un grupo de administradores con el permiso de acceso a raíz.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Acceso raíz o permisos de cuentas de inquilino"](#).
- Si la cuenta de inquilino va a usar la fuente de identidad que se configuró para Grid Manager y quieres otorgar el permiso de acceso a raíz para la cuenta de inquilino a un grupo federado, ya habrás importado ese grupo federado en Grid Manager. No necesitas asignar ningún permiso de Grid Manager a este grupo de administradores. Consulta ["Gestiona grupos de administradores"](#).
- Si deseas permitir que un inquilino de S3 clone los datos de la cuenta y replique los objetos del bucket en otra grid mediante una conexión de federación de grids:
 - Tienes ["configuraste la conexión de federación de grid"](#).
 - El estado de la conexión es **Conectado**.
 - Tienes permiso de acceso root.
 - Ya has revisado las consideraciones para ["gestionar los inquilinos permitidos para la federación de grid"](#).
 - Si la cuenta de inquilino va a utilizar la fuente de identidad que se configuró para Grid Manager, has

importado el mismo grupo federado en Grid Manager en ambas grids.

Al crear el inquilino, deberás seleccionar este grupo para que tenga el permiso de acceso a raíz inicial tanto para la cuenta de inquilino de origen como para la de destino.



Si este grupo de administradores no existe en ambas grids antes de crear el tenant, el tenant no se replica en el destino.

Accede al asistente

Pasos

1. Selecciona **Tenants**.
2. Selecciona **Crear**.

Introduce los datos

Pasos

1. Introduce los datos del inquilino.

Campo	Descripción
Nombre	Un nombre para la cuenta de inquilino. No es necesario que los nombres de los inquilinos sean únicos. Cuando se crea la cuenta de inquilino, recibe un identificador de cuenta único de 20 dígitos.
Descripción (opcional)	Una descripción que ayude a identificar al inquilino. Si vas a crear un inquilino que utilizará una conexión de federación de grid, puedes usar este campo de forma opcional para ayudar a identificar cuál es el inquilino de origen y cuál es el de destino. Por ejemplo, esta descripción para un inquilino creado en Grid 1 también aparecerá para el inquilino replicado en Grid 2: "Este inquilino fue creado en Grid 1."
Tipo de cliente	Debe ser S3 .
Cuota de almacenamiento (opcional)	Si quieres que este inquilino tenga una cuota de almacenamiento, indica un valor numérico para la cuota y las unidades.

2. Selecciona **Continuar**.

Selecciona permisos

Pasos

1. Si lo deseas, selecciona los permisos básicos que quieres que tenga este inquilino.



Algunos de estos permisos tienen requisitos adicionales. Para obtener más información, selecciona el icono de ayuda correspondiente a cada permiso.

Permiso	Si seleccionas...
Permitir los servicios de la plataforma	El arrendatario puede utilizar los servicios de la plataforma S3, como CloudMirror. Consulta "Administra los servicios de plataforma para las cuentas de inquilino de S3" .
Usa tu propia fuente de identidad	El inquilino puede configurar y gestionar su propia fuente de identidad para grupos y usuarios federados. Esta opción está desactivada si tienes "SSO configurado" para tu sistema StorageGRID.
Permitir S3 Select	El inquilino puede realizar solicitudes de la API SelectObjectContent de S3 para filtrar y recuperar datos de objetos. Consulta "Administra S3 Select para cuentas de inquilino". Importante: Las solicitudes de SelectObjectContent pueden reducir el rendimiento del balanceador de carga para todos los clientes de S3 y todos los inquilinos. Activa esta función solo cuando sea necesario y solo para inquilinos de confianza.

2. Si lo deseas, selecciona los permisos avanzados que quieras que tenga este inquilino.

Permiso	Si seleccionas...
Conexión de federación de grid	El inquilino puede usar una conexión de federación de grid, que: • Hace que este inquilino y todos los grupos de inquilinos y usuarios añadidos a la cuenta se clonen desde esta grid (la <i>grid de origen</i>) a la otra grid en la conexión seleccionada (la <i>grid de destino</i>). • Permite a este inquilino configurar la replicación entre grids entre los buckets correspondientes de cada grid. Consulta "Gestiona los inquilinos permitidos para la federación de grid".
Bloqueo de objetos de S3	Permitir al inquilino usar funciones específicas de S3 Object Lock: • Establecer el periodo máximo de retención define durante cuánto tiempo deben conservarse los nuevos objetos añadidos a este bucket, a partir del momento en que se ingieren. • La opción «Permitir modo de cumplimiento» impide que los usuarios sobrescriban o eliminen versiones de objetos protegidos durante el periodo de retención.

3. Selecciona **Continuar**.

Define el acceso a raíz y crea un inquilino

Pasos

1. Define el acceso a raíz para la cuenta de inquilino, en función de si tu sistema StorageGRID utiliza la federación de identidades, el inicio de sesión único (SSO) o ambos.

Opción	Haz esto
Si la federación de identidades no está habilitada	Indica la contraseña que se usará al iniciar sesión en el tenant como usuario raíz local.
Si la federación de identidades está activada	a. Selecciona un grupo federado ya existente para disponer de permiso de acceso a raíz para el inquilino. b. Si lo deseas, indica la contraseña que se usará al iniciar sesión en el tenant como usuario raíz local.
Si están habilitados tanto la federación de identidades como el inicio de sesión único (SSO)	Selecciona un grupo federado existente para tener permiso de acceso a raíz para el inquilino. Ningún usuario local puede iniciar sesión.

2. Selecciona **Create tenant**.

Aparece un mensaje de éxito y el nuevo tenant aparece en la página Tenants. Para saber cómo ver los detalles del tenant y supervisar la actividad del tenant, consulta ["Supervisa la actividad de los inquilinos"](#).



Aplicar la configuración de los inquilinos en toda la grid podría tardar 15 minutos o más, según la conectividad de red, el estado de los nodos y las operaciones de Cassandra.

3. Si has seleccionado el permiso **Usar conexión de federación de grid** para el tenant:

- Confirma que se haya replicado un inquilino idéntico en el otro grid de la conexión. Los inquilinos de ambos grids tendrán el mismo ID de cuenta de 20 dígitos, nombre, descripción, cuota y permisos.



Si aparece el mensaje de error «Tenant creado sin clon», consulta las instrucciones en ["Solucionar errores de federación de grid"](#).

- Si proporcionaste una contraseña de usuario raíz local al definir el acceso a raíz, ["cambiar la contraseña del usuario raíz local"](#) para el inquilino replicado.



Un usuario raíz local no puede iniciar sesión en Tenant Manager en la red de destino hasta que se cambie la contraseña.

Inicia sesión en el tenant (opcional)

Según sea necesario, puedes iniciar sesión en el nuevo inquilino ahora para completar la configuración, o puedes iniciar sesión en el inquilino más tarde. Los pasos de inicio de sesión dependen de si has iniciado sesión en el Grid Manager utilizando el puerto predeterminado (443) o un puerto restringido. Consulta ["Controla el acceso en el cortafuegos externo"](#).

Inicia sesión ahora

Si estás utilizando...	Haz esto...
El puerto 443 y configuras una contraseña para el usuario raíz local	1. Selecciona Sign in as root. Cuando inicias sesión, aparecen enlaces para configurar los buckets, la federación de identidades, los grupos y los usuarios. 2. Selecciona los enlaces para configurar la cuenta de inquilino. Cada enlace abre la página correspondiente en Tenant Manager. Para completar la página, consulta "Instrucciones para usar las cuentas de inquilino".
Puerto 443 y no has establecido una contraseña para el usuario raíz local	Selecciona Sign in e introduce las credenciales de un usuario del grupo federado de acceso a raíz.
Un puerto restringido	1. Selecciona Finalizar 2. Selecciona Restricted en la tabla Tenant para obtener más información sobre cómo acceder a esta cuenta de inquilino. La URL de Tenant Manager tiene este formato: <code>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</code> ◦ <i>FQDN_or_Admin_Node_IP</i> es un nombre de dominio completo o la dirección IP de un nodo de administración ◦ <i>port</i> es el puerto exclusivo para el inquilino ◦ <i>20-digit-account-id</i> es el identificador único de la cuenta del arrendatario

Inicia sesión más tarde

Si estás utilizando...	Haz una de estas cosas...
Puerto 443	• Desde el Grid Manager, selecciona Tenants y luego selecciona Sign in a la derecha del nombre del tenant. • Introduce la URL del inquilino en un navegador web: <code>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</code> ◦ <i>FQDN_or_Admin_Node_IP</i> es un nombre de dominio completo o la dirección IP de un nodo de administración ◦ <i>20-digit-account-id</i> es el identificador único de la cuenta del arrendatario

Si estás utilizando...	Haz una de estas cosas...
Un puerto restringido	• Desde el Grid Manager, selecciona Tenants y luego selecciona Restricted. • Introduce la URL del inquilino en un navegador web: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> ◦ <i>FQDN_or_Admin_Node_IP</i> es un nombre de dominio completo o la dirección IP de un nodo de administración ◦ <i>port</i> es el puerto restringido solo para inquilinos ◦ <i>20-digit-account-id</i> es el identificador único de la cuenta del arrendatario

Configura el inquilino

Sigue las instrucciones de ["Utiliza una cuenta de inquilino"](#) para gestionar los grupos y usuarios del inquilino, las claves de acceso de S3, los buckets, los servicios de plataforma, y la clonación de cuentas y la replicación entre grids.

Editar una cuenta de inquilino de StorageGRID

Puedes editar la cuenta de un inquilino para cambiar el nombre que se muestra, la cuota de almacenamiento o los permisos del inquilino.



Si un inquilino tiene el permiso **Utilizar conexión de federación de grid**, puedes editar los detalles del inquilino desde cualquiera de los grids en la conexión. Sin embargo, los cambios que realices en un grid de la conexión no se copiarán al otro grid. Si quieres mantener los detalles del inquilino exactamente sincronizados entre grids, haz los mismos cambios en ambos grids. Consulta ["Gestiona los inquilinos permitidos para la conexión de federación de grid"](#).

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Acceso raíz o permisos de cuentas de inquilino"](#).



Aplicar la configuración de los inquilinos en toda la grid podría tardar 15 minutos o más, según la conectividad de red, el estado de los nodos y las operaciones de Cassandra.

Pasos

1. Selecciona **Tenants**.

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. Busca la cuenta de inquilino que deseas modificar.

Utiliza el cuadro de búsqueda para buscar un inquilino por nombre o por tenant ID.

3. Selecciona el inquilino. Puedes hacer cualquiera de las siguientes cosas:

- Marca la casilla de selección correspondiente al tenant y selecciona **Actions > Edit**.
- Selecciona el nombre del inquilino para mostrar la página de detalles y selecciona **Editar**.

4. Si lo deseas, puedes modificar los valores de estos campos:

- **Nombre**
- **Descripción**
- **Cuota de almacenamiento**

5. Selecciona **Continuar**.

6. Selecciona o desmarca los permisos de la cuenta de inquilino.

- Si desactivas 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 haya configurado como extremo. Consulta "[Administra los servicios de plataforma para las cuentas de inquilino de S3](#)".
- Modifica 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 configurada para el Grid Manager.

Si **Usar fuente de identidad propia** está:

- Deshabilitado y seleccionado, el inquilino ya ha activado su propio origen de identidad. Un inquilino debe deshabilitar su origen de identidad antes de poder usar el origen de identidad que se configuró para el Grid Manager.
- Si está desactivado y no se ha seleccionado, el inicio de sesión único está habilitado para el

sistema StorageGRID. El inquilino debe usar la fuente de identidad que se configuró para el Grid Manager.

- Selecciona o desmarca el permiso **Allow S3 Select** según lo necesites. Consulta ["Administra S3 Select para cuentas de inquilino"](#).
- Para eliminar el permiso **Usar conexión de federación de grid**:
 - i. Selecciona la pestaña **Grid federation**.
 - ii. Selecciona **Eliminar permiso**.
- Para añadir el permiso **Use grid federation connection**:
 - i. Selecciona la pestaña **Grid federation**.
 - ii. Selecciona la casilla **Usar conexión de federación de grid**.
 - iii. Opcionalmente, selecciona **Clonar usuarios y grupos locales existentes** para clonarlos en el grid remoto. Si quieres, puedes detener la clonación en curso o reintentar la clonación si algunos usuarios o grupos locales no se pudieron clonar después de que se completara la última operación de clonación.
- Para establecer un plazo máximo de conservación o habilitar el modo de cumplimiento:



Debes habilitar S3 Object Lock en la grid antes de poder usar estos ajustes.

- i. Selecciona la pestaña **S3 Object Lock**.
- ii. En el campo **Establecer periodo máximo de conservación**, introduce un valor y selecciona el periodo de tiempo en el menú desplegable.
- iii. Para **Permitir el modo de cumplimiento**, marca la casilla de verificación.

Cambiar la contraseña del usuario raíz local de un tenant de StorageGRID

Es posible que tengas que cambiar la contraseña del usuario raíz local de un inquilino si el usuario raíz se queda sin acceso a la cuenta.

Antes de empezar

- Has 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 tu sistema StorageGRID, el usuario raíz local no puede iniciar sesión en la cuenta del inquilino. Para realizar tareas de usuario raíz, los usuarios deben pertenecer a un grupo federado que tenga el permiso de acceso Root para el inquilino.

Pasos

1. Selecciona **Tenants**.

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	→ 📄

- Selecciona la cuenta de inquilino. Puedes hacer cualquiera de las siguientes cosas:
 - Marca la casilla de selección correspondiente al tenant y selecciona **Actions > Change root password**.
 - Selecciona el nombre del inquilino para abrir la página de detalles y selecciona **Actions > Change root password**.
- Introduce la nueva contraseña para la cuenta del inquilino.
- Selecciona **Guardar**.

Eliminar una cuenta de inquilino de StorageGRID

Puedes eliminar una cuenta de inquilino si quieres eliminar de forma permanente el acceso de ese inquilino al sistema.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).
- Has eliminado todos los buckets y objetos de S3 asociados con la cuenta de inquilino.
- Si se permite al inquilino utilizar una conexión de federación de grid, ya has revisado las consideraciones para ["Eliminar un inquilino con el permiso Use grid federation connection"](#).

Pasos

- Selecciona **Tenants**.
- Busca la cuenta o cuentas de inquilino que quieras eliminar.

Utiliza el cuadro de búsqueda para buscar un inquilino por nombre o por tenant ID.

- Para eliminar varios inquilinos, marca las casillas correspondientes y selecciona **Acciones > Eliminar**.
- Para eliminar un único inquilino, haz una de las siguientes acciones:
 - Marca la casilla de selección y selecciona **Actions > Delete**.

- Selecciona el nombre del inquilino para mostrar la página de detalles y, a continuación, selecciona **Actions > Delete**.

5. Selecciona **Sí**.

Gestiona los servicios de la plataforma

Conoce los servicios de la plataforma StorageGRID

Los servicios de plataforma incluyen la replicación de CloudMirror, las notificaciones de eventos y el servicio de integración de búsqueda.

Si habilitas los servicios de plataforma para las cuentas de inquilino de S3, debes configurar tu grid para que los inquilinos puedan acceder a los recursos externos necesarios para utilizar estos servicios.

Los servicios de plataforma no son compatibles con ["cubos de rama"](#).

CloudMirror replicación

El servicio de replicación CloudMirror de StorageGRID se utiliza para reflejar objetos específicos de un bucket de StorageGRID en un destino externo especificado.

Por ejemplo, podrías usar la replicación CloudMirror para reflejar registros específicos de clientes en Amazon S3 y luego aprovechar los servicios de AWS para hacer análisis de tus datos.

La replicación CloudMirror tiene algunas similitudes y diferencias importantes con la función de replicación entre grids. Para obtener más información, consulta ["Compara la replicación entre grids y la replicación CloudMirror"](#).



CloudMirror replication no es compatible si el bucket de origen tiene activada la función S3 Object Lock.

Notificaciones

Las notificaciones de eventos por bucket se utilizan para enviar notificaciones sobre acciones específicas realizadas en objetos a un clúster externo de Kafka, un endpoint de webhook o Amazon Simple Notification Service especificados.

Por ejemplo, podrías configurar alertas para que se envíen a los administradores sobre cada objeto añadido a un bucket, donde los objetos representan archivos de registro asociados con un evento crítico del sistema.



Aunque es posible configurar las notificaciones de eventos en un bucket con S3 Object Lock activado, los metadatos de S3 Object Lock (incluidos Retain Until Date y el estado de Legal Hold) 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 los metadatos de los objetos de S3 a un índice de Elasticsearch especificado, donde los metadatos pueden buscarse o analizarse usando el servicio externo.

Por ejemplo, podrías configurar tus buckets para que envíen los metadatos de los objetos de S3 a un servicio remoto de Elasticsearch. Luego, podrías usar Elasticsearch para realizar búsquedas en todos los buckets y hacer análisis sofisticados de los patrones presentes en los metadatos de tus objetos.



Aunque la integración con Elasticsearch se puede configurar en un bucket con S3 Object Lock activado, los metadatos de S3 Object Lock (incluidos Retain Until Date y el estado de Legal Hold) de los objetos no se incluirán en los mensajes de notificación.

Los servicios de plataforma les dan a los inquilinos la posibilidad de usar recursos de almacenamiento externos, servicios de notificación y servicios de búsqueda o análisis con sus datos. Como la ubicación de destino de los servicios de plataforma suele estar fuera de tu implementación de StorageGRID, debes decidir si quieres permitir que los inquilinos usen estos servicios. Si es así, debes habilitar el uso de los servicios de plataforma cuando crees o edites cuentas de inquilino. También tienes que configurar tu red para que los mensajes de los servicios de plataforma que generen los inquilinos puedan llegar a sus destinos.

Recomendaciones para usar los servicios de la plataforma

Antes de utilizar los servicios de la plataforma, ten en cuenta las siguientes recomendaciones:

- Si un bucket S3 en el sistema StorageGRID tiene habilitadas tanto la gestión de versiones como la replicación CloudMirror, también deberías habilitar la gestión de versiones del bucket S3 para el endpoint de destino. Esto permite que la replicación CloudMirror genere versiones de objetos similares en el endpoint.
- No debes usar más de 100 inquilinos activos con solicitudes de S3 que requieran replicación de CloudMirror, notificaciones e integración de búsqueda. Tener más de 100 inquilinos activos puede resultar en un rendimiento más lento del cliente S3.
- Las solicitudes dirigidas a un endpoint que no puedan completarse se pondrán en cola hasta un máximo de 500,000 solicitudes. Este límite se reparte a partes iguales entre los tenants activos. A los nuevos tenants se les permite superar temporalmente este límite de 500,000 para que los tenants recién creados no se vean penalizados injustamente.

Información relacionada

- ["Gestiona los servicios de la plataforma"](#)
- ["Configura los ajustes del proxy de almacenamiento"](#)
- ["Supervisar StorageGRID"](#)

Red y puertos para los servicios de plataforma StorageGRID

Si permites que un inquilino de S3 utilice los servicios de la plataforma, debes configurar la red para garantizar que los mensajes de los servicios de la plataforma puedan entregarse a sus destinos.

Puedes habilitar los servicios de plataforma para una cuenta de inquilino de S3 cuando crees o actualices la cuenta de inquilino. Si los servicios de plataforma están habilitados, el inquilino puede crear puntos de conexión que sirvan como destino para la replicación de CloudMirror, las notificaciones de eventos o los mensajes de integración de búsqueda de sus buckets de S3. Estos mensajes de servicios de plataforma se envían desde los nodos de almacenamiento que ejecutan el servicio ADC a los puntos de conexión de destino.

Por ejemplo, los inquilinos podrían configurar los siguientes tipos de puntos finales de destino:

- Un clúster de Elasticsearch alojado localmente
- Una aplicación local que permite recibir mensajes de Amazon Simple Notification Service
- Un clúster de Kafka alojado localmente

- Un endpoint de webhook externo o alojado localmente que admite solicitudes de notificación HTTP POST.

Este endpoint puede alojarse en diversos servidores web, frameworks o herramientas de procesamiento de datos, como Fluentd.

- Un bucket de S3 alojado localmente en la misma 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 los servicios de la plataforma, debes configurar la red o redes que contienen los nodos de almacenamiento del ADC. Debes asegurarte de que se puedan usar los siguientes puertos para enviar mensajes de los servicios de la plataforma a los endpoints de destino.

De forma predeterminada, los mensajes de los servicios de la plataforma se envían a través de los siguientes puertos:

- **80**: Para los URI de puntos finales que comienzan por http (la mayoría de los puntos finales)
- **443**: Para los URI de puntos finales que comienzan con https (la mayoría de los puntos finales)
- **9092**: Para los URI de endpoint que comienzan con http o https (solo endpoints de Kafka)

Los usuarios pueden especificar un puerto diferente cuando crean o editan un endpoint.



Si se utiliza una implementación de StorageGRID como destino para la replicación de CloudMirror, es posible que los mensajes de replicación se reciban en un puerto que no sea el 80 o el 443. Asegúrate de que el puerto que utiliza la implementación de StorageGRID de destino para S3 esté especificado en el endpoint.

Si utilizas un proxy no transparente, también debes ["configura los ajustes del proxy de almacenamiento"](#) para permitir el envío de mensajes a puntos finales externos, como un punto final en internet.

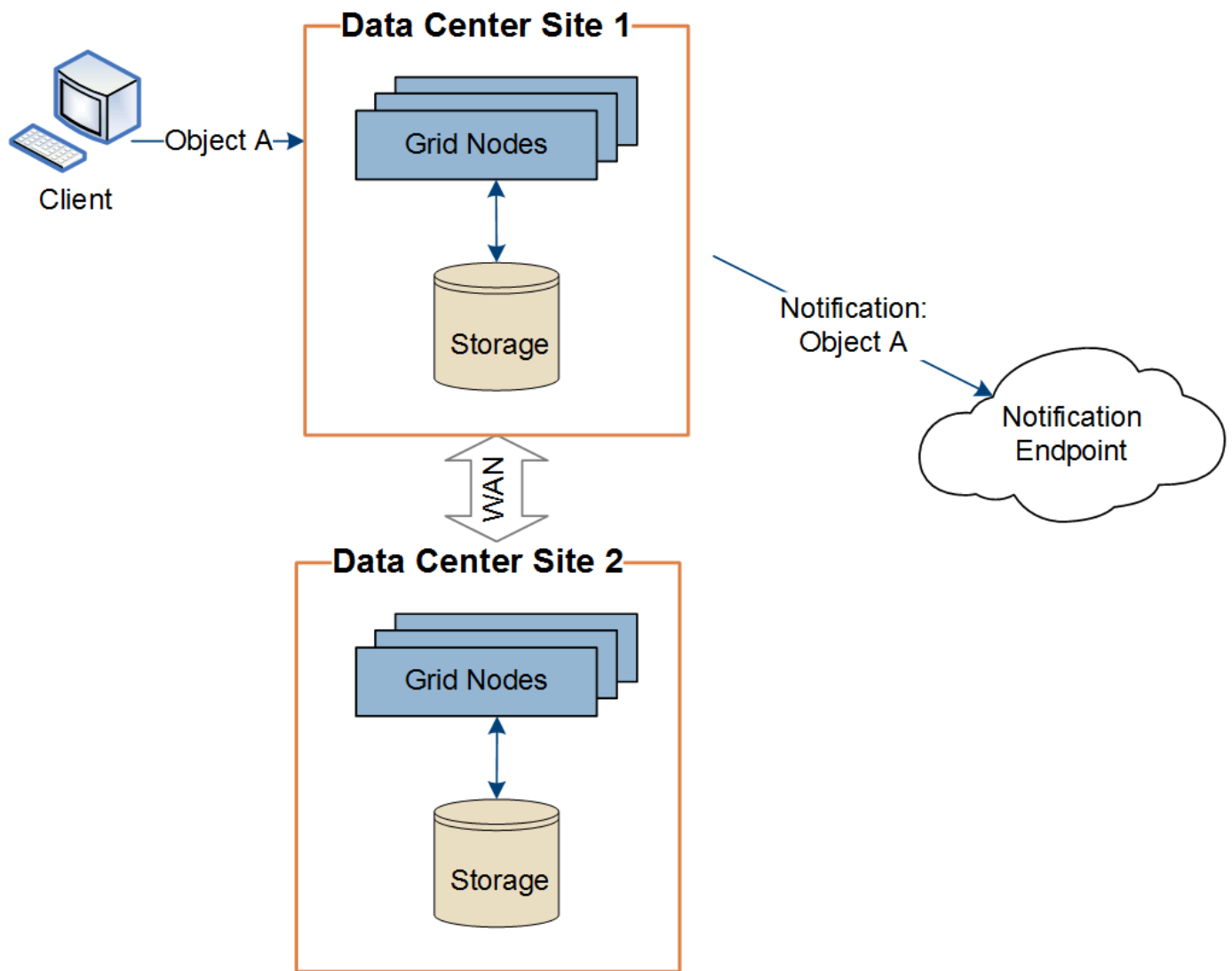
Información relacionada

["Utiliza una cuenta de inquilino"](#)

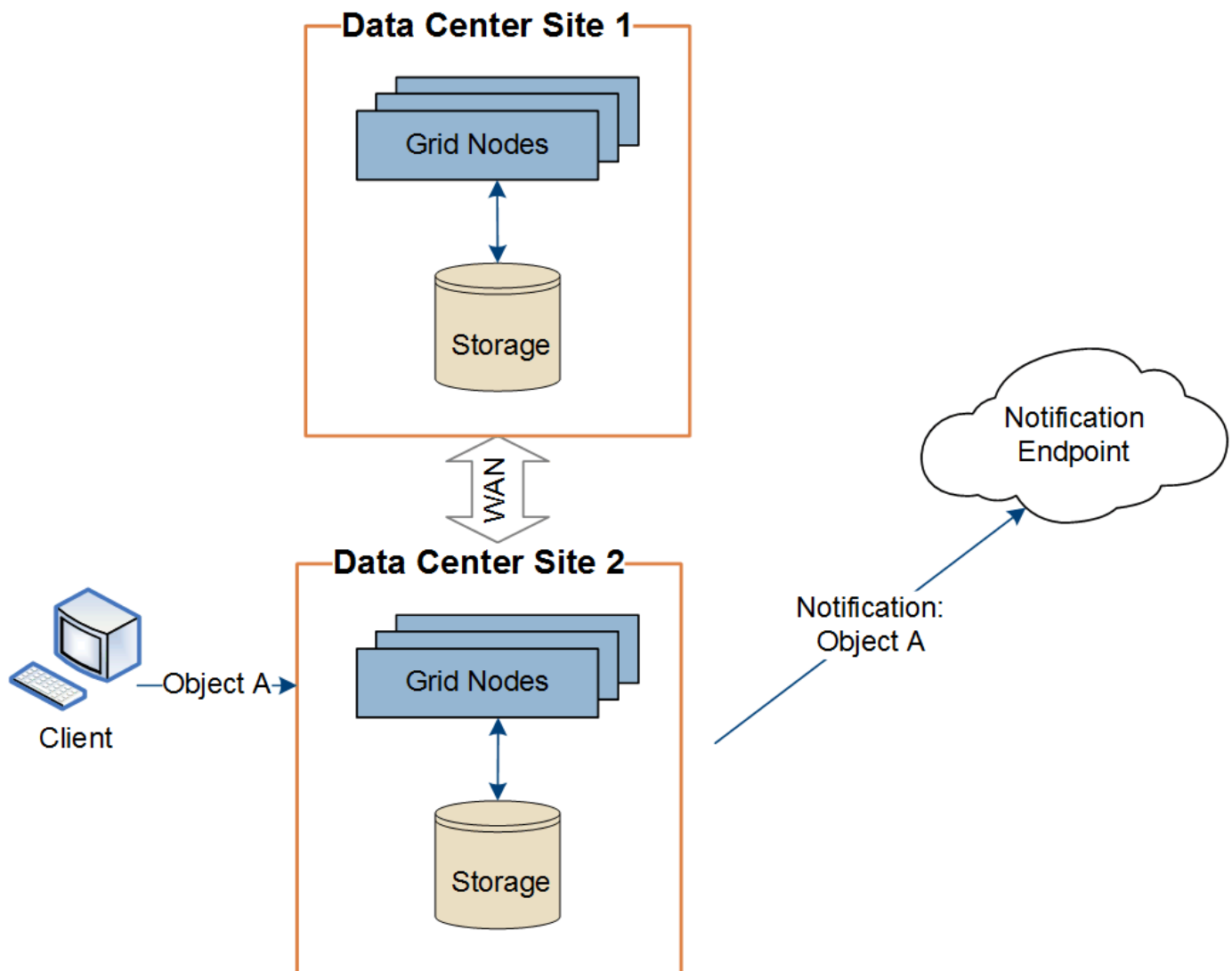
Entrega por sitio de mensajes de servicios de plataforma StorageGRID

Todas las operaciones de los servicios de la plataforma se realizan por sitio.

Es decir, si un inquilino utiliza un cliente para realizar una operación Create de la API S3 sobre un objeto conectándose a un Gateway Node en Data Center Site 1, la notificación sobre esa acción se activa y se envía desde Data Center Site 1.



Si posteriormente el cliente realiza una operación Delete de la API de S3 sobre ese mismo objeto desde Data Center Site 2, la notificación sobre la acción de eliminación se activa y se envía desde Data Center Site 2.



Asegúrate de que la red de cada sitio esté configurada de tal forma que los mensajes de los servicios de la plataforma puedan entregarse a sus destinos.

Soluciona problemas de los servicios de la plataforma StorageGRID

Los puntos finales utilizados en los servicios de la plataforma son creados y gestionados por los usuarios del inquilino en el Tenant Manager. Sin embargo, si un inquilino tiene problemas para configurar o usar los servicios de la plataforma, podrías usar el Grid Manager para ayudar a resolver el problema.

Problemas con los nuevos puntos finales

Antes de que un inquilino pueda usar los servicios de plataforma, debe crear uno o varios endpoints mediante el Tenant Manager. Cada endpoint 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 endpoint incluye tanto la ubicación del recurso externo como las credenciales necesarias para acceder a él.

Cuando un inquilino crea un endpoint, el sistema StorageGRID valida que el endpoint existe y que se puede acceder a él usando las credenciales que se especificaron. La conexión con el endpoint se valida desde un nodo en cada sitio.

Si falla la validación del endpoint, aparecerá un mensaje de error explicando por qué falló la validación del endpoint. El usuario del tenant debe resolver el problema y luego intentar crear el endpoint de nuevo.



La creación del endpoint fallará si los servicios de la plataforma no están habilitados para la cuenta del tenant.

Problemas con los puntos finales existentes

Si se produce un error cuando StorageGRID intenta acceder a un punto final existente, aparece un mensaje en el panel de control de Tenant Manager.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Los usuarios de Tenant pueden acceder a la página Endpoints para consultar el mensaje de error más reciente de cada endpoint y determinar cuánto tiempo hace que ocurrió el error. La columna **Last error** muestra el mensaje de error más reciente de cada endpoint e indica cuánto tiempo hace que ocurrió el error. Los errores que incluyen el icono  ocurrieron 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 logID entre paréntesis. Un administrador de grid o el soporte técnico pueden usar este ID para localizar información más detallada sobre el error en el bycast.log.

Problemas relacionados con los servidores proxy

Si has configurado un "[proxy de almacenamiento](#)" entre los nodos de almacenamiento y los puntos finales del servicio de la plataforma, pueden producirse errores si tu servicio proxy no permite mensajes de StorageGRID. Para resolver estos problemas, revisa la configuración de tu servidor proxy para asegurarte de que los mensajes relacionados con el servicio de la plataforma no estén bloqueados.

Determina si se ha producido un error

Si se ha producido algún error en los endpoints en los últimos 7 días, el panel de control en Tenant Manager muestra un mensaje de alerta. Puedes ir a la página de Endpoints para ver más detalles sobre el error.

Las operaciones del cliente fallan

Algunos problemas con los servicios de plataforma pueden hacer que las operaciones del cliente en el bucket S3 fallen. Por ejemplo, las operaciones del cliente de S3 fallarán si el servicio interno Replicated State Machine (RSM) se detiene o si hay demasiados mensajes de servicios de plataforma en cola para su entrega.

Para comprobar el estado de los servicios:

1. Selecciona **Nodos > site > Nodo de almacenamiento > Resumen**.
2. Comprueba si hay alertas activas en la tabla Alertas.
3. Resuelve cualquier alerta activa. Si es necesario, ponte en contacto con soporte técnico.

Errores de endpoint recuperables e irrecuperables

Una vez creados los puntos finales, pueden producirse errores en las solicitudes de servicios de la plataforma por diversos motivos. Algunos errores se pueden solucionar con la intervención del usuario. Por ejemplo, los errores solucionables pueden deberse a las siguientes causas:

- Las credenciales del usuario se han eliminado o han caducado.
- El contenedor de destino no existe.
- No se puede entregar la notificación.

Si StorageGRID detecta un error recuperable, la solicitud del servicio de la plataforma se volverá a intentar hasta que tenga éxito.

Otros errores son irrecuperables. Por ejemplo, los errores irrecuperables pueden ocurrir por las siguientes razones:

- El punto final se ha eliminado.
- Un punto final de webhook responde a una solicitud de notificación con un error 400 `Bad Request`.

Si StorageGRID detecta un error irrecuperable en un endpoint:

- En el Grid Manager, ve a **Soporte > Herramientas > Métricas > Grafana > Platform Services Overview** para ver los detalles del error.
- En Tenant Manager, ve a **ALMACENAMIENTO (S3) > Puntos de conexión de servicios de la plataforma** para ver los detalles del error.
- Consulta el `/var/local/log/bycast-err.log` para ver los errores relacionados. Los nodos de almacenamiento que cuentan con el servicio ADC contienen este archivo de registro.

No se pueden entregar los mensajes de los servicios de plataforma

Si el destino experimenta un problema que le impide aceptar mensajes de servicios de plataforma, la operación del cliente en el bucket se realiza correctamente, pero el mensaje de servicios de plataforma no se entrega. Por ejemplo, este error puede ocurrir si se actualizan las credenciales en el destino de manera que StorageGRID ya no pueda autenticarse en el servicio de destino.

Comprueba si hay alertas relacionadas.

Menor rendimiento en las solicitudes de servicios 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 supera la velocidad a la que el extremo de destino puede recibirlas. La limitación solo se produce cuando hay una acumulación de solicitudes en espera de enviarse al extremo de destino.

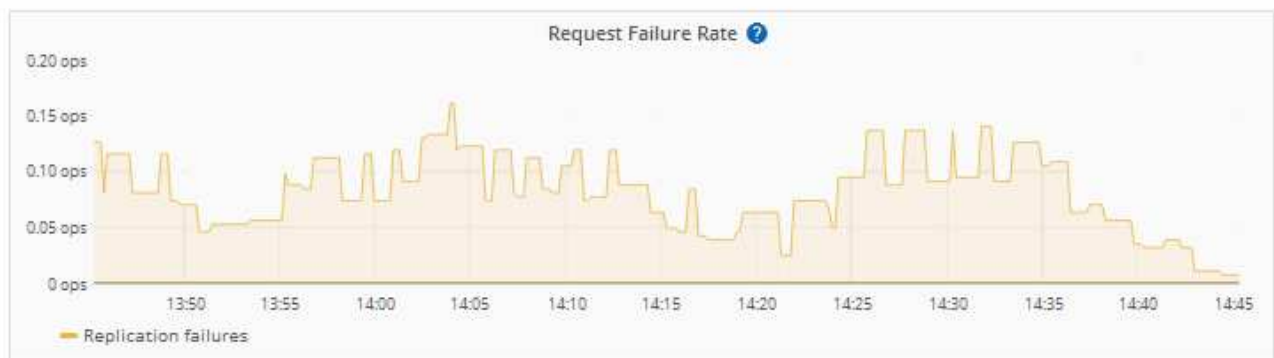
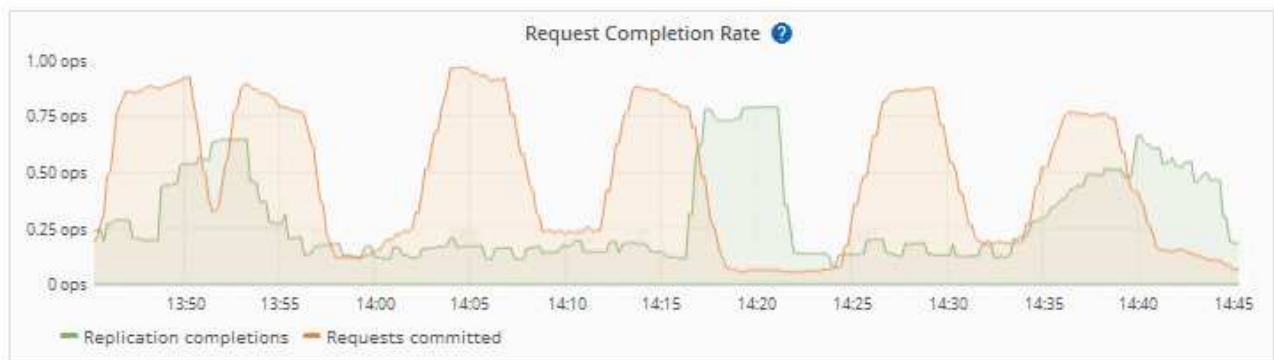
El único efecto visible es que las solicitudes S3 entrantes tardarán más en ejecutarse. Si empiezas a notar una ralentización significativa del rendimiento, deberías reducir la tasa de consumo o usar un endpoint con mayor capacidad. Si la acumulación de solicitudes sigue aumentando, las operaciones S3 de los clientes (como las solicitudes PUT) acabarán fallando.

Las solicitudes de CloudMirror tienen más probabilidades de verse afectadas por el rendimiento del punto final de destino porque normalmente implican más transferencia de datos que las solicitudes de integración de búsqueda o de notificación de eventos.

Las solicitudes de servicio de plataforma fallan

Para consultar la tasa de fallos de las solicitudes de los servicios de plataforma:

1. Selecciona **Nodos**.
2. Selecciona **site** > **Servicios de plataforma**.
3. Consulta el gráfico de la tasa de errores en las solicitudes.



Alerta de indisponibilidad de los servicios de la plataforma

La alerta **Servicios de la plataforma no disponibles** indica que no se pueden realizar operaciones de los servicios de la 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 endpoints.

Para resolver esta alerta, determina qué nodos de almacenamiento del sitio incluyen el servicio RSM. (El servicio RSM está presente en los nodos de almacenamiento que también incluyen el servicio ADC.) Luego, asegúrate de que una mayoría simple de esos nodos de almacenamiento estén en funcionamiento y disponibles.



Si en un sitio fallan varios nodos de almacenamiento que contienen el servicio RSM, pierdes cualquier solicitud de servicio de plataforma pendiente para ese sitio.

Guía adicional para la resolución de problemas en los endpoints de los servicios de plataforma

Para obtener más información, consulta [Utiliza una cuenta de inquilino](#) > [Soluciona problemas de los endpoints de los servicios de la plataforma](#).

Información relacionada

["Soluciona problemas del sistema StorageGRID"](#)

Administra S3 Select para cuentas de inquilinos en StorageGRID

Puedes permitir que ciertos tenants de S3 usen S3 Select para emitir solicitudes SelectObjectContent en objetos individuales.

S3 Select ofrece una forma eficaz de buscar en grandes volúmenes de datos sin tener que implementar una base de datos ni los recursos asociados para habilitar las búsquedas. También reduce el coste y la latencia al recuperar datos.

¿Qué es S3 Select?

S3 Select permite a los clientes de S3 utilizar solicitudes de SelectObjectContent para filtrar y recuperar únicamente los datos necesarios de un objeto. La implementación de S3 Select en StorageGRID incluye un subconjunto de comandos y funciones de S3 Select.

Consideraciones y requisitos para usar S3 Select

Requisitos de administración de Grid

El administrador de la grid debe conceder a los inquilinos la capacidad de S3 Select. Selecciona **Permitir S3 Select** cuando ["crear un inquilino"](#) o ["editar un inquilino"](#).

Requisitos de formato de los objetos

El objeto que deseas consultar debe tener uno de los siguientes formatos:

- **CSV.** Se puede usar tal cual o comprimir 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 en formato Parquet. Debes especificar el formato de salida como CSV o JSON.
 - El tamaño máximo de un grupo de filas sin comprimir es de 512 MB.
 - Debes utilizar los tipos de datos especificados en el esquema del objeto.
 - No puedes usar los tipos lógicos INTERVAL, JSON, LIST, TIME ni UUID.

Requisitos de los endpoints

La solicitud SelectObjectContent debe enviarse a ["Punto final del equilibrador de carga de StorageGRID"](#).

Los nodos de administración y gateway que utiliza el endpoint deben ser uno de los siguientes:

- Un nodo de appliance de servicios
- Un nodo de software basado en VMware
- Un nodo bare metal que ejecuta un kernel con cgroup v2 habilitado

Consideraciones generales

No puedes enviar consultas directamente a los nodos de almacenamiento.



Las solicitudes SelectObjectContent pueden reducir el rendimiento del balanceador de carga para todos los clientes de S3 y todos los inquilinos. Activa esta función solo cuando sea necesario y solo para inquilinos de confianza.

Consulta el ["Instrucciones para usar S3 Select"](#).

Para consultar ["Gráficos de Grafana"](#) de las operaciones S3 Select a lo largo del tiempo, selecciona **Soporte** > **Herramientas** > **Métricas** en el Grid Manager.

Configura las conexiones de los clientes

Configura conexiones de cliente S3 a StorageGRID

Como administrador de grid, gestionas las opciones de configuración que controlan cómo las aplicaciones cliente de S3 se conectan a tu sistema StorageGRID para almacenar y recuperar datos.



Se han eliminado los detalles sobre Swift de esta versión del sitio de documentación. Consulta ["StorageGRID 11.8: configura las conexiones de los clientes S3 y Swift"](#).

Tareas de configuración

1. Realiza las tareas previas necesarias en StorageGRID, según cómo la aplicación cliente se conecte a StorageGRID.

Tareas obligatorias

Debes obtener:

- Direcciones IP
- Nombres de dominio
- Certificado SSL

Tareas opcionales

Opcionalmente, configura:

- Federación de identidades
- SSO

1. Utiliza StorageGRID para obtener los valores que necesita la aplicación para conectarse a la grid. Puedes utilizar el asistente de configuración de S3 o configurar cada entidad de StorageGRID manualmente. +

Usa el asistente de configuración de S3

Sigue los pasos del asistente de configuración de S3.

Configurar manualmente

1. Crear grupo de alta disponibilidad
2. Crear un punto de conexión del equilibrador de carga
3. Crear cuenta de inquilino
4. Crear bucket y claves de acceso
5. Configura la regla y la política de ILM

1. Usa la aplicación S3 para completar la conexión con StorageGRID. Crea entradas de DNS para asociar direcciones IP a cualquier nombre de dominio que tengas pensado usar.

Si es necesario, realiza la configuración adicional de la aplicación.

2. Realiza tareas periódicas en la aplicación y en StorageGRID para gestionar y supervisar el almacenamiento de objetos a lo largo del tiempo.

Información necesaria para conectar StorageGRID a una aplicación cliente

Antes de poder conectar StorageGRID a una aplicación cliente de S3, debes realizar pasos de configuración en StorageGRID y obtener ciertos valores.

¿Qué valores necesito?

La siguiente tabla muestra los valores que debes configurar en StorageGRID y dónde se utilizan esos valores en la aplicación S3 y en el servidor DNS.

Valor	Dónde se configura el valor	Dónde se utiliza el valor
Direcciones IP virtuales (VIP)	StorageGRID > Grupo de alta disponibilidad	Entrada DNS
Puerto	StorageGRID > Punto de conexión del equilibrador de carga	Aplicación de cliente
Certificado SSL	StorageGRID > Punto de conexión del equilibrador de carga	Aplicación de cliente
Nombre del servidor (FQDN)	StorageGRID > Punto de conexión del equilibrador de carga	• Aplicación de cliente • Entrada DNS
ID de la clave de acceso de S3 y clave de acceso secreta	StorageGRID > Usuario y bucket	Aplicación de cliente

Valor	Dónde se configura el valor	Dónde se utiliza el valor
Nombre del bucket/contenedor	StorageGRID > Usuario y bucket	Aplicación de cliente

¿Cómo obtengo estos valores?

En función de tus necesidades, puedes hacer cualquiera de las siguientes cosas para obtener la información que necesitas:

- Usa el **"Asistente de configuración de S3"**. El asistente de configuración de S3 te ayuda a configurar rápidamente los valores necesarios en StorageGRID y genera uno o dos archivos que puedes usar al configurar la aplicación S3. El asistente te guía a través de los pasos necesarios y te ayuda a asegurarte de que tu configuración cumpla con las mejores prácticas de StorageGRID.



Si estás configurando una aplicación S3, se recomienda utilizar el asistente de configuración de S3, a menos que sepas que tienes requisitos especiales o que tu implementación vaya a requerir una personalización significativa.

- Usa el **"Asistente de configuración de FabricPool"**. De forma similar al asistente de configuración de S3, el asistente de configuración de FabricPool te ayuda a configurar rápidamente los valores necesarios y genera un archivo que puedes usar cuando configures un nivel de cloud de FabricPool en ONTAP.



Si planeas usar StorageGRID como el sistema de almacenamiento de objetos para un nivel de cloud de FabricPool, se recomienda usar el asistente de configuración de FabricPool, a menos que sepas que tienes requisitos especiales o que tu implementación requerirá una personalización importante.

- **Configura los elementos manualmente.** Si te estás conectando a una aplicación S3 y prefieres no usar el asistente de configuración de S3, puedes obtener los valores necesarios realizando la configuración manualmente. Sigue estos pasos:
 - a. Configura el grupo de alta disponibilidad (HA) que quieras utilizar para la aplicación S3. Consulta ["Configurar grupos de alta disponibilidad"](#).
 - b. Crea el punto de conexión del equilibrador de carga que utilizará la aplicación S3. Consulta ["Configura los puntos de conexión del equilibrador de carga"](#).
 - c. Crea la cuenta de inquilino que utilizará la aplicación S3. Consulta ["Crear una cuenta de inquilino"](#).
 - d. Para un inquilino de S3, inicia sesión en la cuenta del inquilino y genera un ID de clave de acceso y una clave de acceso secreta para cada usuario que vaya a acceder a la aplicación. Consulta ["Crea tus propias claves de acceso"](#).
 - e. Crea uno o más buckets de S3 dentro de la cuenta de tenant. Para S3, consulta ["Crear un bucket de S3"](#).
 - f. Para añadir instrucciones de ubicación específicas para los objetos que pertenecen al nuevo inquilino o bucket/contenedor, crea una nueva regla de ILM y activa una nueva política de ILM para usar esa regla. Consulta ["Crear regla de ILM"](#) y ["Crear política de ILM"](#).

Seguridad para clientes S3 en StorageGRID

Las cuentas de inquilino de StorageGRID usan aplicaciones de cliente S3 para guardar datos de objetos en StorageGRID. Deberías revisar las medidas de seguridad implementadas para las aplicaciones de cliente.

Resumen

La siguiente lista resume cómo se implementa la seguridad en la API de 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 clientes

ID de clave de acceso y clave de acceso secreta de la cuenta S3

Autorización del cliente

La titularidad del bucket y todas las políticas de control de acceso aplicables

Cómo StorageGRID proporciona seguridad para las aplicaciones cliente

Las aplicaciones cliente de S3 pueden conectarse al servicio Load Balancer en los nodos de Gateway o Admin, o directamente a los nodos de Storage.

- Los clientes que se conectan al servicio de equilibrador de carga pueden usar HTTPS o HTTP, según cómo ["configura el punto de conexión del equilibrador de carga"](#).

HTTPS ofrece una comunicación segura cifrada mediante TLS y es la opción recomendada. Debes asociar un certificado de seguridad al punto final.

HTTP proporciona una comunicación menos segura y sin cifrar, y solo debe usarse para grids 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 la opción predeterminada y se recomienda.

HTTP proporciona una comunicación menos segura y sin cifrar, pero puede usarse opcionalmente ["habilitado"](#) para grids que no sean de producción o de prueba.

- Las comunicaciones entre StorageGRID y el cliente se cifran mediante TLS.
- Las comunicaciones entre el servicio de Load Balancer y los Storage Nodes dentro de la grid están cifradas, ya sea que el endpoint del Load Balancer esté configurado para aceptar conexiones HTTP o HTTPS.
- Los clientes deben proporcionar ["Encabezados de autenticación HTTP"](#) a StorageGRID para realizar operaciones de la API de REST.

Certificados de seguridad y aplicaciones de cliente

En todos los casos, las aplicaciones cliente pueden establecer conexiones TLS utilizando ya sea un certificado de servidor personalizado cargado por el administrador de la grid o un certificado generado por el sistema StorageGRID:

- Cuando las aplicaciones cliente se conectan al servicio de equilibrador de carga, utilizan el certificado que se ha configurado para el punto final del equilibrador de carga. Cada punto final del equilibrador de carga tiene su propio certificado—ya sea un certificado de servidor personalizado cargado por el administrador

de grid o un certificado que el administrador de grid generó en StorageGRID al configurar el punto final.

Consulta ["Aspectos a tener en cuenta 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 crearon para los nodos de almacenamiento al instalar el sistema StorageGRID (que están firmados por la entidad de certificación del sistema) o un único certificado de servidor personalizado proporcionado para el grid por un administrador de grid. Consulta ["agrega un certificado personalizado de la API S3"](#).

Los clientes deben configurarse para que confíen en la autoridad de certificación que haya firmado el certificado que utilicen para establecer conexiones TLS.

Algoritmos de hash y cifrado compatibles con las bibliotecas TLS

El sistema StorageGRID admite un conjunto de conjuntos de cifrado que las aplicaciones cliente pueden utilizar al establecer una sesión TLS. Para configurar los cifrados, ve a **Configuración > Seguridad > Ajustes de seguridad** y selecciona **Políticas de TLS y SSH**.

Versiones compatibles de TLS

StorageGRID es compatible con TLS 1.2 y TLS 1.3.



SSLv3 y TLS 1.1 (o versiones anteriores) ya no son compatibles.

Usa el asistente de configuración de S3

Consideraciones y requisitos del asistente de configuración de StorageGRID S3

Puedes utilizar el asistente de configuración de S3 para configurar StorageGRID como sistema de almacenamiento de objetos para una aplicación S3.

Cuándo utilizar el asistente de configuración de S3

El asistente de configuración de S3 te guía a lo largo de cada paso de la configuración de StorageGRID para su uso con una aplicación S3. Como parte de completar el asistente, descargas archivos que puedes usar para introducir valores en la aplicación S3. Utiliza el asistente para configurar tu sistema más rápido y para asegurarte de que tus ajustes cumplen con las mejores prácticas de StorageGRID.

Si tienes la ["Permiso de acceso raíz"](#), puedes completar el asistente de configuración de S3 cuando empieces a usar StorageGRID Grid Manager, o puedes acceder y completar el asistente en cualquier momento después. Dependiendo de tus necesidades, también puedes configurar manualmente algunos o todos los elementos necesarios y luego usar el asistente para reunir los valores que necesita una aplicación S3.

Antes de utilizar el asistente

Antes de utilizar el asistente, comprueba que has cumplido estos requisitos previos.

Obtener direcciones IP y configurar interfaces VLAN

Si vas a configurar un grupo de alta disponibilidad (HA), ya sabes a qué nodos se conectará la aplicación S3 y qué red StorageGRID se utilizará. También sabes qué valores debes introducir para el CIDR de la subred, la dirección IP de la puerta de enlace y las direcciones IP virtuales (VIP).

Si tienes previsto usar una LAN virtual para segregar el tráfico de la aplicación S3, ya configuraste la

interfaz de la VLAN. Consulta ["Configurar interfaces VLAN"](#).

Configura la federación de identidades y el inicio de sesión único (SSO)

Si tienes previsto usar la federación de identidades o el inicio de sesión único (SSO) para tu sistema StorageGRID, ya habrás habilitado estas funciones. También sabes qué grupo federado debe tener acceso a raíz para la cuenta de inquilino que usará la aplicación S3. Consulta ["Usa la federación de identidades"](#) y ["Configura el inicio de sesión único"](#).

Obtener y configurar nombres de dominio

Ya sabes qué nombre de dominio completo (FQDN) debes usar para StorageGRID. Las entradas del servidor de nombres (DNS) asignarán este FQDN a las direcciones IP virtuales (VIP) del grupo de alta disponibilidad (HA) que crees usando el asistente.

Si tienes pensado utilizar solicitudes de S3 de tipo virtual hosted-style, debes tener ["Nombres de dominio de los endpoints S3 configurados"](#). Se recomienda utilizar solicitudes de tipo virtual hosted-style.

Revisa los requisitos del equilibrador de carga y del certificado de seguridad

Si tienes previsto utilizar el equilibrador de carga de StorageGRID, ya revisaste las consideraciones generales para el equilibrio de carga. Tienes los certificados que vas a cargar o los valores que necesitas para generar un certificado.

Si tienes previsto usar un endpoint de un equilibrador de carga externo (de terceros), tienes el nombre de dominio completo (FQDN), el puerto y el certificado para ese equilibrador de carga.

Configura cualquier conexión de federación de redes

Si deseas permitir que el inquilino de S3 clone los datos de la cuenta y replique los objetos del bucket en otra grid mediante una conexión de federación de grids, comprueba lo siguiente antes de iniciar el asistente de configuración:

- Tienes ["configuraste la conexión de federación de grid"](#).
- El estado de la conexión es **Conectado**.
- Tienes permiso de acceso root.

Accede y completa el asistente de configuración de S3 en StorageGRID

Puedes 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 necesita la aplicación para acceder a un bucket de StorageGRID y guardar objetos.

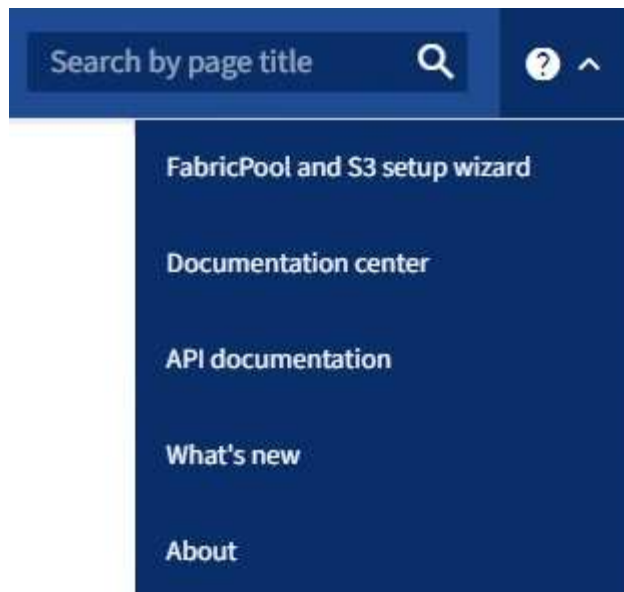
Antes de empezar

- Tienes el ["Permiso de acceso raíz"](#).
- Has revisado la ["consideraciones y requisitos"](#) para usar el asistente.

Accede al asistente

Pasos

1. Inicia sesión en Grid Manager usando una ["navegador web compatible"](#) cuenta.
2. Si aparece en el panel de control el banner **FabricPool and S3 setup wizard**, selecciona el enlace que aparece en el banner. Si el banner ya no aparece, selecciona el icono de ayuda de la barra de encabezado en el Grid Manager y selecciona **FabricPool and S3 setup wizard**.



3. En la sección de aplicación S3 de la página del asistente de configuración de FabricPool y S3, selecciona **Configurar ahora**.

Paso 1 de 6: Configura el grupo de alta disponibilidad

Un grupo de alta disponibilidad (HA) es un conjunto de nodos que contienen, cada uno de ellos, el servicio StorageGRID Load Balancer. Un grupo de alta disponibilidad (HA) puede contener Gateway Nodes, Admin Nodes o ambos.

Puedes usar 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 gestionar la carga de trabajo con poco impacto en las operaciones de S3.

Para obtener más información sobre esta tarea, consulta "[Gestiona grupos de alta disponibilidad](#)".

Pasos

1. Si tienes pensado utilizar un equilibrador de carga externo, no es necesario que crees un grupo de alta disponibilidad. Selecciona **Omitir este paso** y ve a [Paso 2 de 6: Configura el endpoint del balanceador de carga](#).
2. Para utilizar el equilibrador de carga de StorageGRID, puedes crear un nuevo grupo de alta disponibilidad (HA) o usar un grupo de alta disponibilidad (HA) existente.

Crear grupo de alta disponibilidad

- a. Para crear un nuevo grupo de alta disponibilidad, selecciona **Crear grupo de alta disponibilidad**.
- b. En el paso **Introducir datos**, rellena los siguientes campos.

Campo	Descripción
Nombre del grupo HA	Un nombre para mostrar único para este grupo de alta disponibilidad.
Descripción (opcional)	La descripción de este grupo de HA.

- c. En el paso **Add interfaces**, selecciona las interfaces de nodo que quieres usar en este grupo de alta disponibilidad.

Utiliza los encabezados de las columnas para ordenar las filas o introduce un término de búsqueda para encontrar interfaces más rápido.

Puedes seleccionar uno o varios nodos, pero solo puedes seleccionar una interfaz por cada nodo.

- d. Para el paso **Priorizar interfaces**, determina la interfaz principal y cualquier interfaz de respaldo para este grupo de alta disponibilidad.

Arrastra las filas para cambiar los valores de la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa salvo que se produzca un fallo.

Si el grupo de alta disponibilidad (HA) incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se transfieren a la primera interfaz de respaldo según el orden de prioridad. Si esa interfaz falla, las direcciones VIP se transfieren a la siguiente interfaz de respaldo y así sucesivamente. Cuando se resuelven los fallos, las direcciones VIP vuelven a la interfaz disponible con mayor prioridad.

- e. En el paso **Introducir direcciones IP**, completa los siguientes campos.

Campo	Descripción
CIDR de la 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 activado. Por ejemplo, 192.16.0.0/22.

Campo	Descripción
Dirección IP de la puerta de enlace (opcional)	Si las direcciones IP de S3 utilizadas para acceder a StorageGRID no se encuentran en la misma subred que las direcciones VIP de StorageGRID, introduce la dirección IP de la puerta de enlace local de la VIP de StorageGRID. La dirección IP de la puerta de enlace local debe estar dentro de la subred de la VIP.
Dirección IP virtual	Introduce al menos una y no más de diez direcciones VIP para la interfaz activa del grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP. Al menos una dirección debe ser IPv4. Opcionalmente, puedes especificar direcciones IPv4 e IPv6 adicionales.

f. Selecciona **Crear grupo de alta disponibilidad** y luego selecciona **Finalizar** para volver al asistente de configuración de S3.

g. Selecciona **Continuar** para pasar al paso del equilibrador de carga.

Usa el grupo de alta disponibilidad existente

a. Para utilizar un grupo de alta disponibilidad ya existente, selecciona el nombre del grupo en la opción **Select an HA group**.

b. Selecciona **Continuar** para pasar al paso del equilibrador de carga.

Paso 2 de 6: Configura el endpoint del balanceador de carga

StorageGRID utiliza un equilibrador de carga para gestionar la carga de trabajo de las aplicaciones cliente. El equilibrio de carga maximiza la velocidad y la capacidad de conexión entre varios Storage Nodes.

Puedes utilizar el servicio StorageGRID Load Balancer, que está disponible en todos los nodos Gateway y Admin, o puedes conectarte a un equilibrador de carga externo (de terceros). Se recomienda usar el load balancer de StorageGRID.

Para obtener más información sobre esta tarea, consulta ["Aspectos a tener en cuenta para el equilibrio de carga"](#).

Para usar el servicio StorageGRID Load Balancer, selecciona la pestaña **StorageGRID load balancer** y luego crea o selecciona el endpoint del load balancer que quieras usar. Para usar un load balancer externo, selecciona la pestaña **External load balancer** y proporciona los detalles sobre el sistema que ya configuraste.

Crear punto final

Pasos

1. Para crear un punto de conexión de equilibrador de carga, selecciona **Crear punto de conexión**.
2. En el paso **Introducir los datos del punto final**, rellena los siguientes campos.

Campo	Descripción
Nombre	Un nombre descriptivo para el endpoint.
Puerto	El puerto de StorageGRID que deseas utilizar para el equilibrio de carga. Este campo tiene por defecto el valor 10433 para el primer punto final que crees, pero puedes introducir cualquier puerto externo que no esté en uso. Si introduces 80 o 443, el punto final solo se configura en los nodos de Gateway, porque estos puertos están reservados en los nodos de Admin. Nota: No se permiten los puertos utilizados por otros servicios de la red. Consulta "Puertos internos de StorageGRID".
Tipo de cliente	Debe ser S3 .
Protocolo de red	Selecciona HTTPS. Nota: La comunicación con StorageGRID sin cifrado TLS es compatible, pero no se recomienda.

3. En el paso **Seleccionar modo de enlace**, especifica el modo de enlace. El modo de enlace controla cómo se accede al endpoint utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final usando la dirección IP de cualquier Gateway Node o Admin Node, la dirección IP virtual (VIP) de cualquier grupo HA en cualquier red, o el FQDN correspondiente. Utiliza la configuración Global (por defecto) a menos que necesites restringir la accesibilidad de este endpoint.
Direcciones IP virtuales de los grupos de alta disponibilidad	Los clientes deben utilizar una dirección IP virtual (o el nombre de dominio completo correspondiente) de un grupo de alta disponibilidad para acceder a este endpoint. Todos los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que selecciones para los puntos finales no se solapen.

Modo	Descripción
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o los FQDN correspondientes) de las interfaces de los nodos seleccionados para acceder a este endpoint.
Tipo de nodo	En función del tipo de nodo que selecciones, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier Admin Node o la dirección IP (o el FQDN correspondiente) de cualquier Gateway Node para acceder a este endpoint.

4. Para el paso de acceso del inquilino, selecciona una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (por defecto)	Todas las cuentas de inquilinos pueden usar este endpoint para acceder a sus buckets.
Permitir inquilinos seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este endpoint para acceder a sus buckets.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este endpoint para acceder a sus buckets. El resto de inquilinos sí pueden utilizar este endpoint.

5. En el paso **Adjuntar certificado**, selecciona una de las siguientes opciones:

Campo	Descripción
Subir certificado (recomendado)	Utiliza esta opción para cargar un certificado de servidor firmado por una CA, la clave privada del certificado y, opcionalmente, el paquete de CA.
Generar certificado	Utiliza esta opción para generar un certificado autofirmado. Consulta "Configura los puntos de conexión del equilibrador de carga" para ver los detalles de qué debes introducir.
Usa el certificado S3 de StorageGRID	Utiliza esta opción solo si ya has subido o generado una versión personalizada del certificado global de StorageGRID. Consulta "Configura los certificados de la API de S3" para obtener más información.

6. Selecciona **Finalizar** para volver al asistente de configuración de S3.

7. Selecciona **Continuar** para pasar al paso del inquilino y el bucket.



Los cambios en el certificado de un endpoint pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Utiliza el punto de conexión del equilibrador de carga existente

Pasos

1. Para utilizar un endpoint ya existente, selecciona su nombre en **Selecciona un endpoint del balanceador de carga**.
2. Selecciona **Continuar** para pasar al paso del inquilino y el bucket.

Utilizar un equilibrador de carga externo

Pasos

1. Para utilizar un equilibrador de carga externo, completa los siguientes campos.

Campo	Descripción
FQDN	El nombre de dominio completo (FQDN) del equilibrador de carga externo.
Puerto	El número de puerto que utilizará la aplicación S3 para conectarse al equilibrador de carga externo.
Certificado	Copia el certificado del servidor del equilibrador de carga externo y pégalo en este campo.

2. Selecciona **Continuar** para pasar al paso del inquilino y el bucket.

Paso 3 de 6: crea un inquilino y un bucket

Un inquilino es una entidad que puede utilizar aplicaciones de S3 para almacenar y recuperar objetos en StorageGRID. Cada inquilino tiene sus propios usuarios, claves de acceso, buckets, objetos y un conjunto específico de capacidades.

Un bucket es un contenedor que se utiliza para almacenar los objetos y los metadatos de un inquilino. Aunque los inquilinos pueden tener muchos buckets, el asistente te ayuda a crear un inquilino y un bucket de la forma más rápida y sencilla. Si necesitas añadir buckets o configurar opciones más adelante, puedes utilizar el Tenant Manager.

Para obtener más información sobre esta tarea, consulta ["Crear cuenta de inquilino"](#) y ["Crear un bucket de S3"](#).

Pasos

1. Introduce un nombre para la cuenta de inquilino.

Los nombres de los inquilinos no tienen por qué ser únicos. Al crear la cuenta de un inquilino, esta recibe un identificador de cuenta numérico único.

2. Define el acceso a raíz para la cuenta de inquilino, en función de si tu sistema StorageGRID utiliza ["federación de identidades"](#), ["inicio de sesión único \(SSO\)"](#) o ambos.

Opción	Haz esto
Si la federación de identidades no está habilitada	Indica la contraseña que se usará al iniciar sesión en el tenant como usuario raíz local.

Opción	Haz esto
Si la federación de identidades está activada	a. Selecciona un grupo federado ya existente para que el inquilino tenga "Permiso de acceso raíz" . b. Si lo deseas, indica la contraseña que se usará al iniciar sesión en el tenant como usuario raíz local.
Si están habilitados tanto la federación de identidades como el inicio de sesión único (SSO)	Selecciona un grupo federado existente para que el inquilino tenga "Permiso de acceso raíz" . Ningún usuario local puede iniciar sesión.

- Si quieres que el asistente cree el ID de la clave de acceso y la clave de acceso secreta para el usuario raíz, selecciona **Crear automáticamente la clave de acceso S3 del usuario raíz**.

Selecciona esta opción si el único usuario del inquilino va a ser el usuario raíz. Si otros usuarios van a utilizar este inquilino, **"usar Tenant Manager"** para configurar claves y permisos.

- Si quieres crear un bucket para este inquilino ahora, selecciona **Crear bucket para este inquilino**.



Si S3 Object Lock está habilitado para la grid, el bucket creado en este paso no tiene S3 Object Lock habilitado. Si necesitas usar un bucket con S3 Object Lock para esta aplicación de S3, no selecciones crear un bucket ahora. En su lugar, usa Tenant Manager para **"crear el bucket"** más adelante.

- Introduce el nombre del bucket que utilizará la aplicación S3. Por ejemplo, `s3-bucket`.

No puedes cambiar el nombre del bucket después de crearlo.

- Selecciona la **región** para este depósito.

Utiliza la región predeterminada (`us-east-1`) a menos que tengas previsto utilizar ILM en el futuro para filtrar objetos en función de la región del bucket.

- Selecciona **Crear y continuar**.

Paso 4 de 6: descargar datos

En el paso de descarga de datos, puedes descargar uno o dos archivos para guardar los detalles de lo que acabas de configurar.

Pasos

- Si has seleccionado **Crear automáticamente la clave de acceso S3 del usuario raíz**, haz una o ambas de las siguientes cosas:
 - Selecciona **Descargar claves de acceso** para descargar un archivo `.csv` que contiene el nombre de la cuenta del inquilino, el ID de la clave de acceso y la clave de acceso secreta.
 - Selecciona el icono de copiar () para copiar el ID de la clave de acceso y la clave secreta de acceso en el portapapeles.
- Selecciona **Descargar valores de configuración** para descargar un `.txt` archivo que contiene la configuración del punto final del balanceador de carga, el inquilino, el bucket y el usuario raíz.
- Guarda esta información en un lugar seguro.



No cierres esta página hasta que hayas copiado ambas claves de acceso. Las claves dejarán de estar disponibles una vez que cierres esta página. Asegúrate de guardar esta información en un lugar seguro porque puede usarse para obtener datos de tu sistema StorageGRID.

4. Si se te solicita, marca la casilla para confirmar que has descargado o copiado las claves.
5. Selecciona **Continuar** para ir al paso de reglas y políticas de ILM.

Paso 5 de 6: revisa la regla de ILM y la política de ILM para S3

Las reglas de gestión del ciclo de vida de la información (ILM) controlan la ubicación, la duración y el comportamiento de ingesta de todos los objetos en tu sistema StorageGRID. La política de ILM incluida con StorageGRID crea dos copias replicadas de todos los objetos. Esta política está vigente hasta que actives al menos una nueva política.

Pasos

1. Revisa la información que aparece en la página.
2. Si deseas añadir instrucciones específicas para los objetos que pertenecen al nuevo inquilino o bucket, crea una nueva regla y una nueva política. Consulta ["Crear regla de ILM"](#) y ["Usa políticas de ILM"](#).
3. Selecciona **He revisado estos pasos y entiendo lo que tengo que hacer**.
4. Marca la casilla de verificación para indicar que sabes qué hacer a continuación.
5. Selecciona **Continuar** para ir a **Resumen**.

Paso 6 de 6: resumen de revisión

Pasos

1. Revisa el resumen.
2. Toma nota de los detalles de los siguientes pasos, en los que se describe la configuración adicional que podría ser necesaria antes de conectarte al cliente S3. Por ejemplo, al seleccionar **Sign in as root** vas al Tenant Manager, donde puedes añadir usuarios del tenant, crear buckets adicionales y actualizar la configuración de los buckets.
3. Selecciona **Finalizar**.
4. Configura la aplicación usando el archivo que descargaste de StorageGRID o los valores que obtuviste manualmente.

Gestiona grupos de alta disponibilidad

Conoce los grupos de alta disponibilidad de StorageGRID

Los grupos de alta disponibilidad (HA) proporcionan conexiones de datos de alta disponibilidad para los clientes de S3 y conexiones de alta disponibilidad con el Grid Manager y el Tenant Manager.

Puedes 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 del grupo de HA falla, una interfaz de respaldo puede gestionar la carga de trabajo.

Cada grupo de HA proporciona acceso a los servicios compartidos en los nodos seleccionados.

- Los grupos de alta disponibilidad que incluyen Gateway Nodes, Admin Nodes o ambos proporcionan conexiones de datos de alta disponibilidad para los clientes de S3.
- Los grupos de alta disponibilidad que solo incluyen nodos de administración proporcionan conexiones de alta disponibilidad al Grid Manager y al Tenant Manager.
- Un grupo de alta disponibilidad (HA) que incluya únicamente dispositivos de servicios y nodos de software basados en VMware puede proporcionar conexiones de alta disponibilidad para ["Arrendatarios de S3 que utilizan S3 Select"](#). Se recomienda usar grupos de alta disponibilidad (HA) cuando usas S3 Select, pero no es obligatorio.

¿Cómo creas un grupo de alta disponibilidad?

1. Selecciona una interfaz de red para uno o varios nodos de administración o nodos de puerta de enlace. Puedes utilizar una interfaz de red Grid Network (eth0), una interfaz Client Network (eth2), una interfaz VLAN o una interfaz de acceso que hayas añadido al nodo.



No puedes añadir una interfaz a un grupo de alta disponibilidad si tiene una dirección IP asignada por DHCP.

2. Tú especificas una interfaz para que sea la interfaz principal. La interfaz principal es la interfaz activa a menos que ocurra un fallo.
3. Tú determinas el orden de prioridad para cualquier interfaz de Backup.
4. Asignas entre una y diez direcciones IP virtuales (VIP) al grupo. Las aplicaciones de los clientes pueden usar cualquiera de estas direcciones VIP para conectarse a StorageGRID.

Para ver las instrucciones, consulta ["Configurar grupos de alta disponibilidad"](#).

¿Qué es la interfaz activa?

Durante el funcionamiento normal, todas las direcciones VIP del grupo de alta disponibilidad (HA) se añaden a la interfaz primaria, que es la primera interfaz en el orden de prioridad. Mientras la interfaz primaria siga estando disponible, se utiliza cuando los clientes se conectan a cualquier dirección VIP del grupo. Es decir, durante el funcionamiento normal, la interfaz primaria es la interfaz "activa" del grupo.

Del mismo modo, durante el funcionamiento normal, cualquier interfaz de menor prioridad del grupo de alta disponibilidad actúa como interfaz «de reserva». Estas interfaces de reserva no se utilizan a menos que la interfaz principal (la que está activa en ese momento) deje de estar disponible.

Ver el estado actual del grupo de alta disponibilidad de un nodo

Para comprobar si un nodo está asignado a un grupo de alta disponibilidad y determinar su estado actual, selecciona **Nodos > nodo**.

Si la pestaña **Resumen** incluye una entrada para **HA groups**, el nodo está asignado a los HA groups que aparecen en la lista. El valor que aparece tras el nombre del grupo es el estado actual del nodo en el HA group:

- **Activo:** El grupo de alta disponibilidad está alojado actualmente en este nodo.
- **Reserva:** El grupo de alta disponibilidad no está utilizando este nodo en este momento; esta es una interfaz de reserva.
- **Detenido:** El grupo de alta disponibilidad no se puede alojar en este nodo porque el servicio de alta disponibilidad (keepalived) se ha detenido manualmente.

- **Error:** El grupo de alta disponibilidad no se puede alojar en este nodo debido a una o varias de las siguientes causas:
 - El servicio Load Balancer (nginx-gw) no se está ejecutando en el nodo.
 - La interfaz eth0 o VIP del nodo está inactiva.
 - El nodo está inactivo.

En este ejemplo, el nodo de administración principal se ha añadido a dos grupos de alta disponibilidad. Este nodo es actualmente la interfaz activa para el grupo de clientes Admin y una interfaz de respaldo para el grupo de clientes 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 ocurre cuando falla la interfaz activa?

La interfaz que actualmente aloja las direcciones VIP es la interfaz activa. Si el grupo de alta disponibilidad (HA) incluye más de una interfaz y la interfaz activa falla, las direcciones VIP se trasladan a la primera interfaz de respaldo disponible según el orden de prioridad. Si esa interfaz falla, las direcciones VIP se trasladan a la siguiente interfaz de respaldo disponible, y así sucesivamente.

La conmutación por error puede activarse por cualquiera de estas razones:

- El nodo en el que está configurada la interfaz deja de funcionar.
- El nodo en el que se configura la interfaz pierde la 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 debido a fallos de red externos al nodo que aloja la interfaz activa. Del mismo modo, la conmutación por error no se activa por los servicios de Grid Manager o Tenant Manager.

El proceso de conmutación por error suele durar solo unos segundos y es lo suficientemente rápido como para que las aplicaciones cliente apenas noten el impacto y puedan seguir funcionando con normalidad mediante los mecanismos habituales de reintento.

Cuando se resuelve el fallo y una interfaz de mayor prioridad vuelve a estar disponible, las direcciones VIP se mueven automáticamente a la interfaz disponible de mayor prioridad.

Cómo los grupos de HA de StorageGRID proporcionan alta disponibilidad

Puedes utilizar grupos de alta disponibilidad (HA) para proporcionar conexiones de alta disponibilidad a StorageGRID para datos de objetos y para uso administrativo.

- Un grupo de alta disponibilidad puede proporcionar conexiones administrativas de alta disponibilidad al Grid Manager o al Tenant Manager.
- Un grupo de alta disponibilidad puede proporcionar conexiones de datos altamente disponibles para los clientes de S3.
- Un grupo HA que contiene solo una interfaz te permite proporcionar muchas direcciones VIP y configurar explícitamente direcciones IPv6.

Un grupo de alta disponibilidad (HA) solo puede ofrecer alta disponibilidad si todos los nodos incluidos en el grupo prestan los mismos servicios. Al crear un grupo de alta disponibilidad, añade interfaces de los tipos de nodos que prestan los servicios que necesitas.

- **Nodos de administración:** Incluye el servicio de equilibrador de carga y habilita el acceso al Grid Manager o al Tenant Manager.
- **Nodos de puerta de enlace:** Incluyen el servicio de Load Balancer.

Objetivo del grupo HA	Agrega nodos de este tipo al grupo de alta disponibilidad
Acceso a Grid Manager	• Nodo de administración principal (Principal) • Nodos de administración no primarios Nota: El nodo de administración principal debe ser la interfaz principal. Algunos procedimientos de mantenimiento solo pueden realizarse desde el nodo de administración principal.
Acceso solo a Tenant Manager	• Nodos de administración primarios o no primarios
Acceso de cliente S3—servicio de equilibrador de carga	• Nodos de administración • Nodos de puerta de enlace

Objetivo del grupo HA	Agrega nodos de este tipo al grupo de alta disponibilidad
Acceso de cliente S3 para "S3 Select"	• Dispositivos de servicios • Nodos de software basados en VMware Nota: Se recomienda utilizar grupos HA al emplear S3 Select, aunque no es obligatorio.

Limitaciones de usar grupos HA con Grid Manager o Tenant Manager

Si falla el servicio Grid Manager o Tenant Manager, no se activa la conmutación por error del grupo HA.

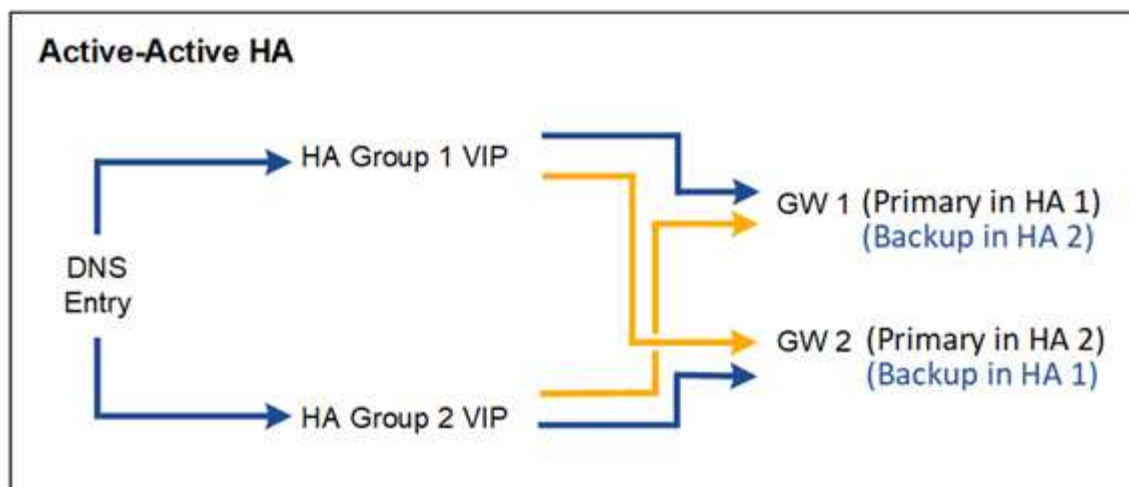
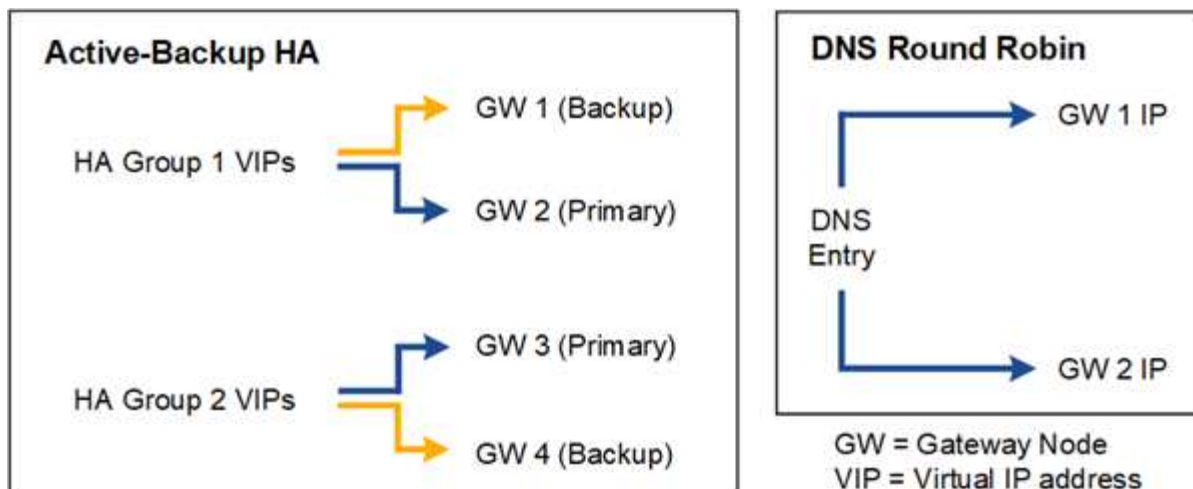
Si has iniciado sesión en Grid Manager o en Tenant Manager cuando se produce una conmutación por error, se cerrará tu sesión y debes volver a iniciar sesión para reanudar tu tarea.

Algunos procedimientos de mantenimiento no se pueden llevar a cabo cuando el nodo de administración principal no está disponible. Durante la conmutación por error, puedes usar Grid Manager para supervisar tu sistema StorageGRID.

Opciones de configuración para los grupos de alta disponibilidad de StorageGRID

Los siguientes diagramas ofrecen ejemplos de diferentes formas en que puedes configurar grupos de alta disponibilidad (HA). Cada opción tiene ventajas y desventajas.

En los diagramas, el azul indica la interfaz principal en el grupo de alta disponibilidad y el amarillo indica la interfaz de respaldo en el grupo de alta disponibilidad.



La tabla resume las ventajas de cada configuración de HA que se muestra en el diagrama.

Configuración	Ventajas	Desventajas
HA activo-backup	- Gestionado por StorageGRID sin dependencias externas. - Conmutación rápida por error.	Solo un nodo de un grupo de alta disponibilidad está activo. Al menos un nodo por grupo de alta disponibilidad estará inactivo.
DNS Round Robin	- Aumento del rendimiento total. - No hay hosts inactivos.	- Conmutación por error lenta, que podría depender del comportamiento del cliente. - Requiere configuración de hardware fuera de StorageGRID. - Es necesario que el cliente realice una comprobación del estado.

Configuración	Ventajas	Desventajas
HA activo-activo	• El tráfico se distribuye entre varios grupos de alta disponibilidad. • Alto rendimiento agregado que escala con el número de grupos de alta disponibilidad. • Conmutación rápida por error.	• Más complicado de configurar. • Requiere configuración de hardware fuera de StorageGRID. • Es necesario que el cliente realice una comprobación del estado.

Configura grupos de alta disponibilidad en StorageGRID

Puedes 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.



Un sistema StorageGRID puede tener un máximo de 255 grupos de alta disponibilidad.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).
- Si tienes previsto utilizar una interfaz VLAN en un grupo de alta disponibilidad (HA), ya has creado la interfaz VLAN. Consulta ["Configurar interfaces VLAN"](#).
- Si tienes previsto utilizar una interfaz de acceso para un nodo de un grupo de alta disponibilidad, ya creaste la interfaz:
 - **Linux (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Linux (después de instalar el nodo):** ["Agrega interfaces trunk o de acceso a un nodo"](#)
 - **VMware (tras instalar el nodo):** ["Agrega interfaces trunk o de acceso a un nodo"](#)



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Crear un grupo de alta disponibilidad

Cuando creas un grupo de alta disponibilidad, seleccionas una o más interfaces y las organizas por orden de prioridad. Luego, asignas una o más direcciones VIP al grupo.

Una interfaz debe pertenecer a un Gateway Node o a un Admin Node para poder incluirse en un grupo de HA. Un grupo de HA solo puede usar una interfaz para un nodo determinado; sin embargo, puedes usar otras interfaces del mismo nodo en otros grupos de HA.

Accede al asistente

Pasos

1. Selecciona **Configuración > Red > Grupos de alta disponibilidad**.
2. Selecciona **Crear**.

Introduce los datos del grupo HA

Pasos

1. Introduce un nombre único para el grupo de alta disponibilidad.
2. Si lo deseas, introduce una descripción para el grupo de alta disponibilidad.
3. Selecciona **Continuar**.

Agrega interfaces al grupo HA

Pasos

1. Selecciona una o varias interfaces para añadir a este grupo de alta disponibilidad.

Utiliza los encabezados de las columnas para ordenar las filas o introduce un término de búsqueda para encontrar interfaces más rápido.

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



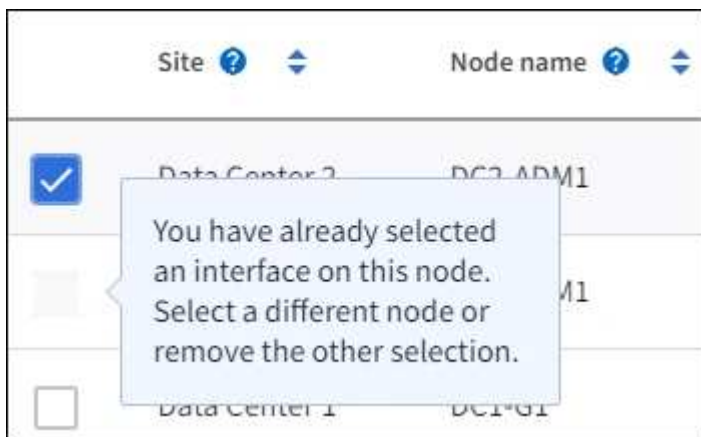
Una vez creada la interfaz VLAN, espera hasta 5 minutos para que la nueva interfaz aparezca en la tabla.

Directrices para la selección de interfaces

- Debes seleccionar al menos una interfaz.
- Solo puedes seleccionar una interfaz por nodo.
- Si el grupo HA está destinado a la protección HA de los servicios de Admin Node, que incluyen Grid Manager y Tenant Manager, selecciona únicamente las interfaces en los Admin Nodes.
- Si el grupo de HA es para la protección de HA del tráfico de clientes S3, selecciona interfaces en los nodos de administración, nodos de gateway o en ambos.
- Si seleccionas interfaces en diferentes tipos de nodos, aparecerá una nota informativa. Se te recuerda que, si ocurre una conmutación por error, es posible que los servicios proporcionados por el nodo que estaba activo anteriormente no estén disponibles en el nuevo nodo activo. Por ejemplo, un nodo

Gateway de respaldo no puede proporcionar protección HA de los servicios del nodo Admin. De manera similar, un nodo Admin de respaldo no puede realizar todos los procedimientos de mantenimiento que puede proporcionar el nodo Admin principal.

- Si no puedes seleccionar una interfaz, su casilla de verificación estará desactivada. La descripción emergente proporciona más información.



- No puedes seleccionar una interfaz si el valor de su subred o su puerta de enlace entra en conflicto con el de otra interfaz seleccionada.
- No puedes seleccionar una interfaz configurada si no tiene una dirección IP estática.

2. Selecciona **Continuar**.

Determina el orden de prioridad

Si el grupo de HA incluye más de una interfaz, puedes determinar cuál es la interfaz primaria y cuáles son las interfaces de respaldo (conmutación por error). Si la interfaz primaria falla, las direcciones VIP se trasladan a la interfaz disponible que tenga la mayor prioridad. Si esa interfaz falla, las direcciones VIP se trasladan a la siguiente interfaz disponible con mayor prioridad, y así sucesivamente.

Pasos

1. Arrastra las filas de 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 salvo que se produzca un fallo.

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 de HA proporciona acceso al Grid Manager, debes seleccionar una interfaz en el nodo de administración primario para que sea la interfaz primaria. Algunos procedimientos de mantenimiento solo se pueden realizar desde el nodo de administración primario.

2. Selecciona **Continuar**.

Introduce direcciones IP

Pasos

1. En el campo **CIDR de la subred**, especifica 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 activado. Por ejemplo, 192.16.0.0/22.



Si utilizas 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](#)

2. Si lo deseas, en caso de que algún cliente administrativo o de inquilino de S3 vaya a acceder a estas direcciones VIP desde una subred diferente, introduce la **dirección IP de la puerta de enlace**. La dirección de la puerta de enlace debe estar dentro de la subred VIP.

Los usuarios de cliente y de administración usarán esta gateway para acceder a las direcciones IP virtuales.

3. Introduce al menos una y no más de diez direcciones VIP para la interfaz activa del grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP y todas estarán activas al mismo tiempo en la interfaz activa.

Debes proporcionar al menos una dirección IPv4. Si lo deseas, puedes especificar direcciones IPv4 e IPv6

adicionales.

4. Selecciona **Crear grupo de alta disponibilidad** y selecciona **Finalizar**.

Se ha creado el grupo HA y ya puedes utilizar las direcciones IP virtuales configuradas.

Próximos pasos

Si vas a utilizar este grupo de alta disponibilidad (HA) para el equilibrio de carga, crea un punto de conexión del equilibrador de carga para determinar el puerto y el protocolo de red y para asociar los certificados necesarios. Consulta ["Configura los puntos de conexión del equilibrador de carga"](#).

Editar un grupo de alta disponibilidad

Puedes editar un grupo de alta disponibilidad (HA) para cambiar su nombre y descripción, añadir o eliminar interfaces, cambiar el orden de prioridad o añadir o actualizar direcciones IP virtuales.

Por ejemplo, es posible que tengas que editar un grupo de alta disponibilidad (HA) si quieres eliminar el nodo asociado con una interfaz seleccionada en un procedimiento de decomisionar un sitio o nombre de nodo.

Pasos

1. Selecciona **Configuración > Red > Grupos de alta disponibilidad**.

La página «Grupos de alta disponibilidad» muestra todos los grupos de alta disponibilidad existentes.

2. Marca la casilla correspondiente al grupo de alta disponibilidad que quieras editar.
3. Haz una de las siguientes cosas, según lo que quieras actualizar:
 - Selecciona **Acciones > Editar dirección IP virtual** para añadir o eliminar direcciones VIP.
 - Selecciona **Acciones > Editar grupo de alta disponibilidad** para actualizar el nombre o la descripción del grupo, añadir o eliminar interfaces, cambiar el orden de prioridad o añadir o eliminar direcciones VIP.
4. Si has seleccionado **Editar dirección IP virtual**:
 - a. Actualiza las direcciones IP virtuales del grupo de alta disponibilidad.
 - b. Selecciona **Guardar**.
 - c. Selecciona **Finalizar**.
5. Si has seleccionado **Editar grupo de alta disponibilidad**:
 - a. Opcionalmente, actualiza el nombre o la descripción del grupo.
 - b. Si lo deseas, selecciona o desmarca las casillas para añadir o eliminar interfaces.



Si el grupo HA proporciona acceso al Grid Manager, debes seleccionar una interfaz en el nodo de administración principal para que sea la interfaz principal. Algunos procedimientos de mantenimiento solo pueden realizarse desde el nodo de administración principal.

- c. Si lo deseas, arrastra las filas para cambiar el orden de prioridad de la interfaz principal y de cualquier interfaz de respaldo de este grupo de alta disponibilidad.
- d. Opcionalmente, actualiza las direcciones IP virtuales.
- e. Selecciona **Guardar** y luego selecciona **Finalizar**.

Eliminar un grupo de alta disponibilidad

Puedes eliminar uno o varios grupos de alta disponibilidad (HA) a la vez.



No puedes eliminar un grupo de alta disponibilidad si está vinculado a un punto final del equilibrador de carga. Para eliminar un grupo de alta disponibilidad, debes quitarlo de cualquier punto final del equilibrador de carga que lo use.

Para evitar interrupciones en los clientes, actualiza las aplicaciones cliente de S3 afectadas antes de eliminar un grupo de HA. Actualiza cada cliente para que se conecte usando otra dirección IP; por ejemplo, la dirección IP virtual de un grupo de HA diferente o la dirección IP configurada para una interfaz durante la instalación.

Pasos

1. Selecciona **Configuración > Red > Grupos de alta disponibilidad**.
2. Revisa la columna **Puntos de conexión del equilibrador de carga** de cada grupo de alta disponibilidad que quieras eliminar. Si aparece algún punto de conexión del equilibrador de carga:
 - a. Ve a **Configuración > Red > Puntos finales del equilibrador de carga**.
 - b. Marca la casilla correspondiente al endpoint.
 - c. Selecciona **Actions > Edit endpoint binding mode**.
 - d. Actualiza el modo de enlace para eliminar el grupo de HA.
 - e. Selecciona **Guardar cambios**.
3. Si no aparece ningún punto de conexión del equilibrador de carga, marca la casilla correspondiente a cada grupo de alta disponibilidad que quieras eliminar.
4. Selecciona **Acciones > Eliminar grupo de alta disponibilidad**.
5. Revisa el mensaje y selecciona **Eliminar grupo de HA** para confirmar tu elección.

Se han eliminado todos los grupos de alta disponibilidad que has seleccionado. Aparece un banner verde de éxito en la página de grupos de alta disponibilidad.

Gestiona el equilibrio de carga

Conoce el equilibrio de carga de StorageGRID

Puedes utilizar el equilibrio de carga para gestionar las cargas de trabajo de ingesta y recuperación de los 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 gestionar 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 varios Storage Nodes.

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 Transport Layer Security (TLS) de las solicitudes de los clientes, inspecciona las solicitudes y establece nuevas conexiones seguras con los nodos de almacenamiento.

El servicio de equilibrio de carga de cada nodo funciona de forma independiente a la hora de reenviar el tráfico de los clientes a los nodos de almacenamiento. Mediante un proceso de ponderación, el servicio de equilibrio

de carga dirige más solicitudes hacia los nodos de almacenamiento con mayor disponibilidad de CPU.



Aunque el servicio StorageGRID Load Balancer es el mecanismo de equilibrio de carga recomendado, es posible que quieras integrar un equilibrador de carga de terceros en su lugar. Para obtener más información, contacta a tu representante de cuenta de NetApp o consulta ["Usa balanceadores de carga de terceros con StorageGRID"](#).

¿Cuántos nodos de equilibrio de carga necesito?

Como práctica recomendada general, cada sitio de tu sistema StorageGRID debería incluir dos o más nodos con el servicio Load Balancer. Por ejemplo, un sitio puede incluir dos Gateway Nodes o tanto un Admin Node como un Gateway Node. Asegúrate de que haya una infraestructura de red, hardware o virtualización adecuada para cada nodo de equilibrio de carga, ya sea que uses servicios appliances, nodos bare metal o nodos basados en máquinas virtuales (VM).

¿Qué es un endpoint de un equilibrador de carga?

Un punto final del equilibrador de carga define el puerto y el protocolo de red (HTTPS o HTTP) que utilizarán las solicitudes entrantes y salientes de las aplicaciones cliente para acceder a los nodos que contienen el servicio Load Balancer. 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 endpoint de equilibrador de carga, usa el Grid Manager o completa los asistentes de configuración de S3 y FabricPool:

- ["Configura los puntos de conexión del equilibrador de carga"](#)
- ["Utiliza el asistente de configuración de S3"](#)
- ["Usa el asistente de configuración de FabricPool"](#)

Aspectos a tener en cuenta para el almacenamiento en caché del equilibrador de carga

El almacenamiento en caché mejora considerablemente el rendimiento cuando una carga de trabajo opera sobre un subconjunto de datos y accede a los objetos varias veces. Además, el almacenamiento en caché permite el acceso remoto al almacenamiento de objetos sin una implementación completa del grid. El almacenamiento en caché del balanceador de carga solo está disponible para Gateway Nodes.

Al crear puntos de conexión del equilibrador de carga:

- Activa el almacenamiento en caché únicamente para las cargas de trabajo almacenables en caché. Las cargas de trabajo que acceden a datos no almacenados en caché con más frecuencia que a los datos almacenados en caché tendrán un rendimiento inferior al que tendrían si no se hubieran gestionado mediante la caché. En algunos casos, las cargas de trabajo con altas tasas de sobrescritura y expulsión también podrían superar la resistencia garantizada de la unidad a la escritura.
- Considera añadir puntos finales o nodos adicionales para almacenar en caché cargas de trabajo individuales que sean buenas candidatas para el almacenamiento en caché.
- Utiliza puntos finales distintos para las cargas de trabajo almacenables en caché y las que no lo son. Esta separación garantiza que los mecanismos de almacenamiento en caché se apliquen correctamente y no interfieran en el procesamiento de datos que no son almacenables en caché.
- Evalúa una carga de trabajo almacenable en caché dirigiéndola al endpoint habilitado para caché. Supervisa y verifica la tasa de aciertos en caché para determinar la idoneidad de la carga de trabajo para el almacenamiento en caché. Esta evaluación ayuda a optimizar el rendimiento y a asegurar un uso eficiente de los recursos de caché.

- ["Revisar los registros de auditoría"](#) para determinar si una carga de trabajo existente sería una buena candidata para el almacenamiento en caché. Para un periodo de tiempo determinado, determina qué porcentaje de solicitudes GET corresponden a objetos únicos. Para que sea adecuado para el almacenamiento en caché, este valor debería ser inferior al 50%.

Ejemplos de cargas de trabajo que podrían ser buenas candidatas para el almacenamiento en caché

- Lagos de datos
- Cálculo de alto rendimiento (HPC)
- Entrenamiento de IA/ML
- Redes de distribución de contenidos (CDN)
- Gestión de activos multimedia
- Producción de vídeos



- Se pueden almacenar en caché varias versiones de un objeto.
- Se admiten operaciones de lectura de rango.

Ejemplos de cargas de trabajo que no son buenas candidatas para el almacenamiento en caché

- FabricPool
- Aplicaciones de backup
- Niveles de almacenamiento



Si algún contenido que vaya a servirse desde la caché requiere cifrado en reposo, ["activar el cifrado de nodos o unidades"](#) en el nodo de la caché.

Tipos de objetos y solicitudes que no se almacenarán en la caché

- El `response-content-encoding` parámetro de consulta
- El parámetro de consulta `partNumber`
- Encabezados condicionales
 - `If-Match`
 - `If-Modified-Since`
 - `If-None-Match`
 - `If-Unmodified-Since`
- Solicitudes que se cifraron en reposo con cualquiera de los siguientes:
 - SSE (cifrado del lado del servidor con claves gestionadas por StorageGRID)
 - SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente)
 - Cifrado de objetos almacenados

Las solicitudes que no estén almacenadas en la caché se reenvían a un LDR de nivel superior como si la caché no estuviera activada.

Información relacionada

- ["Soluciona problemas relacionados con el almacenamiento en caché del equilibrador de carga"](#)
- Para obtener más información sobre el almacenamiento en caché del equilibrador de carga, ponte en contacto con soporte técnico.

Consideraciones para el puerto

El puerto para un punto final del equilibrador de carga es 10433 de forma predeterminada para el primer punto final que crees, pero puedes especificar cualquier puerto externo no utilizado entre 1 y 65535. Si usas el puerto 80 o 443, el punto final usará el servicio de Load Balancer solo en los Gateway Nodes. Estos puertos están reservados en los Admin Nodes. Si usas el mismo puerto para más de un punto final, debes especificar un modo de enlace diferente para cada punto final.

No se permiten los puertos utilizados por otros servicios de grid. Consulta ["Puertos internos de StorageGRID"](#).

Consideraciones para el protocolo de red

En la mayoría de los casos, las conexiones entre las aplicaciones cliente y StorageGRID deben utilizar el cifrado TLS (Transport Layer Security). Conectarse a StorageGRID sin cifrado TLS es compatible pero no se recomienda, especialmente en entornos de producción. Cuando selecciones el protocolo de red para el punto final del equilibrador de carga de StorageGRID, debes seleccionar **HTTPS**.

Consideraciones sobre los certificados de los puntos finales del equilibrador de carga

Si seleccionas **HTTPS** como protocolo de red para el punto final del equilibrador de carga, debes proporcionar un certificado de seguridad. Puedes utilizar cualquiera de estas tres opciones al crear el punto final del equilibrador de carga:

- **Sube un certificado firmado (recomendado).** Este certificado puede estar firmado por una autoridad de certificación (CA) de confianza pública o privada. La mejor práctica es usar un certificado de servidor de una CA de confianza pública para asegurar la conexión. A diferencia de los certificados generados, los certificados firmados por una CA pueden rotarse sin interrupciones, lo que puede ayudar a evitar problemas de caducidad.

Debes obtener los siguientes archivos antes de crear el punto de conexión del equilibrador de carga:

- El archivo del certificado del servidor personalizado.
- El archivo de la 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.**
- **Utiliza el certificado global de StorageGRID S3.** Debes cargar o generar una versión personalizada de este certificado antes de poder seleccionarlo para el punto final del equilibrador de carga. Consulta ["Configura los certificados de la API de S3"](#).

¿Qué valores necesito?

Para crear el certificado, debes conocer todos los nombres de dominio y direcciones IP que utilizarán las aplicaciones cliente de S3 para acceder al endpoint.

La entrada **DN del sujeto** (nombre distintivo) del certificado debe incluir el nombre de dominio completo que utilizará la aplicación cliente para StorageGRID. Por ejemplo:

```
Subject DN:
/C=Country/ST=State/O=Company, Inc./CN=s3.storagegrid.example.com
```

Según sea necesario, el certificado puede utilizar comodines para representar los nombres de dominio completos de todos los nodos de administración y nodos de puerta de enlace que ejecutan el servicio de Load Balancer. Por ejemplo, `*.storagegrid.example.com` utiliza el comodín `*` para representar `adm1.storagegrid.example.com` y `gn1.storagegrid.example.com`.

Si tienes pensado utilizar solicitudes de estilo virtual hosted de S3, el certificado también debe incluir una entrada de **nombre alternativo** para cada "[Nombre de dominio del endpoint S3](#)" que hayas configurado, incluidos los nombres de comodín. Por ejemplo:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```



Si usas comodines para nombres de dominio, revisa "[Directrices de refuerzo de la seguridad para certificados de servidor](#)".

También debes definir una entrada DNS para cada nombre que figure en el certificado de seguridad.

¿Cómo gestiono los certificados que están a punto de caducar?



Si caduca el certificado utilizado para proteger la conexión entre la aplicación S3 y StorageGRID, es posible que la aplicación pierda temporalmente el acceso a StorageGRID.

Para evitar problemas relacionados con la caducidad de los certificados, sigue estas recomendaciones:

- Presta especial atención a cualquier alerta que avise de la proximidad de la fecha de caducidad de un certificado, como las alertas **Caducidad del certificado del punto final del equilibrador de carga** y **Caducidad del certificado global del servidor para la API de S3**.
- Mantén siempre sincronizadas las versiones del certificado de StorageGRID y de la aplicación S3. Si sustituyes o renuevas el certificado utilizado para un punto final del equilibrador de carga, debes sustituir o renovar el certificado equivalente utilizado por la aplicación S3.
- Utiliza un certificado de CA firmado públicamente. Si utilizas un certificado firmado por una CA, puedes reemplazar los certificados que estén a punto de caducar sin interrumpir el servicio.
- Si has generado un certificado autofirmado de StorageGRID y dicho certificado está a punto de caducar, debes sustituirlo manualmente tanto en StorageGRID como en la aplicación S3 antes de que caduque el certificado actual.

Aspectos a tener en cuenta respecto al modo de binding

El modo de vinculación te permite controlar qué direcciones IP se pueden usar para acceder a un endpoint del equilibrador de carga. Si un endpoint utiliza un modo de vinculación, las aplicaciones cliente solo pueden acceder al endpoint si usan una dirección IP permitida o su dominio completo (FQDN) correspondiente. Las aplicaciones cliente que usen cualquier otra dirección IP o FQDN no pueden acceder al endpoint.

Puedes especificar cualquiera de los siguientes modos de enlace:

- **Global** (predeterminado): Las aplicaciones cliente pueden acceder al endpoint utilizando la dirección IP de

cualquier Gateway Node o Admin Node, la dirección IP virtual (VIP) de cualquier HA group en cualquier red, o el FQDN correspondiente. Usa esta configuración a menos que necesites restringir la accesibilidad de un endpoint.

- **Direcciones IP virtuales de los grupos de alta disponibilidad.** Las aplicaciones cliente deben utilizar una dirección IP virtual (o el nombre de dominio completo correspondiente) de un grupo de alta disponibilidad.
- **Interfaces de nodo.** Los clientes deben utilizar las direcciones IP (o los dominios completos correspondientes) de las interfaces de nodo seleccionadas.
- **Tipo de nodo.** En función del tipo de nodo que selecciones, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier Admin Node o la dirección IP (o el FQDN correspondiente) de cualquier Gateway Node.

Consideraciones para el acceso de los inquilinos

El acceso de los inquilinos es una función de seguridad opcional que te permite controlar qué cuentas de inquilinos de StorageGRID pueden utilizar un punto de conexión del equilibrador de carga para acceder a sus buckets. Puedes permitir que todos los inquilinos accedan a un punto de conexión (por defecto) o especificar una lista de los inquilinos permitidos o bloqueados para cada punto de conexión.

Puedes usar esta función para proporcionar un mejor aislamiento de seguridad entre los inquilinos y sus endpoints. Por ejemplo, podrías usar esta función para asegurarte de que los materiales top-secret o altamente clasificados que pertenecen a un inquilino sigan siendo completamente inaccesibles para los demás inquilinos.



A 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 ocurre con el acceso anónimo), se utiliza al propietario del bucket para determinar el inquilino.

Ejemplo de acceso de inquilinos

Para comprender cómo funciona esta función de seguridad, fíjate en el siguiente ejemplo:

1. Has creado dos puntos de conexión del equilibrador de carga, como sigue:
 - Punto de conexión **público**: utiliza el puerto 10443 y permite el acceso a todos los inquilinos.
 - Punto final **Top secret**: utiliza el puerto 10444 y solo permite el acceso al inquilino **Top secret**. Todos los demás inquilinos tienen bloqueado el acceso a este punto final.
2. El `top-secret.pdf` está en un bucket propiedad del inquilino **Top secret**.

Para acceder a `top-secret.pdf`, un usuario del tenant **Top secret** puede enviar una solicitud GET a `https://w.x.y.z:10444/top-secret.pdf`. Dado que este tenant tiene permiso para utilizar el endpoint 10444, el usuario puede acceder al objeto. Sin embargo, si un usuario perteneciente a cualquier otro tenant envía la misma solicitud a la misma URL, recibe inmediatamente un mensaje de Acceso denegado. Se deniega el acceso incluso si las credenciales y la firma son válidas.

Disponibilidad de la CPU

El servicio Load Balancer en cada nodo de administración y nodo de puerta de enlace funciona de forma independiente al reenviar el 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 más frecuencia. A todos los nodos de almacenamiento se les asigna un valor de peso base mínimo, incluso si un nodo informa de un 100 % de utilización o no informa de su utilización.

En algunos casos, la información sobre la disponibilidad de la CPU se limita al sitio donde se encuentra el servicio de Load Balancer.

Configura los puntos finales del equilibrador de carga StorageGRID

Los puntos de conexión del equilibrador de carga determinan los puertos y los protocolos de red que pueden utilizar los clientes de S3 al conectarse al equilibrador de carga de StorageGRID en los nodos Gateway y Admin. También puedes utilizar los puntos de conexión para acceder a Grid Manager, Tenant Manager o a ambos.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).
- Has revisado la ["consideraciones para el equilibrio de carga"](#).
- Si anteriormente has reasignado un puerto que pretendes utilizar para el punto final del equilibrador de carga, tienes ["se eliminó la reasignación de puertos"](#).
- Ya has creado los grupos de alta disponibilidad (HA) que planeas usar. Se recomiendan los grupos de alta disponibilidad, pero no son obligatorios. Consulta ["Gestiona grupos de alta disponibilidad"](#).
- Si el endpoint del equilibrador de carga lo va a utilizar ["Arrendatarios de S3 para S3 Select"](#), no debe usar las direcciones IP ni los FQDN de ningún nodo bare-metal. Solo se admiten dispositivos de servicios y nodos de software basados en VMware para los endpoints del equilibrador de carga que se utilicen para S3 Select.
- Ya has configurado todas las interfaces VLAN que planeas usar. Consulta ["Configurar interfaces VLAN"](#).
- Si vas a crear un endpoint HTTPS (recomendado), tienes la información para el certificado del servidor.



Los cambios en el certificado de un endpoint pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

- Para cargar un certificado, necesitas el certificado del servidor, la clave privada del certificado y, opcionalmente, un paquete de CA.
- Para generar un certificado, necesitas todos los nombres de dominio y direcciones IP que los clientes de S3 usarán para acceder al endpoint. También debes conocer el sujeto (Distinguished Name).
- Si deseas utilizar el certificado de la API S3 de StorageGRID (que también se puede utilizar para conexiones directas a Storage Nodes), ya has reemplazado el certificado predeterminado por un certificado personalizado firmado por una autoridad de certificación externa. Consulta ["Configura los certificados de la API de S3"](#).

Crear un punto de conexión del equilibrador de carga

Cada punto de conexión del equilibrador de carga de clientes S3 especifica un puerto, un tipo de cliente (S3) y un protocolo de red (HTTP o HTTPS). Los puntos de conexión del equilibrador de carga de la interfaz de gestión especifican un puerto, un tipo de interfaz y una Client Network no fiable.

Accede al asistente

Pasos

1. Selecciona **Configuración > Red > Puntos finales del equilibrador de carga**.
2. Para crear un endpoint para un cliente S3, selecciona la pestaña **S3 client**.
3. Para crear un punto de acceso a Grid Manager, Tenant Manager o ambos, selecciona la pestaña **Interfaz de gestión**.
4. Selecciona **Crear**.

Introduce los datos del punto final

Pasos

1. Selecciona las instrucciones adecuadas para introducir los datos correspondientes al tipo de endpoint que deseas crear.

Cliente S3

Campo	Descripción
Nombre	Un nombre descriptivo para el endpoint, que aparecerá en la tabla de la página de endpoints del load balancer.
Puerto	El puerto de StorageGRID que quieres usar para el equilibrio de carga. Este campo tiene por defecto el valor 10433 para el primer endpoint que crees, pero puedes ingresar cualquier puerto externo sin usar entre 1 y 65535. Si introduces 80 o 8443, el endpoint solo se configura en los nodos de Gateway, a menos que hayas liberado el puerto 8443. Entonces puedes usar el puerto 8443 como endpoint S3, y el puerto se configurará tanto en los nodos de Gateway como en los nodos de Admin.
Tipo de cliente	Debe ser S3 .
Protocolo de red	El protocolo de red que utilizarán los clientes al conectarse a este endpoint. • Selecciona HTTPS para una comunicación segura y cifrada mediante TLS (recomendado). Debes adjuntar un certificado de seguridad antes de poder guardar el endpoint. • Selecciona HTTP para una comunicación menos segura y sin cifrar. Utiliza HTTP únicamente para una red que no sea de producción.
Habilitar el almacenamiento en caché	Activa o desactiva "almacenamiento en caché en los nodos de pasarela" para este endpoint del balanceador de carga. Si surgen problemas con el almacenamiento en caché, consulta "Soluciona problemas relacionados con el almacenamiento en caché del equilibrador de carga".

Interfaz de gestión

Campo	Descripción
Nombre	Un nombre descriptivo para el endpoint, que aparecerá en la tabla de la página de endpoints del load balancer.
Puerto	El puerto de StorageGRID que deseas utilizar para acceder al Grid Manager, al Tenant Manager o a ambos. • Grid Manager: 8443 • Tenant Manager: 9443 • Tanto Grid Manager como Tenant Manager: 443 Nota: Puedes utilizar estos puertos predefinidos u otros puertos disponibles.

Campo	Descripción
Tipo de interfaz	Selecciona el botón de opción correspondiente a la interfaz de StorageGRID a la que vas a acceder mediante este endpoint.
Red de clientes no fiables	Selecciona Sí si este endpoint debe estar accesible para redes de clientes no confiables. De lo contrario, selecciona No. Cuando seleccionas Sí, el puerto está abierto en todas las redes de clientes no confiables. Nota: Solo puedes configurar un puerto para que esté abierto o cerrado a redes de clientes no fiables al crear el punto de conexión del equilibrador de carga.

1. Selecciona **Continuar**.

Selecciona un modo de encuadernación

Pasos

1. Selecciona un modo de enlace para el punto final para controlar cómo se accede a él usando cualquier dirección IP o usando direcciones IP e interfaces de red específicas.

Algunos modos de enlace están disponibles tanto para los puntos finales de cliente como para los de la interfaz de gestión. Aquí se enumeran todos los modos para ambos tipos de puntos finales.

Modo	Descripción
Global (valor predeterminado para los puntos finales de cliente)	Los clientes pueden acceder al punto final usando la dirección IP de cualquier Gateway Node o Admin Node, la dirección IP virtual (VIP) de cualquier grupo HA en cualquier red, o el FQDN correspondiente. Utiliza la configuración Global a menos que necesites restringir la accesibilidad de este endpoint.
Direcciones IP virtuales de los grupos de alta disponibilidad	Los clientes deben utilizar una dirección IP virtual (o el nombre de dominio completo correspondiente) de un grupo de alta disponibilidad para acceder a este endpoint. Todos los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que selecciones para los puntos finales no se solapen.
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o los FQDN correspondientes) de las interfaces de los nodos seleccionados para acceder a este endpoint.
Tipo de nodo (solo puntos finales de cliente)	En función del tipo de nodo que selecciones, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier Admin Node o la dirección IP (o el FQDN correspondiente) de cualquier Gateway Node para acceder a este endpoint.

Modo	Descripción
Todos los nodos de administración (valor predeterminado para los endpoints de la interfaz de gestión)	Los clientes deben utilizar la dirección IP (o el nombre de dominio completo correspondiente) de cualquier Admin Node para acceder a este endpoint.

Si hay más de un endpoint que utiliza el mismo puerto, StorageGRID usa este orden de prioridad para decidir qué endpoint usar: **Virtual IPs of HA groups** > **Node interfaces** > **Node type** > **Global**.

Si vas a crear puntos finales de la interfaz de gestión, solo se permiten los nodos de administración.

2. Si has seleccionado **Virtual IPs of HA groups**, selecciona uno o varios HA groups.

Si estás creando puntos finales de la interfaz de gestión, selecciona las VIP asociadas únicamente con los Admin Nodes.

3. Si seleccionaste **Node interfaces**, selecciona una o más interfaces de nodo para cada Admin Node o Gateway Node que quieras asociar con este endpoint.
4. Si seleccionaste **Tipo de nodo**, elige entre Admin Nodes, que incluye tanto el Admin Node principal como cualquier Admin Node no principal, o Gateway Nodes.

Controlar el acceso de los inquilinos



Un punto final de la interfaz de gestión solo puede controlar el acceso de los inquilinos cuando el punto final tiene el [Tipo de interfaz de Tenant Manager](#).

Pasos

1. Para el paso **Acceso del inquilino**, selecciona una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (por defecto)	Todas las cuentas de inquilinos pueden usar este endpoint para acceder a sus buckets. Debes seleccionar esta opción si aún no has creado ninguna cuenta de inquilino. Una vez que hayas añadido cuentas de inquilino, puedes editar el endpoint del balanceador de carga para permitir o bloquear cuentas específicas.
Permitir inquilinos seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este endpoint para acceder a sus buckets.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este endpoint para acceder a sus buckets. El resto de inquilinos sí pueden utilizar este endpoint.

2. Si estás creando un punto final **HTTP**, no necesitas adjuntar un certificado. Selecciona **Crear** para añadir el nuevo punto final del equilibrador de carga. Luego, ve a [Después de que termines](#). De lo contrario, selecciona **Continuar** para adjuntar el certificado.

Adjuntar certificado

Pasos

1. Si vas a crear un punto final **HTTPS**, selecciona el tipo de certificado de seguridad que deseas asociar al punto final.

El certificado protege las conexiones entre los clientes S3 y el servicio Load Balancer en el nodo de administración o en los nodos Gateway.

- **Cargar certificado.** Selecciona esta opción si tienes certificados personalizados para cargar.
- **Generar certificado.** Selecciona esta opción si tienes los valores necesarios para generar un certificado personalizado.
- **Utilizar el certificado S3 de StorageGRID.** Selecciona esta opción si deseas utilizar el certificado global de la API de S3, que también puede usarse para conexiones directas a Storage Nodes.

No puedes seleccionar esta opción a menos que hayas sustituido el certificado predeterminado de la API de S3, que está firmado por la CA de la red, por un certificado personalizado firmado por una autoridad de certificación externa. Consulta ["Configura los certificados de la API de S3"](#).

- **Usar el certificado de la interfaz de gestión.** Selecciona esta opción si quieres usar el certificado de la interfaz de gestión global, que también se puede usar para conexiones directas a Admin Nodes.
2. Si no estás utilizando el certificado S3 de StorageGRID, sube o genera el certificado.

Subir certificado

- a. Selecciona **Cargar certificado**.
- b. Sube los archivos de certificados del servidor necesarios:
 - **Certificado del servidor**: el archivo del certificado personalizado del servidor en codificación PEM.
 - **Clave privada del certificado**: El archivo de la clave privada del certificado del servidor personalizado (`.key`).



Las claves privadas EC deben ser de 224 bits o más. Las claves privadas RSA deben ser de 2048 bits o más.

- **Paquete de 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 certificados de CA codificados en formato PEM, concatenados en el orden de la cadena de certificados.
- c. Despliega **Detalles del certificado** para ver los metadatos de cada certificado que subiste. Si subiste un paquete de CA opcional, cada certificado se muestra en su propia pestaña.
 - Selecciona **Descargar certificado** para guardar el archivo del certificado o selecciona **Descargar paquete de CA** para guardar el paquete de certificados.

Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Selecciona **Copiar certificado PEM** o **Copiar paquete de CA PEM** para copiar el contenido del certificado y pegarlo en otro lugar.
- d. Selecciona **Crear**. + Se crea el extremo del equilibrador de carga. El certificado personalizado se utiliza para todas las nuevas conexiones posteriores entre los clientes de S3 o la interfaz de gestión y el extremo.

Generar certificado

- a. Selecciona **Generar certificado**.
- b. Indica la información del certificado:

Campo	Descripción
Nombre de dominio	Uno o más dominios completos para incluir en el certificado. Usa un <code>*</code> como comodín para representar varios nombres de dominio.
IP	Una o varias direcciones IP para incluir en el certificado.

Campo	Descripción
Asunto (opcional)	Nombre del sujeto X.509 o nombre distintivo (DN) del titular del certificado. Si no se introduce ningún valor en este campo, el certificado generado utiliza el primer nombre de dominio o la primera dirección IP como nombre común (CN) del sujeto.
Días de validez	Número de días después de la creación en los que caduca el certificado.
Agregar extensiones de uso de clave	Si seleccionas esta opción (predeterminada y recomendada), se añaden al certificado generado las extensiones de uso de clave y uso ampliado de clave. Estas extensiones definen la finalidad de la clave incluida en el certificado. Nota: Deja esta casilla marcada a menos que tengas problemas de conexión con clientes antiguos cuando los certificados incluyan estas extensiones.

c. Selecciona **Generar**.

d. Selecciona **Detalles del certificado** para ver los metadatos del certificado generado.

- Selecciona **Descargar certificado** para guardar el archivo del certificado.

Especifica el nombre del archivo del certificado y la ubicación de descarga. Guarda el archivo con la extensión `.pem`.

Por ejemplo: `storagegrid_certificate.pem`

- Selecciona **Copiar certificado PEM** para copiar el contenido del certificado y pegarlo en otro lugar.

e. Selecciona **Crear**.

Se ha creado el extremo del equilibrador de carga. El certificado personalizado se utiliza para todas las nuevas conexiones posteriores entre los clientes de S3 o la interfaz de gestión y este extremo.

Después de que termines

Pasos

1. Si utilizas un servidor DNS, asegúrate de que el DNS incluya un registro que asocie el nombre de dominio completo (FQDN) de StorageGRID a cada dirección IP que los clientes usarán para hacer conexiones.

La dirección IP que introduzcas en el registro DNS depende de si estás utilizando un grupo de alta disponibilidad (HA) de nodos con equilibrio de carga:

- Si has configurado un grupo de alta disponibilidad, los clientes se conectarán a las direcciones IP virtuales de ese grupo.
- Si no utilizas un grupo de alta disponibilidad (HA), los clientes se conectarán al servicio StorageGRID Load Balancer usando la dirección IP de un Gateway Node o Admin Node.

También debes asegurarte de que el registro DNS haga referencia a todos los nombres de dominio de endpoint necesarios, incluidos los nombres con comodín.

2. Proporciona a los clientes de S3 la información necesaria para conectarse al endpoint:

- Número de puerto
- Nombre de dominio completo o dirección IP
- Cualquier detalle de certificado requerido

Ver y editar los puntos de conexión del equilibrador de carga

Puedes ver los detalles de los puntos de conexión del equilibrador de carga existentes, incluidos los metadatos del certificado de un punto de conexión seguro. Puedes cambiar ciertos ajustes de un punto de conexión.

- Para consultar la información básica de todos los endpoints del equilibrador de carga, revisa las tablas en la página de endpoints del equilibrador de carga.
- Para ver todos los detalles sobre un endpoint concreto, incluidos los metadatos del certificado, selecciona el nombre del endpoint en la tabla. La información que se muestra varía en función del tipo de endpoint y de 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, utiliza el menú **Acciones** en la página de puntos finales del equilibrador de carga.



Si pierdes el acceso a Grid Manager mientras editas el puerto de un endpoint de una interfaz de gestión, actualiza la URL y el puerto para recuperar el acceso.



Tras editar un punto final, es posible que tengas que 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. Marca la casilla correspondiente al endpoint. b. Selecciona Acciones > Editar nombre del punto final . c. Introduce el nuevo nombre. d. Selecciona Guardar .	a. Selecciona el nombre del endpoint para ver los detalles. b. Selecciona el icono de edición  . c. Introduce el nuevo nombre. d. Selecciona Guardar .
Editar el puerto del endpoint	a. Marca la casilla correspondiente al endpoint. b. Selecciona Actions > Edit endpoint port . c. Introduce un número de puerto válido. d. Selecciona Guardar .	n/a
Editar el modo de enlace del punto final	a. Marca la casilla correspondiente al endpoint. b. Selecciona Actions > Edit endpoint binding mode . c. Actualiza el modo de enlace según sea necesario. d. Selecciona Guardar cambios .	a. Selecciona el nombre del endpoint para ver los detalles. b. Selecciona Editar modo de enlace . c. Actualiza el modo de enlace según sea necesario. d. Selecciona Guardar cambios .
Editar el certificado del endpoint	a. Marca la casilla correspondiente al endpoint. b. Selecciona Actions > Edit endpoint certificate . c. Sube o genera un nuevo certificado personalizado o empieza a utilizar el certificado global de S3, según sea necesario. d. Selecciona Guardar cambios .	a. Selecciona el nombre del endpoint para ver los detalles. b. Selecciona la pestaña Certificate . c. Selecciona Editar certificado . d. Sube o genera un nuevo certificado personalizado o empieza a utilizar el certificado global de S3, según sea necesario. e. Selecciona Guardar cambios .

Tarea	Menú de acciones	Página de detalles
Editar el acceso del inquilino	a. Marca la casilla correspondiente al endpoint. b. Selecciona Acciones > Editar acceso del inquilino . c. Elige otra opción de acceso, selecciona o elimina inquilinos de la lista o haz ambas cosas. d. Selecciona Guardar cambios .	a. Selecciona el nombre del endpoint para ver los detalles. b. Selecciona la pestaña Tenant access . c. Selecciona Editar acceso de inquilino . d. Elige otra opción de acceso, selecciona o elimina inquilinos de la lista o haz ambas cosas. e. Selecciona Guardar cambios .

Eliminar puntos de conexión del equilibrador de carga

Puedes eliminar uno o varios puntos finales mediante el menú **Actions**, o bien eliminar un único punto final desde la página de detalles.



Para evitar interrupciones en los clientes, actualiza cualquier aplicación cliente de S3 afectada antes de eliminar un endpoint del equilibrador de carga. Actualiza cada cliente para que se conecte usando un puerto asignado a otro endpoint del equilibrador de carga. Asegúrate también de actualizar cualquier información necesaria sobre certificados.



Si pierdes el acceso a Grid Manager al eliminar un punto final de la interfaz de gestión, actualiza la URL.

- Para eliminar uno o varios puntos finales:
 - En la página Load balancer, marca la casilla correspondiente a cada endpoint que quieras eliminar.
 - Selecciona **Acciones > Eliminar**.
 - Selecciona **Aceptar**.
- Para eliminar un endpoint de la página de detalles:
 - En la página «Load balancer», selecciona el nombre del endpoint.
 - Selecciona **Eliminar** en la página de detalles.
 - Selecciona **Aceptar**.

Configura los nombres de dominio del endpoint S3 en StorageGRID

Para admitir las solicitudes de S3 con alojamiento virtual, debes usar Grid Manager para configurar la lista de nombres de dominio de los endpoints de S3 a los que se conectan los clientes de S3.



No se admite el uso de una dirección IP como nombre de dominio de un endpoint. Las próximas versiones impedirán esta configuración.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes "permisos de acceso específicos".
- Has confirmado que no hay ninguna actualización de grid en curso.



No realices ningún cambio en la configuración del nombre de dominio mientras una actualización de la grid está en curso.

Acerca de esta tarea

Para que los clientes puedan utilizar nombres de dominio de endpoint S3, debes hacer todo lo siguiente:

- Utiliza el Grid Manager para añadir los nombres de dominio de los endpoints S3 al sistema StorageGRID.
- Asegúrate de que el "certificado que utiliza el cliente para las conexiones HTTPS con StorageGRID" esté firmado para todos los nombres de dominio que necesite el cliente.

Por ejemplo, si el endpoint es `s3.company.com`, debes asegurarte de que el certificado utilizado para las conexiones HTTPS incluya el endpoint `s3.company.com` y el nombre alternativo del sujeto (SAN) comodín de ese endpoint: `*.s3.company.com`.

- Configura el servidor DNS que utiliza el cliente. Incluye registros DNS para las direcciones IP que utilizan los clientes para establecer conexiones y asegúrate de que los registros hagan referencia a todos los nombres de dominio de los endpoints S3 necesarios, incluidos los nombres con comodines.



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. Debes entender cómo se conectan las aplicaciones cliente a la grid para que incluyas las direcciones IP correctas en los registros DNS.

Los clientes que utilicen conexiones HTTPS (recomendado) con la grid pueden utilizar cualquiera de estos certificados:

- Los clientes que se conectan a un endpoint de equilibrador de carga pueden usar un certificado personalizado para ese endpoint. Cada endpoint de equilibrador de carga se puede configurar para reconocer diferentes nombres de dominio de endpoint de S3.
- Los clientes que se conectan a un punto de conexión del balanceador de carga o directamente a un Storage Node pueden personalizar el certificado global de la API de S3 para incluir todos los nombres de dominio de los puntos de conexión de S3 necesarios.



Si no añades nombres de dominio de endpoint S3 y la lista está vacía, el soporte para solicitudes de S3 con estilo virtual-hosted estará desactivado.

Agrega un nombre de dominio de endpoint S3

Pasos

1. Selecciona **Configuración > Red > Nombres de dominio de endpoint S3**.
2. Introduce el nombre de dominio en el campo **Nombre de dominio 1**. Selecciona **Add another domain name** para añadir más nombres de dominio.
3. Selecciona **Guardar**.

4. Asegúrate de que los certificados del servidor que utilizan los clientes coincidan con los nombres de dominio de los endpoints de S3 requeridos.
 - Si los clientes se conectan a un punto de conexión del equilibrador de carga que utiliza su propio certificado, "[Actualiza el certificado asociado al endpoint](#)".
 - Si los clientes se conectan a un endpoint del equilibrador de carga que utiliza el certificado global de la API de S3 o directamente a los nodos de almacenamiento, "[Actualiza el certificado global de la API de S3](#)".
5. Agrega los registros DNS necesarios para garantizar que se puedan resolver las solicitudes de nombres de dominio de los endpoints.

Resultado

Ahora, cuando los clientes usan el endpoint `bucket.s3.company.com`, el servidor DNS resuelve al endpoint correcto y el certificado autentica el endpoint como se espera.

Cambiar el nombre de dominio del endpoint S3

Si cambias un nombre utilizado por las aplicaciones S3, las solicitudes de tipo virtual-hosted-style fallarán.

Pasos

1. Selecciona **Configuración > Red > Nombres de dominio de endpoint S3**.
2. Selecciona el campo del nombre de dominio que quieras editar y realiza los cambios necesarios.
3. Selecciona **Guardar**.
4. Selecciona **Sí** para confirmar tu cambio.

Eliminar un nombre de dominio de un endpoint S3

Si eliminas un nombre utilizado por las aplicaciones S3, las solicitudes de tipo virtual-hosted-style fallarán.

Pasos

1. Selecciona **Configuración > Red > Nombres de dominio de endpoint S3**.
2. Selecciona el icono de eliminación  junto al nombre de dominio.
3. Selecciona **Sí** para confirmar la eliminación.

Información relacionada

- "[Usa la API de REST de S3](#)"
- "[Ver direcciones IP](#)"
- "[Configurar grupos de alta disponibilidad](#)"

Direcciones IP y puertos para conexiones de cliente de StorageGRID

Para almacenar o recuperar objetos, las aplicaciones cliente de S3 se conectan al servicio Load Balancer, que está incluido en todos los Admin Nodes y Gateway Nodes, o al servicio Local Distribution Router (LDR), que está incluido en todos los Storage Nodes.

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, puedes crear grupos de alta disponibilidad (HA) de nodos de balanceo de carga para ofrecer conexiones altamente disponibles que usen direcciones IP virtuales (VIP). Si quieres conectarte a StorageGRID usando un dominio completo (FQDN) en vez de una

dirección IP o VIP, puedes 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 creaste puntos finales del equilibrador de carga y grupos de alta disponibilidad (HA), consulta [Dónde encontrar direcciones IP](#) para encontrar estos valores en Grid Manager.

Dónde se realiza la conexión	Servicio al que se conecta el cliente	Dirección IP	Puerto
Grupo HA	Equilibrador de carga	Dirección IP virtual de un grupo de alta disponibilidad	Puerto asignado al punto final del equilibrador de carga
Nodo de administración	Equilibrador de carga	Dirección IP del nodo de administración	Puerto asignado al punto final del equilibrador de carga
Nodo de puerta de enlace	Equilibrador de carga	Dirección IP del nodo de Gateway	Puerto asignado al punto final del equilibrador de carga
Nodo de almacenamiento	LDR	Dirección IP del nodo de almacenamiento	Puertos predeterminados de S3: • HTTPS: 18082 • HTTP: 18084

Ejemplos de URL

Para conectar una aplicación cliente al punto final del equilibrador de carga de un grupo de alta disponibilidad (HA) de Gateway Nodes, utiliza una URL con la estructura que se muestra a continuación:

`https://VIP-of-HA-group:LB-endpoint-port`

Por ejemplo, si la dirección IP virtual del grupo de alta disponibilidad es 192.0.2.5 y el número de puerto del punto final del equilibrador de carga es 10443, una aplicación podría utilizar la siguiente URL para conectarse a StorageGRID:

`https://192.0.2.5:10443`

Dónde encontrar direcciones IP

1. Inicia sesión en Grid Manager usando una ["navegador web compatible"](#) cuenta.
2. Para averiguar la dirección IP de un nodo de la red:
 - a. Selecciona **Nodos**.
 - b. Selecciona el nodo de administración, el nodo de puerta de enlace o el nodo de almacenamiento al que quieras conectarte.
 - c. Selecciona la pestaña **Vista general**.
 - d. En la sección Información del nodo, anota las direcciones IP del nodo.

- e. Selecciona **Mostrar más** para ver las direcciones IPv6 y las asignaciones de interfaces.

Puedes establecer conexiones desde aplicaciones cliente a cualquiera de las direcciones IP de la lista:

- **eth0**: Red de grid
- **eth1**: Red de administración (opcional)
- **eth2**: Red de cliente (opcional)



Si estás viendo un nodo de administración o un nodo de puerta de enlace y este es el nodo activo de un grupo de alta disponibilidad, la dirección IP virtual del grupo de alta disponibilidad aparece en eth2.

3. Para averiguar la dirección IP virtual de un grupo de alta disponibilidad:
 - a. Selecciona **Configuración > Red > Grupos de alta disponibilidad**.
 - b. En la tabla, toma nota de la dirección IP virtual del grupo de HA.
4. Para averiguar el número de puerto de un punto final del equilibrador de carga:
 - a. Selecciona **Configuración > Red > Puntos finales del equilibrador de carga**.
 - b. Anota el número de puerto del punto final que quieras utilizar.



Si el número de puerto es 80 o 443, el endpoint solo se configura en los Gateway Nodes, ya que esos puertos están reservados en los Admin Nodes. Todos los demás puertos se configuran tanto en los Gateway Nodes como en los Admin Nodes.

- c. Selecciona el nombre del punto final en la tabla.
- d. Comprueba que el **tipo de cliente** (S3) coincida con la aplicación cliente que va a utilizar el endpoint.

Gestiona redes y conexiones

Configura los ajustes de red de StorageGRID

Desde Grid Manager puedes configurar diversos parámetros de red para ajustar con precisión el funcionamiento de tu sistema StorageGRID.

Configurar interfaces VLAN

Puedes "[crear interfaces de red local virtual \(VLAN\)](#)" para aislar y dividir el tráfico por seguridad, flexibilidad y rendimiento. Cada interfaz VLAN está asociada con una o más interfaces principales en los nodos de administración y los nodos de puerta de enlace. Puedes usar interfaces VLAN en grupos HA y en endpoints de balanceador de carga para segregar el tráfico de cliente o de administración por aplicación o tenant.

Políticas de clasificación del tráfico

Puedes utilizar "[políticas de clasificación del tráfico](#)" para identificar y gestionar diferentes tipos de tráfico de red, incluido el tráfico relacionado con buckets, tenants, subredes de clientes o endpoints de balanceadores de carga específicos. Estas políticas pueden ayudarte a limitar y supervisar el tráfico.

Directrices para redes StorageGRID

Puedes utilizar el Grid Manager para configurar y gestionar las redes y conexiones de

StorageGRID.

Consulta "[Configura las conexiones del cliente S3](#)" para saber cómo conectar clientes de S3.

Redes StorageGRID predeterminadas

De forma predeterminada, StorageGRID admite tres interfaces de red por nodo de la red, lo que te permite configurar la red de cada nodo de forma individual para que se adapte a tus requisitos de seguridad y acceso.

Para obtener más información sobre la topología de red, consulta "[Directrices de redes](#)".

Red de grid

Obligatorio. La red Grid se utiliza para todo el tráfico interno de StorageGRID. Proporciona conectividad entre todos los nodos del grid, en todos los sitios y subredes.

Red de administración

Opcional. La red de administración se utiliza normalmente para la administración y el mantenimiento del sistema. También puede usarse para el acceso de protocolos de cliente. La red de administración suele ser una red privada y no necesita ser enrutable entre sitios.

Red de clientes

Opcional. La red de clientes es una red abierta que se suele utilizar para proporcionar acceso a las aplicaciones cliente de S3, de modo que la red de cuadrícula se pueda aislar y proteger. La red de clientes puede comunicarse con cualquier subred a la que se pueda acceder a través de la puerta de enlace local.

Directrices

- Cada nodo de 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 esté 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 grid, y debe estar en la misma subred que el nodo. Puedes implementar un enrutamiento más complejo en la puerta de enlace si lo necesitas.
- En cada nodo, cada red se asigna a una interfaz de red específica.

Red	Nombre de la interfaz
Grid	eth0
Admin (opcional)	eth1
Cliente (opcional)	eth2

- Si el nodo está conectado a un dispositivo StorageGRID, se utilizan puertos específicos para cada red. Para obtener más información, consulta las instrucciones de instalación de tu dispositivo.
- La ruta predeterminada se genera automáticamente para cada nodo. Si eth2 está habilitada, entonces 0.0.0.0/0 utiliza la red de cliente en eth2. Si eth2 no está habilitada, entonces 0.0.0.0/0 utiliza la Grid Network en eth0.

- La red de clientes no entra en funcionamiento hasta que el nodo de la red se une 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

Si lo deseas, puedes añadir interfaces adicionales a un nodo. Por ejemplo, quizá quieras añadir una interfaz de enlace troncal a un nodo Admin o Gateway, para que puedas usar ["Interfaces de VLAN"](#) para segregar el tráfico que pertenece a diferentes aplicaciones o tenants. O quizá quieras añadir una interfaz de acceso para usarla en un ["grupo de alta disponibilidad \(HA\)"](#).

Para añadir interfaces de tronco o de acceso, consulta lo siguiente:

- **VMware (tras instalar el nodo):** ["VMware: Añadir interfaces de tronco o de acceso a un nodo"](#)
 - **Linux (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Linux (después de instalar el nodo):** ["Agrega interfaces trunk o de acceso a un nodo"](#)



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Ver direcciones IP en StorageGRID

Puedes consultar la dirección IP de cada nodo de grid en tu sistema StorageGRID. Luego, puedes usar esta dirección IP para iniciar sesión en el nodo de grid desde la línea de comandos y realizar varios procedimientos de mantenimiento.

Antes de empezar

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

Acerca de esta tarea

Para obtener información sobre cómo cambiar las direcciones IP, consulta ["Configurar direcciones IP"](#).

Pasos

1. Selecciona **Nodos > nodo de cuadrícula > Resumen**.
2. Selecciona **Mostrar más** a la derecha del título Direcciones IP.

Las direcciones IP de ese nodo de la grid aparecen 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.			

Configura interfaces VLAN en StorageGRID

Crea interfaces de LAN virtual (VLAN) en los nodos de administración y los nodos de puerta de enlace y utilízalas en grupos de alta disponibilidad y puntos finales del equilibrador de carga para aislar y dividir el tráfico por seguridad, flexibilidad y rendimiento. Los nodos seleccionados en el grupo de alta disponibilidad pueden usar las interfaces VLAN para compartir hasta 10 direcciones IP virtuales, así que si un nodo se cae, otro nodo toma el control del tráfico hacia y desde las direcciones IP virtuales.

Aspectos a tener en cuenta sobre las interfaces VLAN

- Creas una interfaz VLAN introduciendo un ID de VLAN y eligiendo una interfaz principal en uno o varios nodos.

- Una interfaz principal debe configurarse como interfaz troncal en el switch.
- Una interfaz principal puede ser la Grid Network (eth0), la Client Network (eth2) o una interfaz troncal adicional para la VM o el host bare-metal (por ejemplo, ens256).
- Para cada interfaz VLAN, solo puedes seleccionar una interfaz principal para un nodo determinado. Por ejemplo, no puedes usar tanto la interfaz Grid Network como la interfaz Client Network en el mismo Gateway Node como interfaz principal para la misma VLAN.
- Si la interfaz VLAN está destinada al tráfico de los nodos de administración, lo que incluye el tráfico relacionado con el Grid Manager y el Tenant Manager, selecciona únicamente las interfaces de los nodos de administración.
- Si la interfaz VLAN está destinada al tráfico del cliente S3, selecciona interfaces en los nodos de administración o en los nodos de puerta de enlace.
- Si necesitas añadir interfaces de enlace troncal, consulta la siguiente información para obtener más detalles:
 - **VMware (tras instalar el nodo):** ["VMware: Añadir interfaces de tronco o de acceso a un nodo"](#)
 - **Linux (antes de instalar el nodo):** ["Crear archivos de configuración de nodos"](#)
 - **Linux (después de instalar el nodo):** ["Agrega interfaces trunk o de acceso a un nodo"](#)



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Crear una interfaz VLAN

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).
- Se ha configurado una interfaz de enlace troncal en la red y se ha conectado a la VM o al nodo Linux. Conoces el nombre de la interfaz de enlace troncal.
- Ya conoces el ID de la VLAN que estás configurando.

Acerca de esta tarea

Es posible que tu administrador de red haya configurado una o varias interfaces de enlace troncal y una o varias VLAN para segregar el tráfico de clientes o de administración correspondiente a diferentes aplicaciones o inquilinos. Cada VLAN se identifica mediante un identificador numérico o una etiqueta. Por ejemplo, tu red podría usar la VLAN 100 para el tráfico de FabricPool y la VLAN 200 para una aplicación de archivado.

Puedes utilizar el Grid Manager para crear interfaces VLAN que permitan a los clientes acceder a StorageGRID en una VLAN específica. Cuando creas interfaces VLAN, debes especificar el ID de la VLAN y seleccionar las interfaces principales (trunk) en uno o varios nodos.

Accede al asistente

Pasos

1. Selecciona **Configuración > Red > Interfaces VLAN**.
2. Selecciona **Crear**.

Introduce los datos de las interfaces de VLAN

Pasos

- 1. Especifica el ID de la VLAN en tu red. Puedes introducir cualquier valor entre 1 y 4094.

Los ID de VLAN no tienen por qué ser únicos. Por ejemplo, puedes usar el ID de VLAN 200 para el tráfico de administración en un sitio y el mismo ID de VLAN para el tráfico de clientes en otro sitio. Puedes crear interfaces de VLAN independientes con diferentes conjuntos de interfaces principales en cada sitio. Sin embargo, dos interfaces de VLAN con el mismo ID no pueden compartir la misma interfaz en un nodo. Si especificas un ID que ya se ha utilizado, aparece un mensaje.

- 2. Opcionalmente, escribe una breve descripción para la interfaz VLAN.
- 3. Selecciona **Continuar**.

Elige interfaces principales

La tabla muestra las interfaces disponibles para todos los nodos de administración y los nodos de pasarela en cada sitio de tu grid. Las interfaces de Admin Network (eth1) no pueden usarse como interfaces principales y no se muestran.

Pasos

- 1. Selecciona una o más interfaces principales a las que conectar esta VLAN.

Por ejemplo, podrías querer asociar una VLAN a la interfaz Client Network (eth2) de un Gateway Node y un Admin Node.

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.

Search...

	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. Selecciona **Continuar**.

Confirma la configuración

Pasos

1. Revisa la configuración y realiza los cambios que sean necesarios.
 - Si necesitas cambiar el ID de la VLAN o la descripción, selecciona **Introducir detalles de la VLAN** en la parte superior de la página.
 - Si necesitas cambiar una interfaz principal, selecciona **Elegir interfaces principales** en la parte superior de la página o selecciona **Anterior**.
 - Si necesitas eliminar una interfaz principal, selecciona el icono de la papelera .
2. Selecciona **Guardar**.
3. Espera hasta 5 minutos para que la nueva interfaz aparezca como opción en la página **Grupos de alta disponibilidad** y se incluya en la tabla **Interfaces de red** del nodo (**Nodos** > *parent interface node* > **Red**).

Editar una interfaz VLAN

Al editar una interfaz VLAN, puedes realizar los siguientes tipos de cambios:

- Modifica el ID o la descripción de la VLAN.
- Agregar o eliminar interfaces principales.

Por ejemplo, es posible que quieras eliminar una interfaz principal de una interfaz de VLAN si tienes previsto decomisionar el nodo asociado.

Ten en cuenta lo siguiente:

- No puedes cambiar el ID de una VLAN si la interfaz de la VLAN se usa en un grupo HA.
- No puedes eliminar una interfaz principal si esa interfaz se usa en un grupo de alta disponibilidad.

Por ejemplo, supón que la VLAN 200 está conectada a las interfaces principales en 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, puedes eliminar la interfaz principal no utilizada del nodo B, pero no puedes eliminar la interfaz principal utilizada del nodo A.

Pasos

1. Selecciona **Configuración** > **Red** > **Interfaces VLAN**.
2. Marca la casilla de la interfaz VLAN que quieras editar. A continuación, selecciona **Acciones** > **Editar**.
3. Si lo deseas, actualiza el ID de la VLAN o la descripción. Luego, selecciona **Continuar**.

No puedes actualizar el ID de una VLAN si la VLAN se usa en un grupo de alta disponibilidad (HA).

4. Si lo deseas, marca o desmarca las casillas de selección para añadir interfaces principales o eliminar interfaces que no se utilicen. Luego, selecciona **Continuar**.
5. Revisa la configuración y realiza los cambios que sean necesarios.
6. Selecciona **Guardar**.

Eliminar una interfaz VLAN

Puedes eliminar una o varias interfaces VLAN.

No puedes eliminar una interfaz VLAN si actualmente se está usando en un grupo HA. Debes quitar la interfaz VLAN del grupo HA antes de poder eliminarla.

Para evitar cualquier interrupción en el tráfico de clientes, considera hacer una de las siguientes cosas:

- Agrega una nueva interfaz VLAN al grupo HA antes de eliminar esta interfaz VLAN.
- Crea un nuevo grupo de alta disponibilidad que no utilice esta interfaz VLAN.
- Si la interfaz VLAN que quieres eliminar es actualmente la interfaz activa, edita el grupo de alta disponibilidad. Mueve la interfaz VLAN que quieres eliminar al final de la lista de prioridades. Espera hasta que se establezca la comunicación en la nueva interfaz primaria y luego elimina la interfaz anterior del grupo de alta disponibilidad. Por último, elimina la interfaz VLAN de ese nodo.

Pasos

1. Selecciona **Configuración > Red > Interfaces VLAN**.
2. Marca la casilla de selección correspondiente a cada interfaz VLAN que desees eliminar. A continuación, selecciona **Actions > Delete**.
3. Selecciona **Sí** para confirmar tu elección.

Se han eliminado todas las interfaces VLAN que has seleccionado. Aparece un mensaje verde de éxito en la página de interfaces VLAN.

Habilita StorageGRID CORS para una interfaz de gestión

Como administrador de la grid, puedes habilitar el intercambio de recursos entre orígenes (CORS) para las solicitudes de la API de gestión a StorageGRID, si quieres que los datos en StorageGRID sean accesibles usando las API de gestión desde otro dominio.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- El ["Permiso de acceso raíz"](#) proporciona acceso a todas las solicitudes de configuración de CORS.

Acerca de esta tarea

CORS es un mecanismo de seguridad que permite a las aplicaciones web cliente de un dominio acceder a recursos de un dominio diferente. Por ejemplo, supón que quieres crear un panel de control de monitorización para StorageGRID en el dominio `http://www.example.com`. Al habilitar CORS en StorageGRID para `http://www.example.com` y "Grid Manager", el dominio de StorageGRID responde a las solicitudes de la API de gestión de Grid desde `http://www.example.com`.

Las solicitudes de la API de gestión (mgmt-api) con `application/json` o `multipart/formdata` solicitudes para `Content-Type` son compatibles con CORS.

Pasos

1. En Grid Manager, ve a **CONFIGURACIÓN > Red > Ajustes CORS de la interfaz de gestión**.
2. Selecciona **Grid Manager**, **Tenant Manager** o ambas opciones.
 - **Grid Manager**: habilita CORS para las solicitudes de la API de gestión de Grid entre dominios.
 - **Tenant Manager**: habilita CORS para las solicitudes de la API de gestión de inquilinos entre dominios.
3. Introduce la URL del otro dominio en el campo **Dominios**.

Selecciona **Add another domain** si deseas habilitar CORS en StorageGRID para más de un dominio.

4. Selecciona **Guardar**.

Información relacionada

["Configura StorageGRID CORS para los buckets y los objetos"](#)

Gestiona las políticas de clasificación del tráfico

Políticas de clasificación de tráfico en StorageGRID

Las políticas de clasificación de tráfico te permiten identificar y supervisar diferentes tipos de tráfico de red. Estas políticas pueden ayudarte a limitar y supervisar el tráfico para mejorar tus ofertas de calidad de servicio (QoS).

Las políticas de clasificación de tráfico se aplican a los puntos de conexión en el servicio de equilibrador de carga de StorageGRID para los nodos de puerta de enlace y los nodos de administración. Para crear políticas de clasificación de tráfico, ya debes haber creado puntos de conexión del equilibrador de carga.

Reglas de coincidencia

Cada política de clasificación del tráfico contiene una o varias reglas de coincidencia para identificar el tráfico de red relacionado con una o varias de las siguientes entidades:

- Buckets
- Subred
- Inquilino
- Puntos de conexión del equilibrador de carga

StorageGRID supervisa el tráfico que coincide con cualquier regla de la política de acuerdo con los objetivos de dicha regla. Todo el tráfico que coincida con cualquier regla de una política se gestiona mediante dicha política. Por el contrario, puedes establecer reglas para que coincidan con todo el tráfico excepto el de una entidad específica.

Limitación del tráfico

Si lo deseas, puedes añadir los siguientes tipos de límite a una política:

- Ancho de banda de agregado
- Ancho de banda por solicitud
- Solicitudes simultáneas
- Tasa de solicitud

Los valores límite se aplican por cada equilibrador de carga. Si el tráfico se distribuye simultáneamente entre varios equilibradores de carga, las tasas máximas totales son un múltiplo de los límites de tasa que especifiques.



Puedes crear políticas para limitar el ancho de banda de 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 de agregado pueden imponer un impacto adicional menor en el rendimiento del tráfico no limitado.

Para los límites de ancho de banda de agregado o por solicitud, las solicitudes se transmiten de entrada o de salida a la velocidad que configures. 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 cuenta para otras políticas coincidentes menos específicas que contengan políticas de límite de ancho de banda de agregado. Para todos los demás tipos de límites, las solicitudes de los clientes se retrasan 250 milisegundos y reciben una respuesta 503 Slow Down en el caso de las solicitudes que superen cualquier límite de política coincidente.

En el Grid Manager, puedes consultar los gráficos de tráfico y comprobar que las políticas están aplicando los límites de tráfico que esperas.

Utiliza políticas de clasificación del tráfico con SLA

Puedes usar las políticas de clasificación del tráfico junto con los límites de capacidad y la protección de datos para hacer cumplir los acuerdos de nivel de servicio (SLA) que proporcionan detalles específicos sobre capacidad, protección de datos y rendimiento.

El siguiente ejemplo muestra tres niveles de un SLA. Puedes crear políticas de clasificación de tráfico para alcanzar los objetivos de rendimiento de cada nivel de SLA.

Nivel de servicio	Capacidad	Protección de datos	Rendimiento máximo permitido	Coste
Oro	1 PB de almacenamiento permitido	3 copia de la regla ILM	25 000 solicitudes por segundo 5 GB/s (40 Gbps) de ancho de banda	\$\$\$ al mes
Plata	250 TB de almacenamiento permitidos	2 copia de la regla ILM	10 K solicitudes/seg 1,25 GB/s (10 Gbps) de ancho de banda	\$\$ al mes
Bronce	100 TB de almacenamiento permitidos	2 copia de la regla ILM	5 K solicitudes/seg 1 GB/s (8 Gbps) de ancho de banda	\$ al mes

Crear políticas de clasificación de tráfico StorageGRID

Puedes crear políticas de clasificación de tráfico si quieres supervisar y, opcionalmente, limitar el tráfico de red por bucket, expresión regular de bucket, CIDR, extremo de equilibrador de carga o inquilino. Opcionalmente, puedes establecer límites para una política en función del ancho de banda, el número de solicitudes simultáneas o la tasa de solicitudes.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).
- Has creado los puntos de conexión del equilibrador de carga que deseas hacer coincidir.
- Has creado todos los tenants que deseas que coincidan.

Pasos

1. Selecciona **Configuración > Red > Clasificación del tráfico**.
2. Selecciona **Crear**.
3. Introduce un nombre y una descripción (opcional) para la política y selecciona **Continuar**.

Por ejemplo, describe a qué se aplica esta política de clasificación del tráfico y qué limitará.

4. Selecciona **Add rule** e indica los siguientes datos para crear una o varias reglas de coincidencia para la política. Cualquier política que crees debe tener al menos una regla de coincidencia. Selecciona **Continue**.

Campo	Descripción
Tipo	Selecciona los tipos de tráfico a los que se aplica la regla de coincidencia. Los tipos de tráfico son bucket, bucket regex, CIDR, load balancer endpoint y tenant.
Valor de coincidencia	Introduce el valor que coincida con el tipo seleccionado. • Depósito: introduce uno o varios nombres de depósitos. • Expresión regular de buckets: introduce una o varias expresiones regulares que se usan para buscar coincidencias con un conjunto de nombres de buckets. La expresión regular no está anclada. Usa el ancla ^ para buscar coincidencias al principio del nombre del bucket y usa el ancla \$ para buscar coincidencias al final del nombre. La coincidencia de expresiones regulares admite un subconjunto de la sintaxis de PCRE (expresión regular compatible con Perl). • CIDR: introduce una o varias subredes IPv4, en notación CIDR, que coincidan con la subred deseada. • Punto final del equilibrador de carga: selecciona un nombre de punto final. Estos son los puntos finales del equilibrador de carga que has definido en el "Configura los puntos de conexión del equilibrador de carga". • Inquilino: la coincidencia de inquilino usa el ID de la clave de acceso. Si la solicitud no contiene un ID de clave de acceso (por ejemplo, acceso anónimo), entonces se utiliza la titularidad del bucket al que se accede para determinar el inquilino.

Campo	Descripción
Coincidencia inversa	Si deseas filtrar todo el tráfico de red <i>excepto</i> aquel que coincida con el tipo y el valor de coincidencia que acabas de definir, marca la casilla Coincidencia inversa. En caso contrario, deja la casilla desmarcada. Por ejemplo, si quieres que esta política se aplique a todos los puntos finales del equilibrador de carga excepto uno, especifica el punto final del equilibrador de carga que se va a excluir y selecciona Coincidencia inversa. En una política que contenga varios criterios de coincidencia, donde al menos uno sea un criterio de coincidencia inversa, ten cuidado de no crear una política que coincida con todas las solicitudes.

5. Si lo deseas, selecciona **Add a limit** y elige los siguientes detalles para añadir uno o varios límites con los que controlar el tráfico de red al que se aplica una regla.



StorageGRID recopila métricas incluso si no agregas ningún límite, así puedes entender las tendencias del tráfico.

Campo	Descripción
Tipo	El tipo de límite que deseas aplicar al tráfico de red que coincide con la regla. Por ejemplo, puedes limitar el ancho de banda o la frecuencia de solicitudes. Nota: Puedes crear políticas para limitar el ancho de banda de 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 de 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 de agregado no está disponible. Los límites del ancho de banda de agregado pueden suponer un impacto menor adicional en el rendimiento del tráfico no limitado. En cuanto a los límites de ancho de banda, StorageGRID aplica la política que mejor se ajusta al tipo de límite establecido. Por ejemplo, si tienes una política que limita el tráfico en una sola dirección, el tráfico en la dirección opuesta no tendrá límite, incluso si hay tráfico que coincide con políticas adicionales que tienen límites de ancho de banda. StorageGRID aplica 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 bucket • Inquilino • Punto final • Coincidencias CIDR no exactas (que no sean /32) • Coincidencias inversas

Campo	Descripción
Aplica a	Si este límite se aplica a las solicitudes de lectura de los clientes (GET o HEAD) o a las solicitudes de escritura (PUT, POST o DELETE).
Valor	El valor al que se limitará el tráfico de red, según la unidad que selecciones. Por ejemplo, introduce 10 y selecciona MiB/s para evitar que el tráfico de red que coincida con esta regla supere los 10 MiB/s. Nota: dependiendo del ajuste de las unidades, las unidades disponibles serán binarias (por ejemplo, GiB) o decimales (por ejemplo, GB). Para cambiar el ajuste de las unidades, selecciona el menú desplegable de usuario en la parte superior derecha de Grid Manager y, a continuación, selecciona Preferencias de usuario .
Unidad	La unidad que describe el valor que has introducido.

Por ejemplo, si quieres establecer un límite de ancho de banda de 4 GB/s para un nivel de SLA, crea dos límites de ancho de banda de agregado: GET/HEAD a 4 GB/s y PUT/POST/DELETE a 4 GB/s.

6. Selecciona **Continuar**.
7. Lee y revisa la política de clasificación de tráfico. Usa el botón **Anterior** para volver y realizar cambios según sea necesario. Cuando estés satisfecho con la política, selecciona **Guardar y continuar**.

El tráfico del cliente S3 ahora se gestiona según la política de clasificación del tráfico.

Después de que termines

"[Ver métricas de tráfico de red](#)" para verificar que las políticas estén aplicando los límites de tráfico que esperas.

Edita una política de clasificación de tráfico de StorageGRID

Puedes editar una política de clasificación del tráfico para cambiar su nombre o descripción, o para crear, editar o eliminar cualquier regla o límite de la política.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tienes el "[Permiso de acceso raíz](#)".

Pasos

1. Selecciona **Configuración > Red > Clasificación del tráfico**.

Aparece la página «Políticas de clasificación del tráfico» y las políticas existentes se muestran en una tabla.

2. Edita la política mediante el menú «Acciones» o la página de detalles. Consulta "[crear políticas de clasificación del tráfico](#)" para saber qué datos debes introducir.

Menú de acciones

- a. Marca la casilla para la política.
- b. Selecciona **Acciones** > **Editar**.

Página de detalles

- a. Selecciona el nombre de la política.
- b. Selecciona el botón **Editar** situado junto al nombre de la política.

3. En el paso «Introducir el nombre de la política», si lo deseas, edita el nombre o la descripción de la política y selecciona **Continuar**.
4. En el paso «Add matching rules», puedes añadir una regla o editar el **Tipo** y el **Valor de coincidencia** de la regla existente, y seleccionar **Continuar**.
5. En el paso «Establecer límites», puedes añadir, editar o eliminar un límite de forma opcional y seleccionar **Continuar**.
6. Revisa la política actualizada y selecciona **Guardar y continuar**.

Se han guardado los cambios que has realizado en la política y ahora el tráfico de red se gestiona de acuerdo con las políticas de clasificación de tráfico. Puedes ver los gráficos de tráfico y verificar que las políticas estén aplicando los límites de tráfico que esperas.

Eliminar una política de clasificación de tráfico StorageGRID

Puedes eliminar una política de clasificación de tráfico si ya no la necesitas. Asegúrate de eliminar la política correcta porque una política no se puede recuperar cuando se elimina.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).

Pasos

1. Selecciona **Configuración** > **Red** > **Clasificación del tráfico**.

Aparece la página de políticas de clasificación del tráfico con las políticas existentes listadas en una tabla.

2. Elimina la política usando el menú Acciones o la página de detalles.

Menú de acciones

- a. Marca la casilla para la política.
- b. Selecciona **Acciones** > **Eliminar**.

Página de detalles de la política

- a. Selecciona el nombre de la política.
- b. Selecciona el botón **Eliminar** junto al nombre de la política.

3. Selecciona **Sí** para confirmar que quieres eliminar la política.

La política se eliminó.

Ver métricas de tráfico de red en StorageGRID

Puedes supervisar el tráfico de red consultando los gráficos disponibles en la página de políticas de clasificación del tráfico.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Acceso raíz o permisos de cuentas de inquilino"](#).

Acerca de esta tarea

Para cualquier política de clasificación de tráfico existente, puedes consultar las métricas del servicio de equilibrador de carga para determinar si la política está limitando correctamente el tráfico en la red. Los datos de los gráficos pueden ayudarte a determinar si necesitas ajustar la política.

Aunque no se establezcan límites en una política de clasificación del tráfico, se recopilan métricas y los gráficos ofrecen información útil para comprender las tendencias del tráfico.

Pasos

1. Selecciona **Configuración > Red > Clasificación del tráfico**.

Aparece la página «Políticas de clasificación del tráfico» y las políticas existentes se muestran en la tabla.

2. Selecciona el nombre de la política de clasificación de tráfico para la que quieres ver las métricas.
3. Selecciona la pestaña **Métricas**.

Aparecen los gráficos de la política de clasificación del tráfico. Los gráficos muestran métricas únicamente para el tráfico que coincide con la política seleccionada.

En esta página se incluyen los siguientes gráficos.

- Tasa de solicitudes: Este gráfico muestra la cantidad de ancho de banda que se ajusta a esta política y que gestionan todos los equilibradores de carga. Los datos recibidos incluyen los encabezados de todas las solicitudes y el tamaño del cuerpo de las respuestas que contienen datos en el cuerpo. Los datos enviados incluyen los encabezados de todas las solicitudes y el tamaño del cuerpo de las respuestas que contienen datos en el cuerpo.



Cuando las solicitudes se han completado, este gráfico solo muestra el uso del ancho de banda. En el caso de solicitudes lentas o de objetos de gran tamaño, el ancho de banda instantáneo real puede diferir de los valores que se muestran en este gráfico.

- Tasa de respuestas con error: Este gráfico muestra una tasa aproximada a la que las solicitudes que cumplen esta política devuelven errores (código de estado HTTP ≥ 400) a los clientes.
- Duración media de las solicitudes (sin errores): este gráfico muestra la duración media de las solicitudes correctas que cumplen esta política.
- Uso del ancho de banda de la política: Este gráfico muestra la cantidad de ancho de banda correspondiente a esta política gestionada por todos los equilibradores de carga. Los datos recibidos incluyen los encabezados de las solicitudes y el tamaño del cuerpo de las respuestas que tienen datos

en el cuerpo. Los datos enviados incluyen los encabezados de las respuestas y el tamaño del cuerpo de las respuestas para las solicitudes que incluyen datos en el cuerpo de la respuesta.

4. Coloca el cursor sobre un gráfico de líneas para que aparezca una ventana emergente con los valores correspondientes a una parte concreta del gráfico.
5. Selecciona **Grafana dashboard** justo debajo del título Metrics para ver todos los gráficos de una política. Además de los cuatro gráficos de la pestaña **Metrics**, puedes ver dos gráficos más:
 - Tasa de solicitudes de escritura por tamaño de objeto: la tasa correspondiente a las solicitudes PUT/POST/DELETE que cumplen esta política. Al situar el cursor sobre una celda concreta, se muestran las tasas por segundo. Las tasas que se muestran al pasar el cursor por encima se redondean a números enteros y pueden indicar 0 aunque haya solicitudes distintas de cero en el bucket.
 - Tasa de solicitudes de lectura por tamaño de objeto: la tasa de solicitudes GET/HEAD que coinciden con esta política. Al colocarte sobre una celda individual, verás las tasas por segundo. Las tasas que se muestran en la vista al pasar el cursor se truncan a números enteros y podrían mostrar 0 si hay solicitudes distintas de cero en el bucket.
6. También puedes acceder a los gráficos desde el menú **Support**.
 - a. Selecciona **Soporte > Herramientas > Métricas**.
 - b. Selecciona **Política de clasificación del tráfico** en la sección **Grafana**.
 - c. Selecciona la política en el menú situado en la parte superior izquierda de la página.
 - d. Coloca 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 al recuento y el número de solicitudes por segundo durante ese periodo de tiempo.

Las políticas de clasificación de tráfico se identifican por su ID. Los ID de las políticas se muestran en la página Políticas de clasificación de tráfico.

7. Analiza los gráficos para determinar con qué frecuencia la política está limitando el tráfico y si necesitas ajustar la política.

Cifrados admitidos para conexiones TLS salientes en StorageGRID

El sistema StorageGRID admite un conjunto limitado de conjuntos de cifrado para las conexiones de Transport Layer Security (TLS) con los sistemas externos utilizados para la federación de identidades y Cloud Storage Pools.

Versiónes compatibles de TLS

StorageGRID es compatible con TLS 1.2 y TLS 1.3 para conexiones con sistemas externos usados para la federación de identidades y Cloud Storage Pools.

Los algoritmos de cifrado TLS compatibles con sistemas externos se han seleccionado para garantizar la compatibilidad con una amplia gama de sistemas externos. Esta lista es más amplia que la de los algoritmos de cifrado compatibles con las aplicaciones cliente de S3. Para configurar los algoritmos de cifrado, ve a **Configuración > Seguridad > Ajustes de seguridad** y selecciona **Políticas de TLS y SSH**.



Las opciones de configuración de TLS, como las versiones de protocolo, los cifrados, los algoritmos de intercambio de claves y los algoritmos MAC, no se pueden configurar en StorageGRID. Ponte en contacto con tu representante de cuenta de NetApp si tienes alguna solicitud específica sobre estos ajustes.

Beneficios de las conexiones HTTP activas, inactivas y concurrentes en StorageGRID

La forma en que configuras las conexiones HTTP puede afectar el rendimiento del sistema StorageGRID. Las configuraciones varían según si la conexión HTTP está activa o inactiva, o si tienes varias conexiones simultáneas.

Puedes identificar los beneficios de rendimiento para los siguientes tipos de conexiones HTTP:

- Conexiones HTTP inactivas
- Conexiones HTTP activas
- Conexiones HTTP simultáneas

Ventajas de mantener abiertas las conexiones HTTP inactivas

Mantén abiertas las conexiones HTTP cuando las aplicaciones cliente estén inactivas para permitir transacciones posteriores. Mantén abierta una conexión HTTP inactiva durante un máximo de 10 minutos. StorageGRID podría cerrar automáticamente una conexión HTTP que esté abierta e inactiva durante más de 10 minutos.

Las conexiones HTTP abiertas e inactivas ofrecen las siguientes ventajas:

- Reducción de la latencia desde el momento en que el sistema StorageGRID determina que debe realizar una transacción HTTP hasta el momento en que el sistema StorageGRID puede llevar a cabo dicha transacción

La reducción de la latencia es la principal ventaja, especialmente por el tiempo que se necesita para establecer conexiones TCP/IP y TLS.

- Aumento de la tasa de transferencia de datos al preparar el algoritmo de inicio lento de TCP/IP con transferencias realizadas anteriormente
- Notificación instantánea de varias clases de condiciones de fallo que interrumpen la conectividad entre la aplicación cliente y el sistema StorageGRID

Decide cuánto tiempo mantener abierta una conexión inactiva, equilibrando los beneficios del slow start y la asignación de recursos.

Ventajas de las conexiones HTTP activas

En el caso de las conexiones directas a los nodos de almacenamiento, debes limitar la duración de una conexión HTTP activa a un máximo de 10 minutos, incluso si la conexión HTTP realiza transacciones de forma continua.

Determinar la duración máxima durante la cual debe mantenerse abierta una conexión 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 los nodos de almacenamiento, limitar las conexiones HTTP activas ofrece los siguientes beneficios:

- Permite un equilibrio de carga óptimo en todo el sistema StorageGRID.

Con el tiempo, puede que una conexión HTTP ya no sea óptima a medida que cambian los requisitos de balanceo de carga. El sistema realiza su mejor balanceo de carga cuando las aplicaciones cliente establecen una conexión HTTP independiente para cada transacción, pero este método anula las valiosas

ventajas asociadas con las conexiones persistentes.

- Permite a las aplicaciones cliente dirigir las transacciones HTTP a los servicios LDR que tengan espacio disponible.
- Permite iniciar los procedimientos de mantenimiento.

Algunos procedimientos de mantenimiento solo comienzan después de que se completan todas las conexiones HTTP en curso.

En el caso de las conexiones de los clientes al servicio Load Balancer, limitar la duración de las conexiones abiertas puede ser útil para permitir que algunos procedimientos de mantenimiento se inicien sin demora. Si no se limita la duración de las conexiones de los clientes, las conexiones activas pueden tardar varios minutos en cerrarse automáticamente.

Ventajas de las conexiones HTTP simultáneas

Debes mantener abiertas varias conexiones TCP/IP con el sistema StorageGRID para permitir el paralelismo, lo que aumenta el rendimiento. El número óptimo de conexiones paralelas depende de diversos factores.

Las conexiones HTTP simultáneas ofrecen las siguientes ventajas:

- Latencia reducida

Las transacciones pueden iniciarse de inmediato en lugar de esperar a que se completen otras transacciones.

- Aumento del rendimiento

El sistema StorageGRID puede realizar transacciones en paralelo y aumentar el rendimiento global de las transacciones.

Las aplicaciones cliente deberían establecer varias conexiones HTTP. Cuando una aplicación cliente tenga que realizar una transacción, puede seleccionar y usar inmediatamente cualquier conexión establecida que no esté procesando una transacción en ese momento.

La topología de cada sistema StorageGRID tiene un rendimiento máximo diferente para las transacciones y conexiones simultáneas. El rendimiento máximo depende de la computación, la red, los recursos de almacenamiento, los enlaces WAN y el número de servidores, servicios y aplicaciones que admite el sistema StorageGRID.

Los sistemas StorageGRID suelen admitir varias aplicaciones cliente. Ten esto en cuenta cuando determines el número máximo de conexiones simultáneas. Si la aplicación cliente consta de varias entidades de software y cada una de ellas establece conexiones con el sistema StorageGRID, suma todas las conexiones de las distintas entidades. Es posible que tengas que ajustar el número máximo de conexiones simultáneas en las siguientes situaciones:

- La topología del sistema StorageGRID influye en el número máximo de transacciones y conexiones simultáneas que el sistema puede admitir.
- Es posible que las aplicaciones cliente que interactúan con el sistema StorageGRID a través de una red con un ancho de banda limitado tengan que reducir el nivel de concurrencia para garantizar que las transacciones individuales se completen en un tiempo razonable.
- Cuando hay muchas aplicaciones cliente que comparten el sistema StorageGRID, es posible que tengas que reducir el nivel de concurrencia para evitar sobrepasar los límites del sistema.

Separación de los grupos de conexiones HTTP para operaciones de lectura y escritura

Puedes usar pools de conexiones HTTP independientes para las operaciones de lectura y escritura, y controlar qué parte de un pool utilizar para cada una. Los pools de conexiones HTTP independientes te permiten controlar mejor las transacciones y equilibrar las cargas.

Las aplicaciones cliente pueden generar cargas en las que predomine la recuperación de datos (lectura) o el almacenamiento de datos (escritura). Con grupos separados de conexiones HTTP para las transacciones de lectura y escritura, puedes ajustar cuánto de cada grupo se dedica a las transacciones de lectura o escritura.

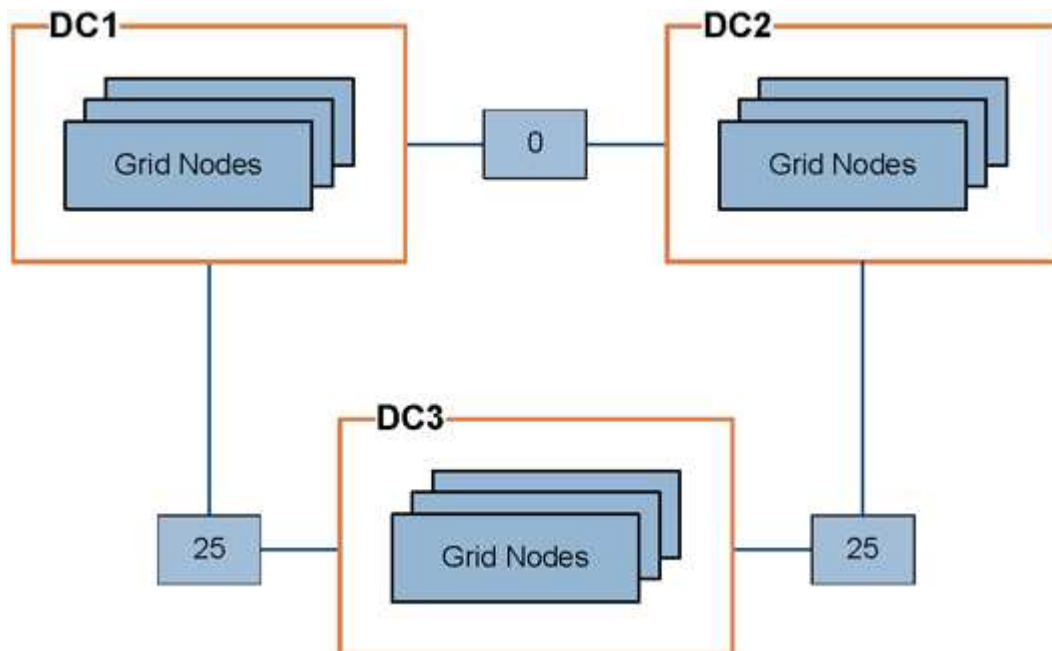
Administra los costes de enlace en StorageGRID

Los costes de enlace te permiten priorizar qué centro de datos proporciona un servicio solicitado cuando existen dos o más centros de datos. Puedes ajustar los costes de enlace para reflejar la latencia entre los sitios.

¿Qué son los costes de enlace?

- Los costes de enlace se utilizan para priorizar qué copia del objeto se usa para cumplir con las recuperaciones de objetos.
- Los costes de enlace son utilizados por la Grid Management API y la Tenant Management API para determinar qué servicios internos de StorageGRID se deben usar.
- El servicio Load Balancer en los nodos de administración y los nodos de puerta de enlace utiliza los costes de enlace para dirigir las conexiones de clientes. Consulta ["Aspectos a tener en cuenta para el equilibrio de carga"](#).

El diagrama muestra una red de tres sitios en la que se han configurado los costes de enlace entre los sitios:



- El servicio de equilibrio de carga en los nodos de administración y los nodos de puerta de enlace distribuye por igual las conexiones de los clientes a todos los nodos de almacenamiento en el mismo sitio del centro de datos y a cualquier sitio de centro de datos con un coste de enlace de 0.

En el ejemplo, un nodo de puerta de enlace en el centro de datos 1 (DC1) distribuye de forma equitativa

las conexiones de los clientes a los nodos de almacenamiento en DC1 y a los nodos de almacenamiento en DC2. Un nodo de puerta de enlace en DC3 envía las conexiones de los clientes solo a los nodos de almacenamiento en DC3.

- Al recuperar un objeto del que existen varias copias replicadas, StorageGRID recupera la copia del centro de datos que tiene el menor coste de enlace.

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 coste de enlace de DC1 a DC2 es 0, que es menor que el coste de enlace de DC3 a DC2 (25).

Los costes de enlace son valores numéricos relativos arbitrarios que carecen de una unidad de medida específica. Por ejemplo, un coste de enlace de 50 se utiliza con menos preferencia que un coste de 25. La tabla muestra los costes de enlace más habituales.

Enlace	Coste del enlace	Notas
Entre los sitios físicos del centro de datos	25 (por defecto)	Centros de datos conectados mediante un enlace WAN.
Entre 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.

Actualizar los costes de los enlaces

Puedes actualizar los costes de los enlaces entre los centros de datos para reflejar la latencia entre los sitios.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Otros permisos de configuración de grid"](#).

Pasos

1. Selecciona **Soporte > Otros > Coste 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	Link Destination			Actions
	10	20	30	
Data Center 1	0	25	25	



2. Selecciona un sitio en **Origen del enlace** e introduce un valor de coste comprendido entre 0 y 100 en **Destino del enlace**.

No puedes cambiar el coste del enlace si el origen es el mismo que el destino.

Para cancelar los cambios, selecciona  **Revert**.

3. Selecciona **Aplicar cambios**.

Usa AutoSupport

Conoce AutoSupport en StorageGRID

La función AutoSupport permite que StorageGRID envíe paquetes de estado y salud al soporte técnico de NetApp.

Usar AutoSupport ayuda a resolver los problemas más rápido. El soporte técnico puede supervisar las necesidades de almacenamiento de tu sistema y ayudarte a determinar si necesitas añadir nuevos nodos o sitios. Opcionalmente, AutoSupport puede enviar paquetes a un destino adicional.

StorageGRID tiene dos tipos de AutoSupport:

- **StorageGRID AutoSupport** informa de los problemas de software de StorageGRID. Activado de forma predeterminada la primera vez que instalas StorageGRID. Puedes ["cambia la configuración predeterminada de AutoSupport"](#) si lo necesitas.



Si StorageGRID AutoSupport no está habilitado, aparece un mensaje en el panel de control de Grid Manager. El mensaje incluye un enlace a la página de configuración de AutoSupport. Si cierras el mensaje, no volverá a aparecer hasta que se borre la caché del navegador, incluso si AutoSupport sigue deshabilitado.

- El **AutoSupport de hardware del appliance** informa de los problemas del appliance StorageGRID. Debes ["Configura el hardware AutoSupport en cada dispositivo"](#).

¿Qué es Active IQ?

Active IQ es un asesor digital basado en cloud que aprovecha el análisis predictivo y la sabiduría colectiva de la base instalada de NetApp. Sus evaluaciones continuas de riesgos, alertas predictivas, orientación prescriptiva y acciones automatizadas te ayudan a prevenir problemas antes de que ocurran, lo que lleva a una mejor salud del sistema y una mayor disponibilidad del sistema.

Si deseas utilizar los paneles de control y las funciones de Active IQ en el sitio de soporte de NetApp, debes activar AutoSupport.

["Documentación de Active IQ Digital Advisor"](#)

Información incluida en el paquete AutoSupport

Un paquete de AutoSupport contiene los siguientes archivos y detalles.

Nombre del archivo	Campos	Descripción
AUTOSUPPORT-HISTORY.XML	Número de secuencia de AutoSupport + destino para este AutoSupport + estado de la 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.
AUTOSUPPORT.XML	Nodo + Protocolo para contactar soporte técnico + URL de soporte técnico para HTTP/HTTPS + Dirección de soporte técnico + AutoSupport OnDemand estado + AutoSupport OnDemand URL del servidor + AutoSupport OnDemand intervalo de sondeo	Archivo de estado de AutoSupport. Proporciona detalles del protocolo utilizado, la dirección y URL de soporte técnico, el intervalo de sondeo y si OnDemand AutoSupport está habilitado o deshabilitado.

Nombre del archivo	Campos	Descripción
BUCKETS.XML	ID del bucket + ID de la cuenta + Versión de compilación + Configuración de restricción de ubicación + Cumplimiento activado + Configuración de cumplimiento + Bloqueo de objetos S3 activado + Configuración de bloqueo de objetos S3 + Configuración de consistencia + CORS activado + Configuración de CORS + Tiempo de último acceso activado + Política activada + Configuración de política + Notificaciones activadas + Configuración de notificaciones + Cloud Mirror activado + Configuración de Cloud Mirror + Búsqueda activada + Configuración de búsqueda + Etiquetado de bucket activado + Configuración de etiquetado de bucket + Configuración de versionado	Proporciona detalles de configuración y estadísticas a nivel de bucket. Los ejemplos de configuraciones de bucket incluyen servicios de plataforma, cumplimiento y consistencia de bucket.
GRID-CONFIGURATIONS.XML	ID del atributo + Nombre del atributo + Valor + Índice + ID de la tabla + Nombre de la tabla	Archivo de configuración para toda la red. Contiene información sobre los certificados de la red, el espacio reservado para metadatos, los parámetros de configuración para toda la red (cumplimiento, S3 Object Lock, compresión de objetos, alertas, syslog y configuración de ILM), detalles del perfil de código de borrado, el nombre DNS y " Nombre de la NMS ".
GRID-SPEC.XML	Especificaciones de grid, XML sin procesar	Se utiliza para configurar e implementar StorageGRID. Contiene las especificaciones de grid, la dirección IP del servidor NTP, la dirección IP del servidor DNS, la topología de red y los perfiles de hardware de los nodos.
GRID-TASKS.XML	Nodo + Ruta del servicio + ID del atributo + Nombre del atributo + Valor + Índice + ID de la tabla + Nombre de la tabla	Archivo de estado de las tareas de grid (procedimientos de mantenimiento). Proporciona detalles sobre las tareas activas, finalizadas, completadas, fallidas y pendientes de grid.

Nombre del archivo	Campos	Descripción
GRID.JSON	Grid + Revisión + Versión del software + Descripción + Licencia + Contraseñas + DNS + NTP + Sitios + Nodos	Información del grid.
ILM-CONFIGURATION.XML	ID del atributo + Nombre del atributo + Valor + Índice + ID de la tabla + Nombre de la tabla	Lista de atributos para las configuraciones de ILM.
ILM-STATUS.XML	Nodo + Ruta del servicio + ID del atributo + Nombre del atributo + Valor + Índice + ID de la tabla + Nombre de la tabla	Archivo de información de métricas de ILM. Contiene las tasas de evaluación de ILM para cada nodo y las métricas de todo el grid.
ILM.XML	XML sin procesar de ILM	Archivo de políticas activas de ILM. Contiene información detallada sobre las políticas activas de ILM, como el ID del grupo de almacenamiento, el comportamiento de ingesta, los filtros, las reglas y la descripción.
LOG.TGZ	<i>n/a</i>	Archivo de registro descargable. Contiene <code>bycast-err.log</code> y <code>servermanager.log</code> de cada nodo.
MANIFEST.XML	Orden de recopilación + Nombre de archivo de contenido de AutoSupport para estos datos + Descripción de este elemento de datos + Número de bytes recopilados + Tiempo empleado en la recopilación + Estado de este elemento de datos + Descripción del error + Tipo de contenido de AutoSupport para estos datos +	Contiene metadatos de AutoSupport y descripciones breves de todos los archivos de AutoSupport.
NMS-ENTITIES.XML	Índice de atributo + OID de la entidad + ID del nodo + ID del modelo del dispositivo + Versión del modelo del dispositivo + Nombre de la entidad	Entidades de grupo y de servicio en el " Árbol NMS ". Proporciona detalles de la topología de grid. El nodo se puede determinar según los servicios que se ejecutan en el nodo.

Nombre del archivo	Campos	Descripción
OBJECTS-STATUS.XML	Nodo + Ruta del servicio + ID del atributo + Nombre del atributo + Valor + Índice + ID de la tabla + Nombre de la tabla	Estado de los objetos, incluyendo el estado del escaneo en segundo plano, la transferencia activa, la tasa de transferencia, el total de transferencias, la tasa de eliminación, los fragmentos dañados, los objetos perdidos, los objetos que faltan, los intentos de reparación, la tasa de escaneo, el periodo estimado de escaneo y el estado de finalización de la reparación.
SERVER-STATUS.XML	Nodo + Ruta del servicio + ID del atributo + Nombre del atributo + Valor + Índice + ID de la tabla + Nombre de la tabla	Configuraciones del servidor. Contiene los siguientes datos para cada nodo: tipo de plataforma, sistema operativo, memoria instalada, memoria disponible, conectividad de almacenamiento, número de serie del chasis del dispositivo de almacenamiento, número de unidades con error 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.
SERVICE-STATUS.XML	Nodo + Ruta del servicio + ID del atributo + Nombre del atributo + Valor + Índice + ID de la tabla + Nombre de la tabla	Archivo de información del nodo de servicio. Contiene detalles como el espacio de tabla asignado, el espacio de tabla libre, las métricas de Reaper de la base de datos, la duración de la reparación de segmentos, la duración del trabajo de reparación, los reinicios automáticos de trabajos y la finalización automática de trabajos.
STORAGE-GRADES.XML	ID de nivel de almacenamiento + Nombre del nivel de almacenamiento + ID del nodo de almacenamiento + Ruta del nodo de almacenamiento	Archivo de definiciones de nivel de almacenamiento para cada nodo de almacenamiento.
RESUMEN-ATRIBUTOS.XML	OID del grupo + Ruta del grupo + ID del atributo de resumen + Nombre del atributo de resumen + Valor + Índice + ID de la tabla + Nombre de la tabla	Datos a grandes rasgos sobre el estado del sistema que resumen la información de uso de StorageGRID. Proporciona detalles como el nombre de grid, los nombres de los sitios, el número de Storage Nodes por grid y por sitio, el tipo de licencia, la capacidad y el uso de la licencia, las condiciones de soporte técnico del software y los detalles de las operaciones S3.

Nombre del archivo	Campos	Descripción
SYSTEM-ALERTS.XML	Nombre + Gravedad + Nombre de nodo + Estado de la alerta + Nombre del sitio + Hora de activación de la alerta + Hora de resolución de la alerta + ID de la regla + ID del nodo + ID del sitio + Silenciada + Otras anotaciones + Otras etiquetas	Alertas actuales del sistema que indican posibles problemas en el sistema StorageGRID.
USERAGENTS.XML	Agente de usuario + Número de días + Total de peticiones HTTP + Total de bytes ingeridos + Total de bytes recuperados + Peticiones PUT + Peticiones GET + Peticiones DELETE + Peticiones HEAD + Peticiones POST + Peticiones OPTIONS + Tiempo medio de petición (ms) + Tiempo medio de petición PUT (ms) + Tiempo medio de petición GET (ms) + Tiempo medio de petición DELETE (ms) + Tiempo medio de petición HEAD (ms) + Tiempo medio de petición POST (ms) + Tiempo medio de petición OPTIONS (ms)	Estadísticas basadas en los agentes de usuario de la aplicación. Por ejemplo, el número de operaciones PUT/GET/DELETE/HEAD por agente de usuario y el tamaño total en bytes de cada operación.
X-HEADER-DATA	X-Netapp-asup-generated-on + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject + X-Netapp-asup-system-id + X-Netapp-asup-model-name +	Datos de cabecera de AutoSupport.

Configura AutoSupport en StorageGRID

De forma predeterminada, la función AutoSupport de StorageGRID está habilitada cuando instalas StorageGRID por primera vez. Sin embargo, debes configurar el hardware AutoSupport en cada appliance. Si lo necesitas, puedes cambiar la configuración de AutoSupport.

Si quieres cambiar la configuración de StorageGRID AutoSupport, realiza tus cambios solo en el nodo de administración primario. Debes [configura el hardware AutoSupport](#) en cada appliance.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).
- Si vas a utilizar HTTPS para enviar paquetes de AutoSupport, has proporcionado acceso saliente a internet al nodo de administración primario, ya sea directamente o ["utilizando un servidor proxy"](#) (no se requieren conexiones entrantes).
- Si se selecciona HTTP en la página de StorageGRID AutoSupport, tienes ["configuraste un servidor proxy"](#) para reenviar los paquetes de AutoSupport como HTTPS. Los servidores de NetApp AutoSupport rechazarán los paquetes enviados mediante HTTP.
- Si vas a utilizar SMTP como protocolo para los paquetes de AutoSupport, ya has configurado un servidor de correo SMTP.

Acerca de esta tarea

Puedes usar cualquier combinación de las siguientes opciones para enviar paquetes de AutoSupport al soporte técnico:

- **Semanal:** envía automáticamente paquetes de AutoSupport una vez a la semana. Configuración predeterminada: habilitado.
- **Activado por eventos:** envía automáticamente paquetes de AutoSupport cada hora o cuando ocurran eventos importantes del sistema. Configuración predeterminada: habilitado.
- **Bajo demanda:** Permite que el soporte técnico solicite que tu sistema StorageGRID envíe automáticamente paquetes de AutoSupport, lo cual resulta útil cuando están trabajando activamente en un problema (requiere el protocolo de transmisión HTTPS AutoSupport). Configuración predeterminada: desactivado.
- **Activado por el usuario:** envía manualmente paquetes de AutoSupport en cualquier momento.
- **Recopilación de registros:** ["recopilar manualmente archivos de registro y datos del sistema y enviar un paquete de AutoSupport"](#).

Especifica el protocolo para los paquetes de AutoSupport

Puedes utilizar cualquiera de los siguientes protocolos para enviar paquetes AutoSupport:

- **HTTPS:** Esta es la configuración predeterminada y recomendada para las nuevas instalaciones. Este protocolo utiliza el puerto 443. Si quieres [habilita la función de AutoSupport on Demand](#), debes utilizar HTTPS.
- **HTTP:** Si seleccionas HTTP, debes configurar un servidor proxy para que reenvíe los paquetes de AutoSupport como HTTPS. Los servidores de NetApp AutoSupport rechazan los paquetes enviados mediante HTTP. Este protocolo utiliza el puerto 80.
- **SMTP:** usa esta opción si quieres que los paquetes de AutoSupport se envíen por correo electrónico.

El protocolo que configures se utiliza para enviar todo tipo de paquetes de AutoSupport.

Pasos

1. Selecciona **Soporte > Herramientas > AutoSupport > Configuración**.
2. Selecciona el protocolo que deseas utilizar para enviar paquetes AutoSupport.
3. Si has seleccionado **HTTPS**, indica si deseas utilizar un certificado de soporte de NetApp (certificado TLS) para proteger la conexión con el servidor de soporte técnico.
 - **Verificar certificado** (por defecto): garantiza que la transmisión de paquetes AutoSupport sea segura. El certificado de soporte de NetApp ya viene instalado con el software StorageGRID.

- **No verificar el certificado:** Selecciona esta opción solo cuando tengas una buena razón para no usar la validación del certificado, como cuando haya un problema temporal con un certificado.

4. Selecciona **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 a la semana.

Para saber cuándo se enviará el paquete semanal de AutoSupport, ve a la pestaña **AutoSupport > Results**. En la sección **Weekly AutoSupport**, consulta el valor de **Next Scheduled Time**.

Puedes desactivar el envío automático de los paquetes semanales de AutoSupport en cualquier momento.

Pasos

1. Selecciona **Soporte > Herramientas > AutoSupport > Configuración**.
2. Desmarca la casilla **Habilitar AutoSupport semanal**.
3. Selecciona **Guardar**.

Desactivar AutoSupport activado por eventos

De forma predeterminada, el sistema StorageGRID está configurado para enviar un paquete de AutoSupport al soporte técnico cada hora.

Puedes desactivar AutoSupport activado por eventos en cualquier momento.

Pasos

1. Selecciona **Soporte > Herramientas > AutoSupport > Configuración**.
2. Desmarca la casilla de verificación **Habilitar AutoSupport activado por eventos**.
3. Selecciona **Guardar**.

Habilita AutoSupport bajo demanda

AutoSupport on Demand puede ayudarte a resolver los problemas en los que el soporte técnico esté trabajando activamente.

De forma predeterminada, AutoSupport on Demand está desactivado. Activar esta función permite al soporte técnico solicitar que tu sistema StorageGRID envíe paquetes de AutoSupport de forma automática. El soporte técnico también puede establecer el intervalo de tiempo de sondeo para las consultas de AutoSupport on Demand.

El soporte técnico no puede activar ni desactivar AutoSupport on Demand.

Pasos

1. Selecciona **Soporte > Herramientas > AutoSupport > Configuración**.
2. Selecciona **HTTPS** para el protocolo.
3. Selecciona la casilla **Habilitar AutoSupport semanal**.
4. Selecciona la casilla **Enable AutoSupport on Demand**.
5. Selecciona **Guardar**.

AutoSupport on Demand está activado, y el soporte técnico puede enviar solicitudes de AutoSupport on Demand a StorageGRID.

Desactivar la comprobación de actualizaciones de software

De forma predeterminada, StorageGRID se comunica con NetApp para determinar si hay actualizaciones de software disponibles para tu sistema. Si hay disponible una corrección urgente o una nueva versión de StorageGRID, la nueva versión se muestra en la página de actualización de StorageGRID.

Si lo deseas, puedes desactivar la comprobación de actualizaciones de software. Por ejemplo, si tu sistema no dispone de acceso a la WAN, deberías desactivar la comprobación para evitar errores de descarga.

Pasos

1. Selecciona **Soporte > Herramientas > AutoSupport > Configuración**.
2. Desmarca la casilla **Buscar actualizaciones de software**.
3. Selecciona **Guardar**.

Añade un destino de AutoSupport adicional

Cuando activas AutoSupport, los paquetes de estado y salud se envían al soporte técnico. Puedes especificar un destino adicional para todos los paquetes de AutoSupport.

Para comprobar o cambiar el protocolo utilizado para enviar paquetes de AutoSupport, consulta las instrucciones para [especifica el protocolo para los paquetes de AutoSupport](#).



No puedes usar el protocolo SMTP para enviar paquetes de AutoSupport a un destino adicional.

Pasos

1. Selecciona **Soporte > Herramientas > AutoSupport > Configuración**.
2. Selecciona **Activar destino adicional de AutoSupport**.
3. Especifica lo siguiente:

Nombre de host

El nombre de host o la dirección IP de un servidor de destino adicional de AutoSupport.



Solo puedes introducir un destino adicional.

Puerto

El puerto que se utiliza para conectarse a un servidor de destino adicional de AutoSupport. El valor predeterminado es el puerto 80 para HTTP o el puerto 443 para HTTPS.

Validación del certificado

Si se utiliza un certificado TLS para proteger la conexión con el destino adicional.

- Selecciona **Verificar certificado** para usar la validación de certificados.
- Selecciona **No verificar certificado** para enviar tus paquetes de AutoSupport sin validación del certificado.

Selecciona esta opción solo cuando tengas una buena razón para no utilizar la validación de

certificados, como cuando haya un problema temporal con un certificado.

4. Si seleccionaste **Verificar certificado**, haz lo siguiente:

- a. Busca la ubicación del certificado de la CA.
- b. Sube el archivo del certificado de la CA.

Aparecen los metadatos del certificado de la CA.

5. Selecciona **Guardar**.

Todos los futuros paquetes semanales, activados por eventos y por el usuario de AutoSupport se enviarán al destino adicional.

Configura AutoSupport para dispositivos

AutoSupport para los 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 tanto de problemas de hardware como de software. Debes configurar AutoSupport en cada dispositivo excepto en el SGF6112, que no requiere configuración adicional. AutoSupport se implementa de forma diferente para los dispositivos de servicios y los dispositivos de almacenamiento.

Usa SANtricity para habilitar AutoSupport en cada dispositivo de almacenamiento. Puedes configurar SANtricity AutoSupport durante la configuración inicial del dispositivo o después de que se haya instalado:

- Para los dispositivos SG6000 y SG5700, ["configura AutoSupport en SANtricity System Manager"](#)

Los paquetes de AutoSupport de los dispositivos E-Series se pueden incluir en StorageGRID AutoSupport si configuras la entrega de AutoSupport mediante proxy en ["SANtricity System Manager"](#).

StorageGRID AutoSupport no notifica problemas de hardware, como fallos en los módulos DIMM o en las tarjetas de interfaz del host (HIC). Sin embargo, algunos fallos de componentes podrían activar ["alertas de hardware"](#). Para los dispositivos StorageGRID con un controlador de gestión de placa base (BMC), puedes configurar notificaciones por correo electrónico y trampas SNMP para informar de fallos de hardware:

- ["Configura notificaciones por correo electrónico para alertas de BMC"](#)
- ["Configura los ajustes de SNMP para BMC"](#)

Información relacionada

["Soporte de NetApp"](#)

Activar manualmente un paquete de AutoSupport en StorageGRID

Para ayudar al soporte técnico a solucionar problemas con tu sistema StorageGRID, puedes activar manualmente el envío de un paquete de AutoSupport.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes acceso Root u otro permiso de configuración de grid.

Pasos

1. Selecciona **Soporte > Herramientas > AutoSupport**.
2. En la pestaña **Acciones**, selecciona **Enviar AutoSupport activado por el usuario**.

StorageGRID intenta enviar un paquete de AutoSupport al sitio de soporte de NetApp. Si el intento tiene éxito, se actualizan los valores de **Resultado más reciente** y **Hora del último éxito** en la pestaña **Resultados**. Si hay algún problema, el valor de **Resultado más reciente** se actualiza a "Fallido" y StorageGRID no vuelve a intentar enviar el paquete de AutoSupport.

3. Después de 1 minuto, actualiza la página AutoSupport en tu navegador para acceder a los resultados más recientes.



Además, puedes ["recopilar archivos de registro y datos del sistema más exhaustivos"](#) y enviarlos al sitio de soporte de NetApp.

Soluciona problemas de los paquetes StorageGRID AutoSupport

Si un intento de enviar un paquete de AutoSupport falla, el sistema StorageGRID realiza diferentes acciones según el tipo de paquete de AutoSupport. Puedes comprobar el estado de los paquetes de AutoSupport seleccionando **Support > Tools > AutoSupport > Results**.

Cuando el paquete AutoSupport no se envía, aparece "Failed" en la pestaña **Resultados** de la página **AutoSupport**.



Si configuraste un servidor proxy para reenviar paquetes de AutoSupport a NetApp, debes ["Verifica que los parámetros de configuración del servidor proxy sean correctos"](#).

Fallo del paquete semanal de AutoSupport

Si un paquete semanal de AutoSupport no se envía, el sistema StorageGRID realiza las siguientes acciones:

1. Actualiza el atributo «Resultado más reciente» a «Reintentando».
2. Intenta reenviar el paquete de AutoSupport 15 veces cada cuatro minutos durante una hora.
3. Después de una hora de errores en el envío, actualiza el atributo «Resultado más reciente» a «Fallido».
4. Intenta enviar de nuevo un paquete de AutoSupport en la siguiente hora programada.
5. Mantiene la programación habitual 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 vuelva a estar disponible, envía inmediatamente un paquete AutoSupport si no se ha enviado ningún paquete durante siete días o más.

Error en el paquete AutoSupport provocado por el usuario o por un evento

Si un paquete de AutoSupport activado por el usuario o por un evento no se envía correctamente, el sistema StorageGRID toma las siguientes acciones:

1. Muestra un mensaje de error si el error es conocido. Por ejemplo, si un usuario selecciona el protocolo SMTP sin introducir los parámetros de configuración de correo electrónico correctos, 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 volver a enviar el paquete.
3. Registra el error en `nms.log`.

Si se produce un fallo y el protocolo seleccionado es SMTP, comprueba que el servidor de correo electrónico del sistema StorageGRID esté correctamente configurado y que tu servidor de correo electrónico esté en funcionamiento (**Soporte > Alarmas (heredadas) > Configuración de correo electrónico heredada**). Es posible que aparezca el siguiente mensaje de error en la página AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page`.

Aprende cómo ["configurar los ajustes del servidor de correo electrónico"](#).

Corrige un fallo de paquete de AutoSupport

Si se produce un fallo y SMTP es el protocolo seleccionado, comprueba que el servidor de correo electrónico del sistema StorageGRID esté configurado correctamente y que tu servidor de correo electrónico esté funcionando. Es posible que aparezca el siguiente mensaje de error en la página de AutoSupport: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page`.

Envía paquetes de E-Series AutoSupport a través de StorageGRID

Puedes enviar paquetes de AutoSupport de SANtricity System Manager de E-Series al soporte técnico a través de un nodo de administración de StorageGRID en lugar de a través del puerto de gestión del dispositivo de almacenamiento.

Consulta ["AutoSupport de hardware de E-Series"](#) para obtener más información sobre cómo utilizar AutoSupport con los dispositivos de la E-Series.

Antes de empezar

- Has iniciado sesión en el Grid Manager utilizando un ["navegador web compatible"](#).
- Tienes el ["Permiso de administrador de almacenamiento o acceso Root"](#).
- Has configurado SANtricity AutoSupport:
 - Para los dispositivos SG6000 y SG5700, ["configura AutoSupport en SANtricity System Manager"](#)



Debes disponer del firmware 8.70 o superior de SANtricity para acceder a SANtricity System Manager mediante Grid Manager.

Acerca de esta tarea

Los paquetes de E-Series AutoSupport contienen detalles del hardware de almacenamiento y son más específicos que otros paquetes de AutoSupport enviados por el sistema StorageGRID.

Puedes 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 usar el puerto de gestión del dispositivo. AutoSupport packages transmitidos de esta manera son enviados por el ["Remitente preferido Admin Node"](#) y utilizan cualquier ["Configuración del proxy de administrador"](#) que se haya configurado en el Grid Manager.

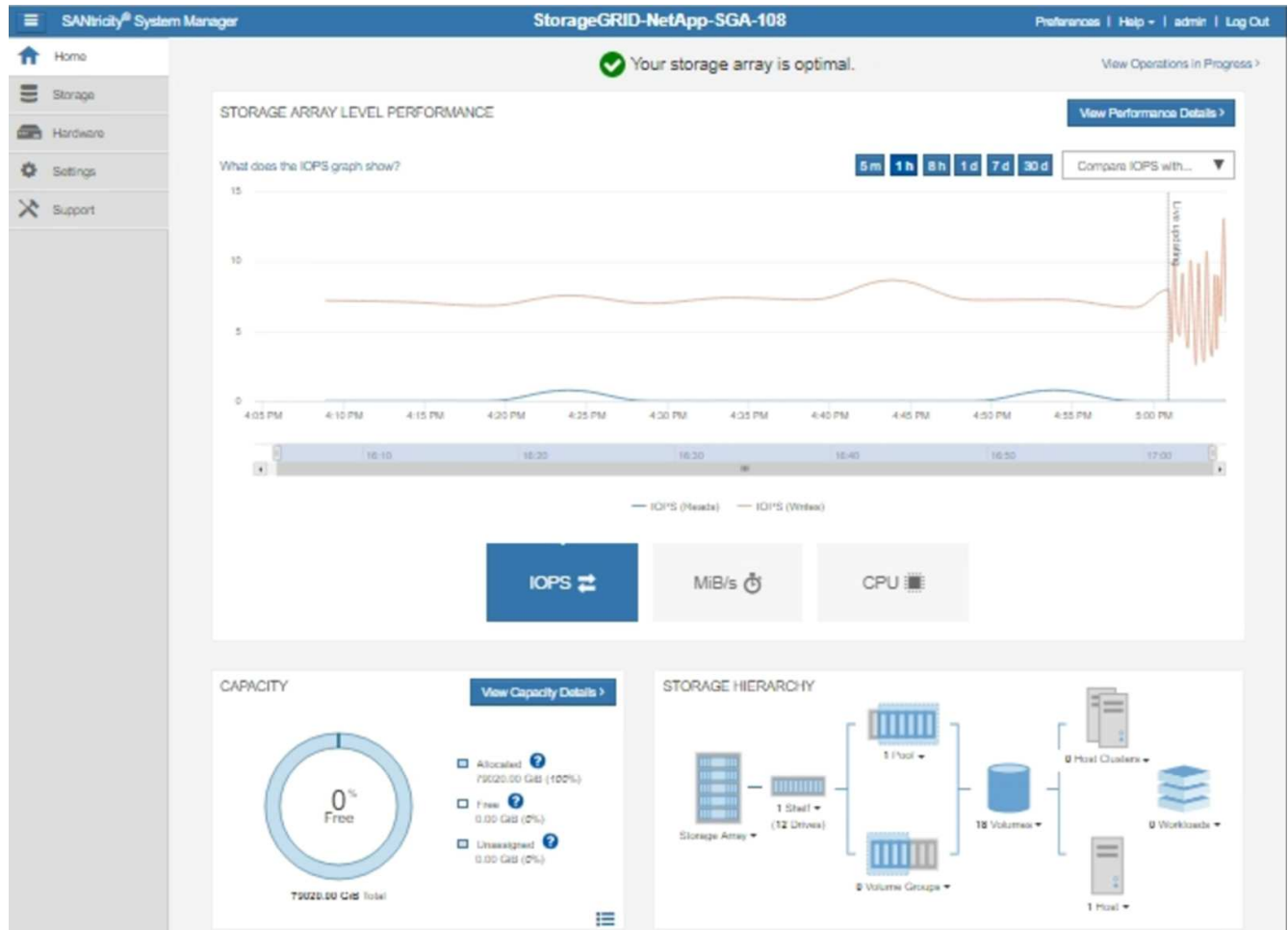


Este procedimiento solo es para configurar un servidor proxy de StorageGRID para paquetes de E-Series AutoSupport. Para obtener más detalles sobre la configuración de E-Series AutoSupport, consulta el ["NetApp E-Series y documentación de SANtricity"](#).

Pasos

1. En el Grid Manager, selecciona **Nodos**.
2. En la lista de nodos de la izquierda, selecciona el nodo del dispositivo de almacenamiento que quieres configurar.
3. Selecciona **SANtricity System Manager**.

Aparece la página de inicio de SANtricity System Manager.



4. Selecciona **Asistencia > Centro de asistencia > 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](#)

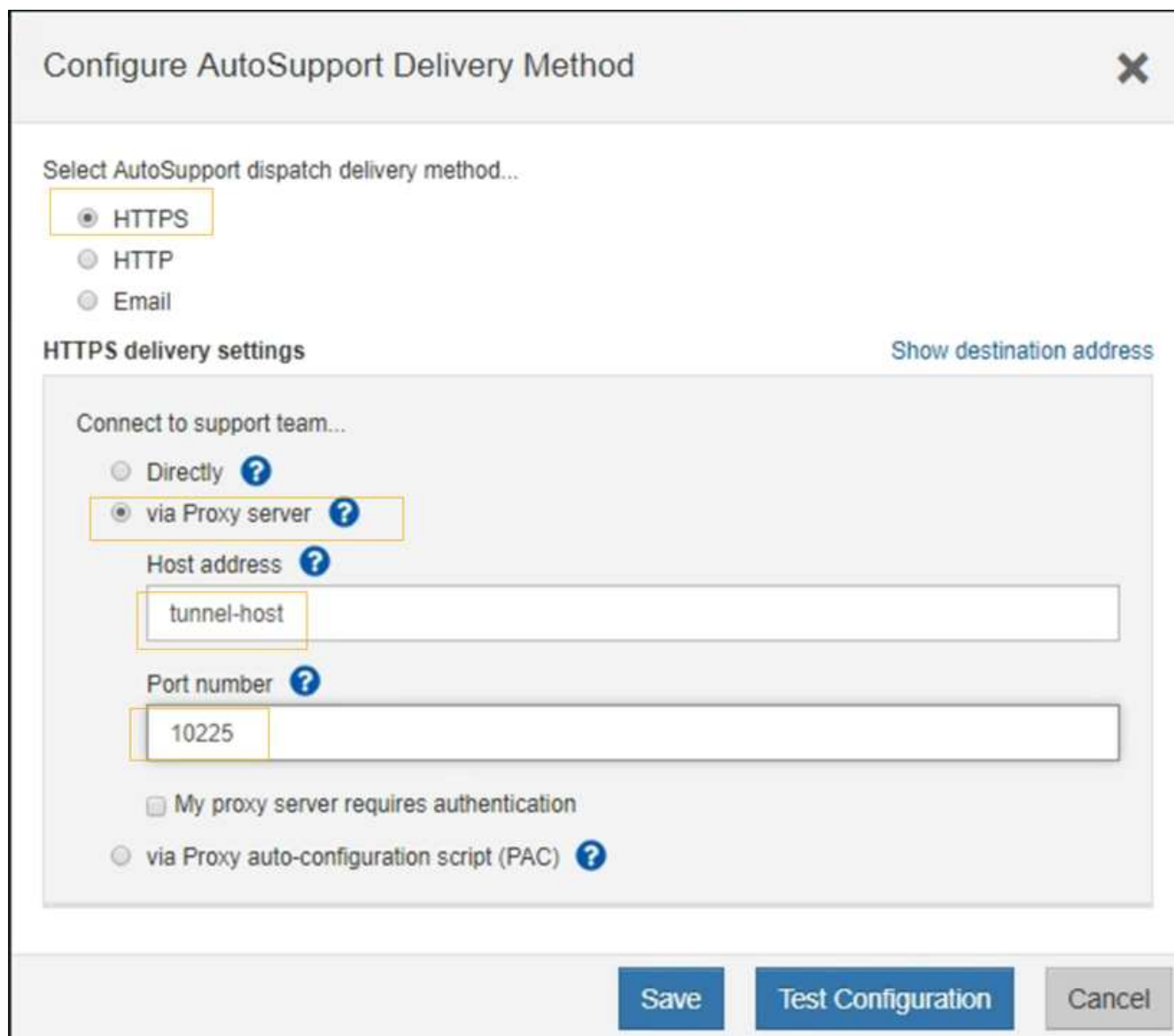
Enable AutoSupport Maintenance window to allow maintenance activities to be performed on the storage array without generating support cases.

[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. Selecciona **Configurar método de entrega de AutoSupport**.

Aparece la página Configurar el método de entrega de AutoSupport.



6. Selecciona **HTTPS** como método de entrega.



El certificado que permite HTTPS viene preinstalado.

7. Selecciona **a través de un servidor proxy**.

8. Introduce `tunnel-host` para el campo **Dirección del servidor**.

`tunnel-host` es la dirección especial que debes usar en un nodo de administración para enviar paquetes E-Series AutoSupport.

9. Introduce `10225` en el campo **Número de puerto**.

`10225` es el número de puerto en el servidor proxy de StorageGRID que recibe los paquetes de AutoSupport del controlador E-Series en el dispositivo.

10. Selecciona **Test Configuration** para probar el enrutamiento y la configuración de tu servidor proxy de AutoSupport.

Si es correcta, aparece un mensaje en un banner verde: "Tu configuración de AutoSupport ha sido verificada."

Si la prueba falla, aparecerá un mensaje de error en un banner rojo. Comprueba la configuración de DNS y la red de StorageGRID, asegúrate de que "[Remitente preferido Admin Node](#)" pueda conectarse al sitio de soporte de NetApp y vuelve a intentar la prueba.

11. Selecciona **Guardar**.

La configuración se guarda y aparece un mensaje de confirmación: «El método de entrega AutoSupport ha sido configurado.»

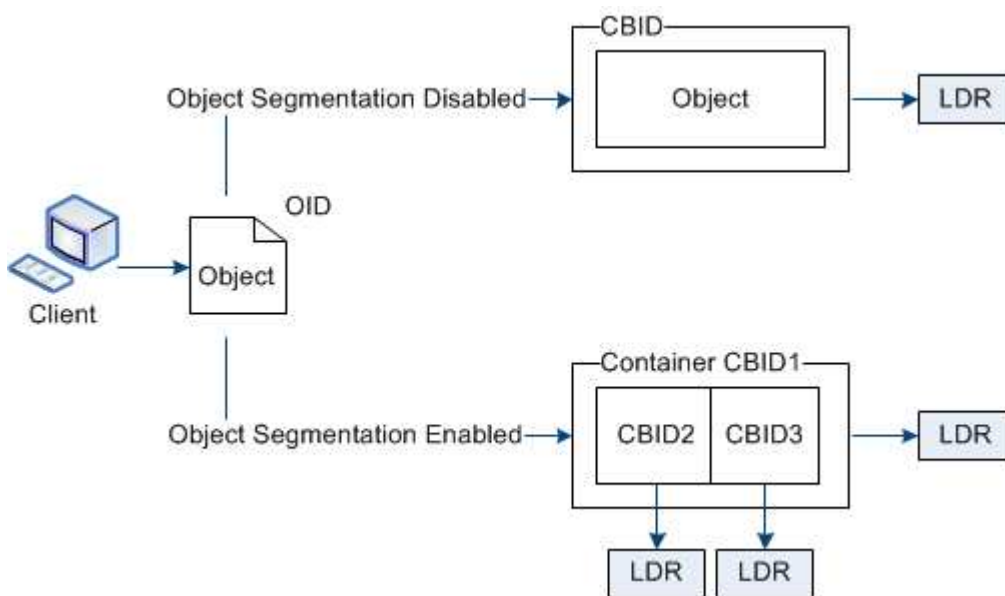
Gestionar nodos de almacenamiento

Usa las opciones de almacenamiento

Conoce la segmentación de objetos en StorageGRID

La segmentación de objetos es el proceso de dividir un objeto en un conjunto de objetos más pequeños de tamaño fijo para optimizar el almacenamiento y el uso de recursos en objetos grandes. La carga multiparte de S3 también crea objetos segmentados, con un objeto que representa cada parte.

Cuando se incorpora un objeto al sistema StorageGRID, el servicio LDR divide el objeto en segmentos y crea un contenedor de segmentos que incluye como contenido la información de cabecera de todos los segmentos.



Al recuperar un contenedor de segmentos, el servicio LDR reconstruye el objeto original a partir de sus segmentos y devuelve el objeto al cliente.

El contenedor y los segmentos no se almacenan necesariamente en el mismo nodo de almacenamiento. El contenedor y los segmentos pueden almacenarse en cualquier nodo de almacenamiento dentro del grupo de almacenamiento especificado en la regla de ILM.

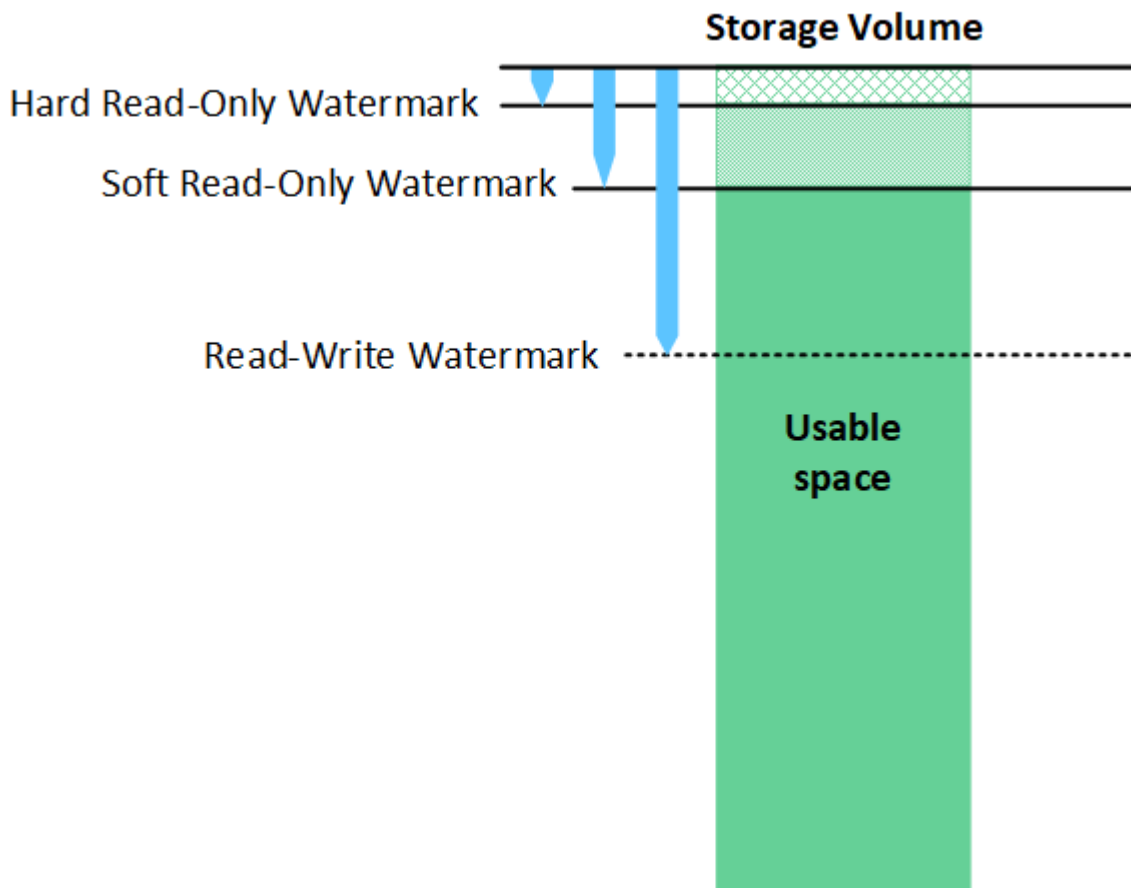
El sistema StorageGRID trata cada segmento de forma independiente y cada uno contribuye al recuento de atributos como Objetos gestionados y Objetos almacenados. Por ejemplo, si un objeto almacenado en el

sistema StorageGRID se divide en dos segmentos, el valor de Objetos gestionados aumenta en tres después de que la ingesta se complete, de la siguiente manera:

segment container + segment 1 + segment 2 = three stored objects

Conoce las marcas de agua de los volúmenes de almacenamiento en StorageGRID

StorageGRID utiliza tres umbrales 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 hayan pasado a un estado de solo lectura vuelvan a estar en modo de lectura/escritura.



Las marcas de agua de volumen de almacenamiento solo se aplican al espacio utilizado para los datos de objetos replicados y con código de borrado. Para obtener más información sobre el espacio reservado para los metadatos de los objetos en el volumen 0, visita ["Gestiona el almacenamiento de metadatos de objetos"](#).

¿Qué es la marca de agua soft de solo lectura?

La **marca de nivel de «solo lectura» del volumen de almacenamiento** es la primera marca que indica que el espacio útil de un Storage Node para datos de objetos se está llenando.

Si cada volumen de un nodo de almacenamiento tiene menos espacio libre que el umbral de solo lectura flexible de dicho volumen, el nodo de almacenamiento pasa al *modo de solo lectura*. El modo de solo lectura

significa que el nodo de almacenamiento ofrece servicios de solo lectura al resto del sistema StorageGRID, pero atiende todas las solicitudes de escritura pendientes.

Por ejemplo, supongamos que cada volumen en un Storage Node tiene un límite flexible de solo lectura de 10 GB. En cuanto cada volumen tenga menos de 10 GB de espacio libre, el Storage Node pasa al modo solo lectura flexible.

¿Qué es la marca de agua de solo lectura estricta?

El **umbral de solo lectura del volumen de almacenamiento** es el siguiente umbral que indica que el espacio utilizable de un nodo para datos de objetos se está llenando.

Si el espacio libre en un volumen es inferior a la marca de agua de solo lectura estricta 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 inferior a sus marcas de agua de solo lectura estricta.

Por ejemplo, supongamos que cada volumen en un Storage Node tiene un límite mínimo de solo lectura de 5 GB. En cuanto cada volumen tenga menos de 5 GB de espacio libre, el Storage Node ya no acepta solicitudes de escritura.

El umbral de solo lectura duro siempre es menor que el umbral de solo lectura blando.

¿Qué es la marca de agua de lectura/escritura?

El **nivel de referencia de lectura/escritura del volumen de almacenamiento** solo se aplica a los nodos de almacenamiento que han pasado al modo de solo lectura. Determina cuándo el nodo puede volver a estar en modo de lectura/escritura. Cuando el espacio libre de cualquier volumen de almacenamiento de un nodo de almacenamiento es superior al nivel de referencia de lectura/escritura de ese volumen, el nodo vuelve automáticamente al estado de lectura/escritura.

Por ejemplo, supongamos que el nodo de almacenamiento ha pasado al modo de solo lectura. Supongamos también que cada volumen tiene un watermark de lectura/escritura de 30 GB. En cuanto el espacio libre de cualquier volumen aumenta a 30 GB, el nodo vuelve a estar en modo de lectura/escritura.

La marca de agua de lectura/escritura siempre es mayor que tanto la marca de agua blanda de solo lectura como la marca de agua dura de solo lectura.

Ver marcas de nivel de agua del volumen de almacenamiento

Puedes consultar la configuración actual de las marcas de agua y los valores optimizados por el sistema. Si no se están utilizando marcas de agua optimizadas, puedes determinar si puedes o debes ajustar la configuración.

Antes de empezar

- Has completado la actualización a StorageGRID 11.6 o una versión posterior.
- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).

Ver la configuración actual de la marca de agua

Puedes consultar la configuración actual de las marcas de agua de almacenamiento en el Grid Manager.

Pasos

1. Selecciona **Support > Other > Storage watermarks**.
2. En la página de marcas de agua de almacenamiento, fíjate en la casilla de selección Usar valores optimizados.
 - Si se marca la casilla, 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 modifiques estos valores. Si lo deseas, puedes [Ver marcas de agua de almacenamiento optimizadas](#).

- Si la casilla «Usar valores optimizados» no está marcada, se están utilizando marcas de agua personalizadas (no optimizadas). No se recomienda utilizar ajustes de marcas de agua personalizadas. Sigue las instrucciones de "[Solución de problemas de alertas de anulación de marcas de agua de solo lectura bajas](#)" para determinar si puedes o debes ajustar la configuración.

Al especificar ajustes personalizados para la marca de agua, debes introducir valores superiores a 0.

Ver marcas de agua de almacenamiento optimizadas

StorageGRID utiliza dos métricas de Prometheus para mostrar los valores optimizados que ha calculado para el umbral de solo lectura (soft) del volumen de almacenamiento. Puedes consultar los valores optimizados mínimos y máximos para cada Storage Node en tu grid.

1. Selecciona **Soporte > Herramientas > Métricas**.
2. En la sección Prometheus, selecciona el enlace para acceder a la interfaz de usuario de Prometheus.
3. Para ver la marca de agua mínima recomendada de solo lectura, introduce la siguiente métrica de Prometheus y selecciona **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 flexible para todos los volúmenes de almacenamiento de cada Storage Node. Si este valor es mayor que el ajuste personalizado de la marca de agua de solo lectura flexible del volumen de almacenamiento, se activa la alerta **Low read-only watermark override** para el Storage Node.

4. Para ver el límite máximo recomendado de marcas de agua soft de solo lectura, introduce la siguiente métrica de Prometheus y selecciona **Execute**:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

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

Administra el almacenamiento de metadatos de objetos en StorageGRID

La capacidad de metadatos de objetos de un sistema StorageGRID controla el número máximo de objetos que se pueden almacenar en ese sistema. Para asegurarte de que tu sistema StorageGRID tenga espacio suficiente para almacenar objetos nuevos, debes comprender dónde y cómo almacena StorageGRID los metadatos de objetos.

¿Qué son los metadatos de un objeto?

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

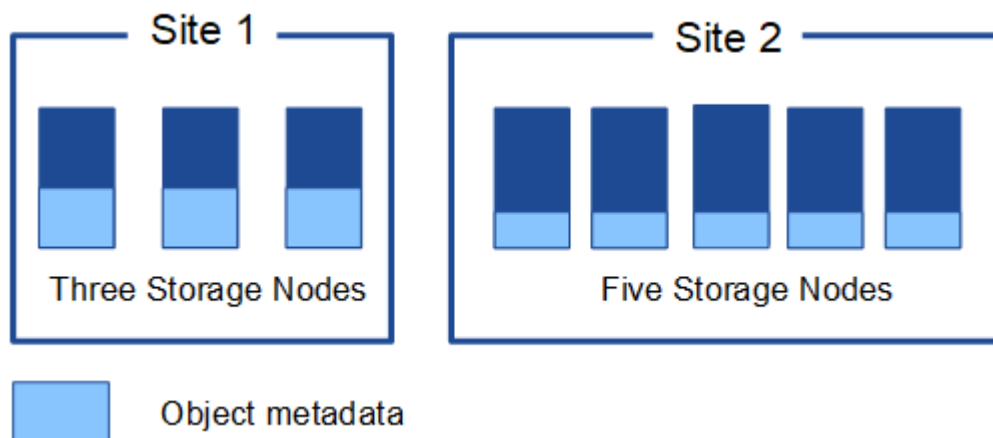
En el caso de un objeto en StorageGRID, los metadatos del objeto incluyen los siguientes tipos de información:

- Metadatos del sistema, incluidos un identificador único para cada objeto (UUID), el nombre del objeto, el nombre del bucket de S3, el nombre o el identificador de la cuenta del tenant, el tamaño lógico del objeto, la fecha y hora en que se creó el objeto por primera vez y la fecha y hora en que se modificó por última vez.
- Cualquier par clave-valor de metadatos de usuario personalizados asociados al objeto.
- Para los objetos de S3, cualquier par clave-valor de etiquetas asociado con el objeto.
- En el caso de las copias replicadas de objetos, la ubicación de almacenamiento actual de cada copia.
- En el caso de las copias de objetos con código de borrado, la ubicación actual de almacenamiento de cada fragmento.
- Para las copias de objetos en un Cloud Storage Pool, la ubicación del objeto, incluyendo el nombre del bucket externo y el identificador único del objeto.
- Para los objetos segmentados y los objetos multiparte, los identificadores de segmento y los tamaños de los datos.

¿Cómo se almacenan los metadatos de los objetos?

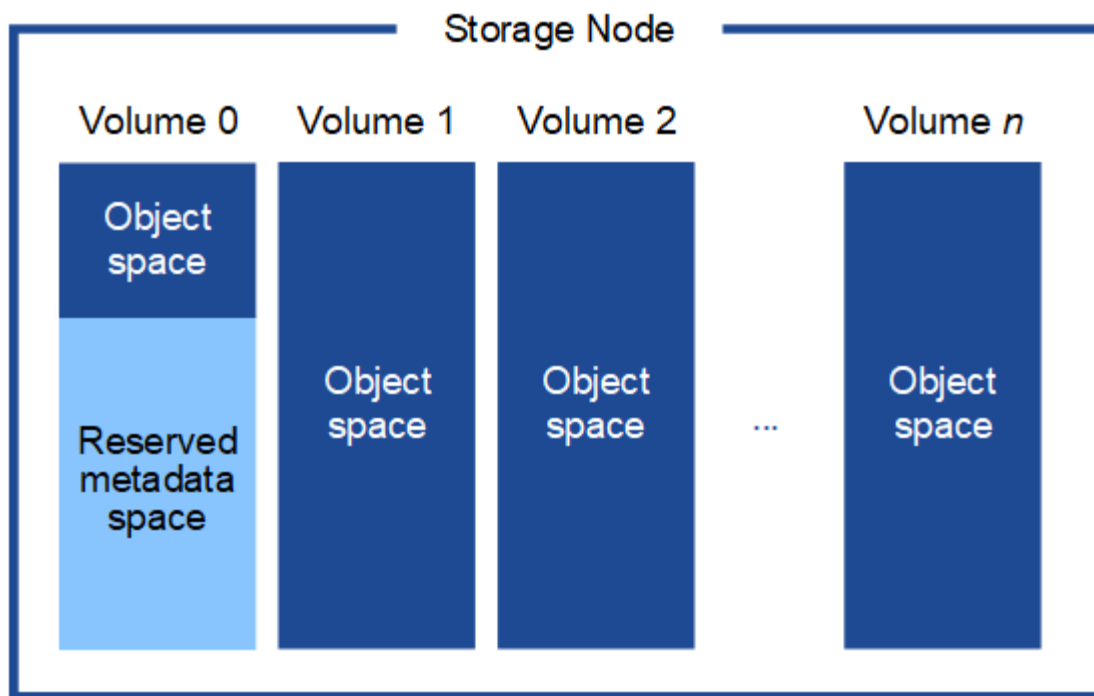
StorageGRID mantiene los metadatos de los objetos en una base de datos Cassandra, que se almacena de forma independiente de los datos de los objetos. Para proporcionar redundancia y proteger los metadatos de los objetos frente a pérdidas, StorageGRID almacena tres copias de los metadatos de todos los 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 de un único 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 Storage Node. Utiliza el espacio reservado para almacenar metadatos de objetos y realizar operaciones esenciales de la base de datos. El espacio restante en el volumen de almacenamiento 0 y todos los demás volúmenes de almacenamiento del Storage Node se utilizan exclusivamente para datos de objetos (copias replicadas y fragmentos con codificación de borrado).

La cantidad de espacio que se reserva para los metadatos de los objetos en un Storage Node concreto depende de varios factores, que se describen a continuación.

Configuración del espacio reservado para metadatos

El *espacio reservado para metadatos* es un ajuste 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 este ajuste se basa en:

- La versión del software que utilizabas cuando instalaste StorageGRID por primera vez.
- La cantidad de RAM de 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 12,0	128 GB o más en cada Storage Node en el grid	8 TB (8.000 GB)
	Menos de 128 GB en cualquier nodo de almacenamiento en el grid	3 TB (3.000 GB)
11.1 a 11.4	128 GB o más en cada nodo de almacenamiento en cualquier centro	4 TB (4.000 GB)

Versión utilizada para la instalación inicial de StorageGRID	Cantidad de RAM en los nodos de almacenamiento	Configuración predeterminada del espacio reservado para metadatos
	Menos de 128 GB en cualquier nodo de almacenamiento de cada emplazamiento	3 TB (3.000 GB)
11.0 o anterior	Cualquier cantidad	2 TB (2.000 GB)

Ver la configuración de espacio reservado para metadatos

Sigue estos pasos para consultar la configuración del espacio reservado para metadatos de tu sistema StorageGRID.

Pasos

1. Selecciona **Configuración > Sistema > Ajustes de almacenamiento**.
2. En la página de configuración de almacenamiento, despliega la sección **Espacio reservado para metadatos**.

En StorageGRID 11.8 o versiones posteriores, el valor del espacio reservado para 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 Storage Node tenga 128 GB o más de RAM es 8,000 GB (8 TB).

Espacio realmente reservado para metadatos

A diferencia de la configuración de espacio reservado para metadatos a nivel de sistema, el *espacio reservado real* para los metadatos de los objetos se determina para cada Storage Node. Para cualquier Storage Node, el espacio reservado real para metadatos depende del tamaño del volumen 0 de ese nodo y de la configuración de espacio reservado para metadatos a nivel de sistema.

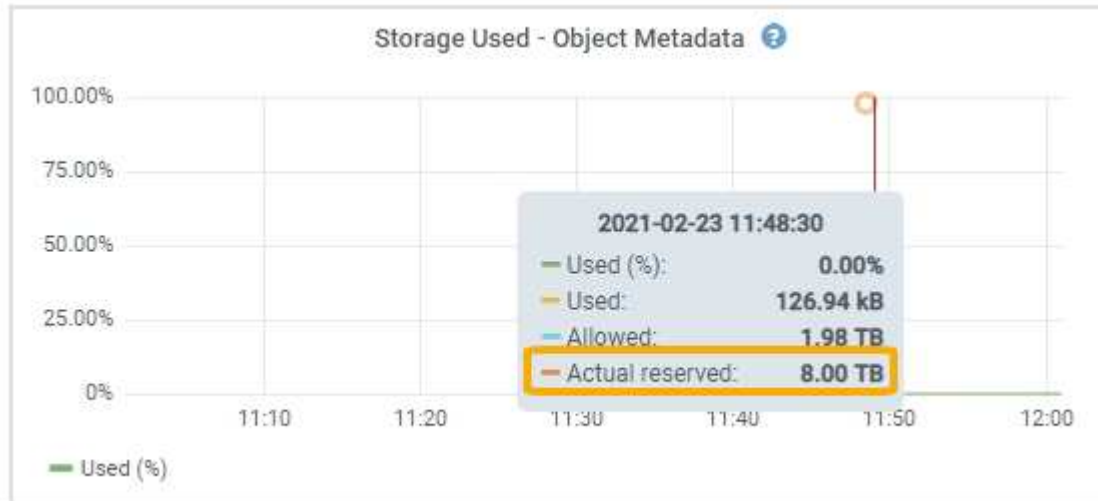
Tamaño del volumen 0 del nodo	Espacio realmente reservado para metadatos
Menos de 500 GB (uso no productivo)	10% del volumen 0
500 GB o más + o + Nodos de almacenamiento solo para metadatos	El menor de estos valores: • Volumen 0 • Configuración del espacio reservado para metadatos Nota: Solo se requiere un rangedb para los nodos de almacenamiento que contienen únicamente metadatos.

Ver el espacio realmente reservado para metadatos

Sigue estos pasos para ver el espacio reservado real para los metadatos en un nodo de almacenamiento concreto.

Pasos

1. Desde el Grid Manager, selecciona **Nodes > Storage Node**.
2. Selecciona la pestaña **Storage**.
3. Coloca el cursor sobre el gráfico «Almacenamiento utilizado - metadatos de objetos» y busca el valor **espacio reservado real**.



En la captura de pantalla, el valor **Reservado real** es de 8 TB. Esta captura de pantalla corresponde a un Storage Node grande en una nueva instalación de StorageGRID 11.6. Como la configuración de espacio reservado para metadatos a nivel de sistema es menor que el volumen 0 de este Storage Node, el espacio reservado real para este nodo es igual a la configuración de espacio reservado para metadatos.

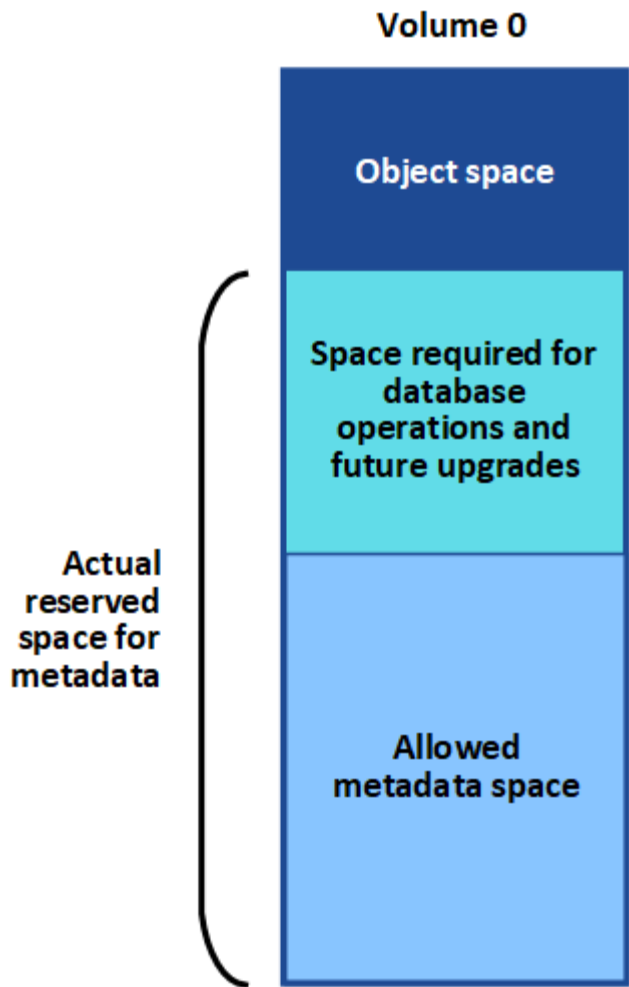
Ejemplo de espacio real reservado para metadatos

Supongamos que instalas un nuevo sistema StorageGRID con la versión 11.7 o posterior. Para este ejemplo, supón que cada Storage Node tiene más de 128 GB de RAM y que el volumen 0 de Storage Node 1 (SN1) es de 6 TB. Según estos valores:

- El **espacio reservado para metadatos** de todo el sistema está configurado en 8 TB. (Este es el valor predeterminado para una nueva instalación de StorageGRID 11.6 o superior si cada Storage Node tiene más de 128 GB de RAM).
- El espacio realmente reservado para los metadatos de SN1 es de 6 TB. (Se reserva todo el volumen porque el volumen 0 es más pequeño que la configuración de **Espacio reservado para metadatos**.)

Espacio permitido para metadatos

El espacio real reservado para los metadatos en cada nodo de almacenamiento se subdivide en el espacio disponible para los metadatos de los objetos (el espacio de metadatos permitido) y el espacio necesario para las operaciones esenciales de la base de datos (como la compactación y la reparación) y las futuras actualizaciones de hardware y software. El espacio de metadatos permitido determina la capacidad total de los objetos.



La siguiente tabla muestra cómo StorageGRID calcula el **espacio permitido para metadatos** de los distintos nodos de almacenamiento, en función de la cantidad de memoria del nodo y del espacio reservado para metadatos.

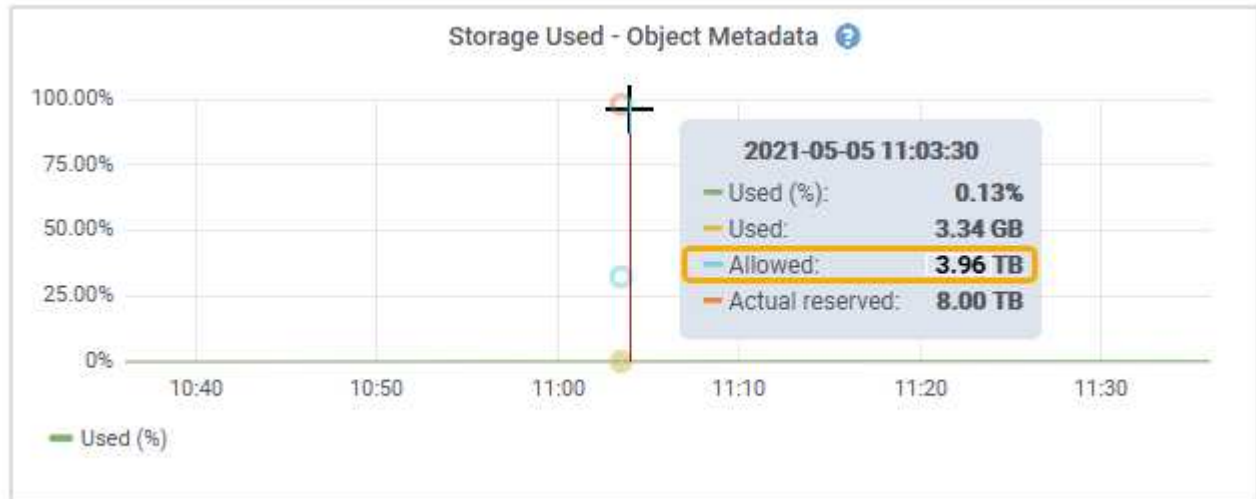
	Cantidad de memoria en el nodo de almacenamiento		
	< 128 GB	>= 128 GB	Espacio realmente reservado para metadatos
≤ 4 TB	60 % del espacio reservado para metadatos, hasta un máximo de 1,32 TB	60 % del espacio reservado para metadatos, hasta un máximo de 1,98 TB	4 TB

Ver el espacio de metadatos permitido

Sigue estos pasos para consultar el espacio de metadatos permitido para un Storage Node.

Pasos

1. Desde el Grid Manager, selecciona **Nodes**.
2. Selecciona el nodo de almacenamiento.
3. Selecciona la pestaña **Storage**.
4. Coloca el cursor sobre el gráfico "Almacenamiento utilizado - metadatos del objeto" y busca el valor **Allowed**.



En la captura de pantalla, el valor **Permitido** es de 3,96 TB, que es el valor máximo para un Storage Node cuyo espacio reservado para metadatos es superior a 4 TB.

El valor **Permitido** se corresponde con esta métrica de Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Ejemplo de espacio permitido para metadatos

Supongamos que instalas un sistema StorageGRID con la versión 11.6. Para este ejemplo, supón que cada nodo de almacenamiento tiene más de 128 GB de RAM y que el volumen 0 del nodo de almacenamiento 1 (SN1) es de 6 TB. Según estos valores:

- El **espacio reservado para metadatos** de todo el sistema está configurado en 8 TB. (Este es el valor predeterminado para StorageGRID 11.6 o superior cuando cada Storage Node tiene más de 128 GB de RAM.)
- El espacio realmente reservado para los metadatos de SN1 es de 6 TB. (Se reserva todo el volumen porque el volumen 0 es más pequeño que la configuración de **Espacio reservado para metadatos**.)
- El espacio permitido para metadatos en SN1 es de 3 TB, según el cálculo que se muestra en la [tabla con el espacio permitido para los metadatos](#): (espacio reservado para metadatos – 1 TB) × 60 %, hasta un máximo de 3,96 TB.

Cómo influyen los nodos de almacenamiento de distintos tamaños en la capacidad de los objetos

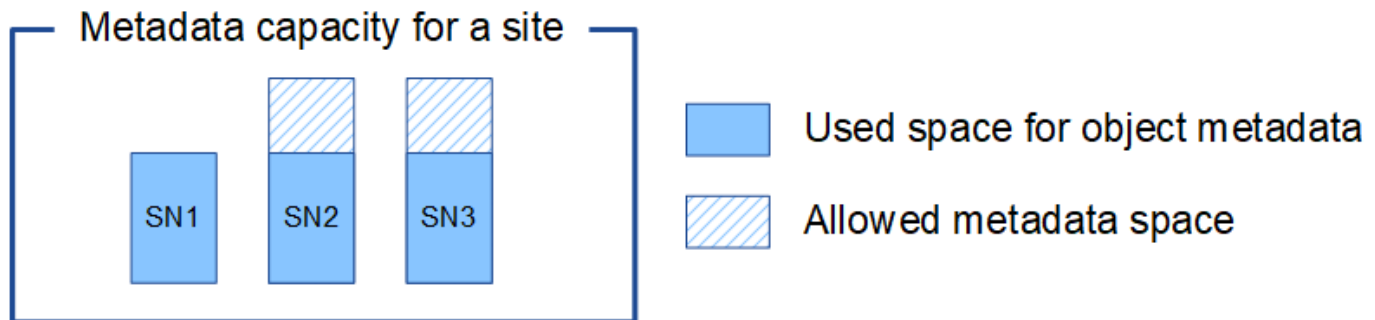
Como se describió anteriormente, StorageGRID distribuye de manera uniforme los metadatos de objetos entre los nodos de almacenamiento de cada sitio. Por este motivo, si un sitio contiene nodos de almacenamiento de diferentes tamaños, el nodo más pequeño del sitio determina la capacidad de metadatos del sitio.

Considera el siguiente ejemplo:

- Tienes una red de un único sitio que contiene tres nodos de almacenamiento de distintos tamaños.
- La opción **Espacio reservado para metadatos** está configurada en 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 reservado real de metadatos	Espacio permitido para metadatos
SN1	2,2 TB	2,2 TB	1,32 TB
SN2	5 TB	4 TB	1,98 TB
SN3	6 TB	4 TB	1,98 TB

Como los metadatos de objetos se distribuyen de manera uniforme entre los nodos de almacenamiento de un sitio, cada nodo de este ejemplo solo puede albergar 1,32 TB de metadatos. No se pueden usar los 0,66 TB adicionales de espacio de metadatos permitido para SN2 y SN3.



Del mismo modo, porque StorageGRID mantiene todos los metadatos de los objetos de un sistema StorageGRID en cada sitio, la capacidad total de metadatos de un sistema StorageGRID se determina por la capacidad de metadatos de objetos del sitio más pequeño.

Y dado que la capacidad de metadatos de los objetos determina el número máximo de objetos, cuando un nodo agota su capacidad de metadatos, la grid está, en efecto, llena.

Información relacionada

- Para saber cómo supervisar la capacidad de metadatos de los objetos de cada Storage Node, consulta las instrucciones para ["Supervisión de StorageGRID"](#).
- Para aumentar la capacidad de metadatos de objetos de tu sistema, ["expandir una grid"](#) añadiendo nuevos Storage Nodes.

Aumenta la configuración de espacio reservado para metadatos en StorageGRID

Es posible que puedas aumentar el parámetro del sistema Espacio reservado para metadatos si tus Storage Nodes cumplen requisitos específicos de RAM y espacio disponible.

Lo que necesitas

- Has iniciado sesión en Grid Manager usando una ["navegador web compatible"](#).

- Tienes el ["Permiso de acceso root o el permiso de otra configuración de grid"](#).

Acerca de esta tarea

Es posible que puedas aumentar manualmente el valor de Espacio reservado para metadatos a nivel de sistema hasta 8 TB.

Solo puedes aumentar el valor de la configuración de Espacio reservado para metadatos a nivel del sistema si ambas afirmaciones son verdaderas:

- Los nodos de almacenamiento de cualquier sitio de tu sistema cuentan cada uno con 128 GB o más de RAM.
- Los nodos de almacenamiento de cualquier sitio en tu sistema tienen suficiente espacio disponible en el volumen de almacenamiento 0.

Ten en cuenta que, si aumentas este parámetro, reducirás al mismo tiempo el espacio disponible para el almacenamiento de objetos en el volumen de almacenamiento 0 de todos los Storage Nodes. Por este motivo, es posible que prefieras establecer el espacio reservado para metadatos en un valor inferior a 8 TB, según tus necesidades previstas de metadatos de objetos.



En general, es mejor utilizar un valor más alto que uno más bajo. Si el valor de «Espacio reservado para metadatos» es demasiado alto, puedes reducirlo más adelante. Por el contrario, si aumentas el valor más adelante, es posible que el sistema tenga que mover datos de objetos para liberar espacio.

Para obtener una explicación detallada de cómo la configuración «Espacio reservado para metadatos» afecta al espacio permitido para el almacenamiento de metadatos de objetos en un Storage Node concreto, consulta ["Gestiona el almacenamiento de metadatos de objetos"](#).

Pasos

1. Determina la configuración actual del Espacio reservado para metadatos.
 - a. Selecciona **Configuración > Sistema > Ajustes de almacenamiento**.
 - b. Toma nota del valor de **Espacio reservado para metadatos**.
2. Asegúrate de que tienes suficiente espacio disponible en el volumen de almacenamiento 0 de cada Storage Node para aumentar este valor.
 - a. Selecciona **Nodos**.
 - b. Selecciona el primer nodo de almacenamiento en la cuadrícula.
 - c. Selecciona la pestaña Storage.
 - d. En la sección Volumes, busca la entrada **/var/local/rangedb/0**.
 - e. Comprueba que el valor Disponible sea igual o superior a la diferencia entre el nuevo valor que deseas utilizar y el valor actual de Espacio reservado para metadatos.

Por ejemplo, si el valor actual de la opción «Espacio reservado para metadatos» es de 4 TB y quieres aumentarlo a 6 TB, el valor de «Disponible» debe ser de 2 TB o más.

- f. Repite 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 continúes con este procedimiento.
 - Si cada nodo de almacenamiento tiene suficiente espacio disponible en el volumen 0, pasa al siguiente paso.

3. Asegúrate de que cada nodo de almacenamiento cuente con al menos 128 GB de RAM.
 - a. Selecciona **Nodos**.
 - b. Selecciona el primer nodo de almacenamiento en la cuadrícula.
 - c. Selecciona la pestaña **Hardware**.
 - d. Pasa el cursor sobre el gráfico de uso de memoria. Asegúrate de que **Total Memory** sea de al menos 128 GB.
 - e. Repite 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 de Espacio reservado para metadatos. No continúes con este procedimiento.
 - Si cada nodo de almacenamiento tiene al menos 128 GB de memoria total, pasa al siguiente paso.
4. Actualiza la configuración del Espacio reservado para metadatos.
 - a. Selecciona **Configuración > Sistema > Ajustes de almacenamiento**.
 - b. Selecciona **Espacio reservado para metadatos**.
 - c. Introduce el nuevo valor.

Por ejemplo, para introducir 8 TB, que es el valor máximo admitido, escribe **8000000000000** (8 seguido de 12 ceros)
 - d. Selecciona **Guardar**.

Comprime objetos almacenados en StorageGRID

Puedes activar la compresión de objetos para reducir el tamaño de los objetos almacenados en StorageGRID, de modo que estos ocupen menos espacio de almacenamiento.

Antes de empezar

- Has 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 desactivada. Si activas la compresión, StorageGRID intenta comprimir cada objeto al guardarlo, utilizando una compresión sin pérdidas.



Si modificas esta configuración, la nueva configuración tardará aproximadamente un minuto en aplicarse. El valor configurado se almacena en caché para mejorar el rendimiento y la escalabilidad.

Antes de activar la compresión de objetos, ten en cuenta lo siguiente:

- No debes seleccionar la opción **Comprimir objetos almacenados** a menos que sepas que los datos que se van a almacenar son comprimibles.
- Las aplicaciones que guardan objetos en StorageGRID pueden comprimir objetos antes de guardarlos. Si una aplicación cliente ya ha comprimido un objeto antes de guardarlo en StorageGRID, seleccionar esta opción no reducirá aún más el tamaño del objeto.
- No selecciones **Comprimir objetos almacenados** si estás usando NetApp FabricPool con StorageGRID.

- Si se selecciona **Comprimir objetos almacenados**, las aplicaciones cliente de S3 deben evitar realizar operaciones GetObject que especifiquen que se devuelva un rango de bytes. Estas operaciones de "lectura de rango" son ineficientes porque StorageGRID debe descomprimir 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, resulta ineficiente leer un rango de 10 MB de un objeto comprimido de 50 GB.

Si los rangos se leen de objetos comprimidos, las solicitudes de los clientes pueden agotar el tiempo de espera.



Si necesitas comprimir objetos y tu aplicación cliente debe utilizar lecturas por rango, aumenta el tiempo de espera de lectura de la aplicación.

Pasos

1. Selecciona **Configuración > Sistema > Storage settings > Object compression**.
2. Marca la casilla **Comprimir objetos almacenados**.
3. Selecciona **Guardar**.

Gestiona nodos de almacenamiento completos en StorageGRID

A medida que los nodos de almacenamiento alcanzan su capacidad, debes ampliar el sistema StorageGRID añadiendo nuevo almacenamiento. Hay tres opciones disponibles: añadir volúmenes de almacenamiento, añadir bandejas de expansión de almacenamiento y añadir nodos de almacenamiento.

Agregar volúmenes de almacenamiento

Cada nodo de almacenamiento admite un número máximo de volúmenes de almacenamiento. El máximo definido varía según la plataforma. Si un nodo de almacenamiento tiene menos volúmenes de almacenamiento que el número máximo, puedes añadir volúmenes para aumentar su capacidad. Consulta las instrucciones para "[Ampliar un sistema StorageGRID](#)".

Agrega bandejas de expansión de almacenamiento

Algunos nodos de almacenamiento de los dispositivos StorageGRID, como el SG6060 o el SG6160, pueden admitir bandejas de almacenamiento adicionales. Si tienes dispositivos StorageGRID con capacidad de expansión que aún no se han ampliado a la capacidad máxima, puedes añadir bandejas de almacenamiento para aumentar la capacidad. Consulta las instrucciones para "[Ampliar un sistema StorageGRID](#)".

Agregar nodos de almacenamiento

Puedes aumentar la capacidad de almacenamiento añadiendo Storage Nodes. Al añadir almacenamiento, debes tener muy en cuenta las reglas de ILM actualmente activas y los requisitos de capacidad. Consulta las instrucciones para "[Ampliar un sistema StorageGRID](#)".

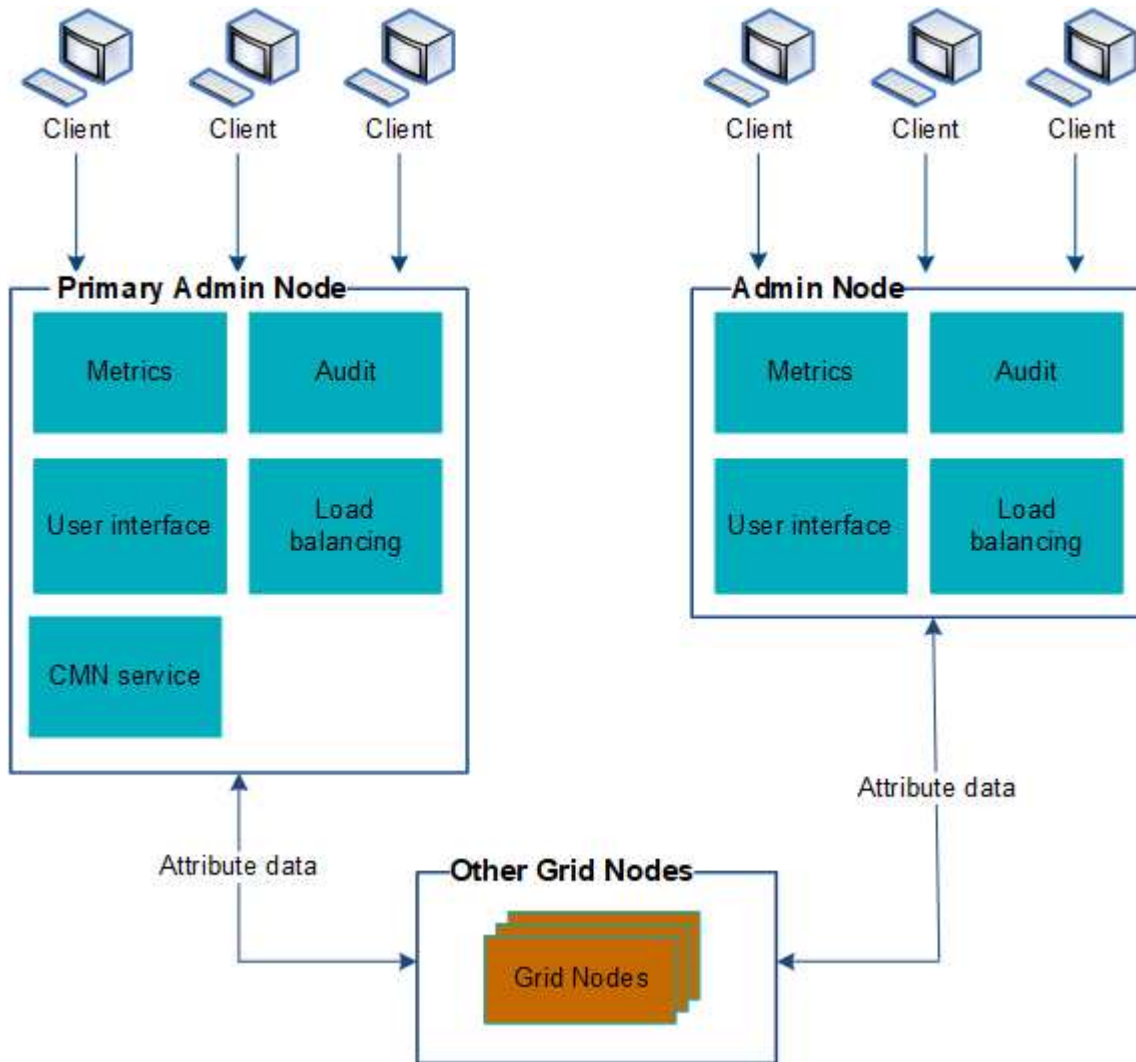
Gestionar nodos de administración

Usa varios nodos de administración en StorageGRID

Un sistema StorageGRID puede incluir varios nodos de administración para que puedas supervisar y configurar tu sistema StorageGRID de forma continua, incluso si falla uno de

los nodos de administración.

Si un nodo de administración deja de estar disponible, el procesamiento de atributos continúa, las alertas siguen activándose y las notificaciones por correo electrónico y los paquetes de AutoSupport siguen enviándose. Sin embargo, disponer de varios nodos de administración no ofrece protección frente a fallos, salvo en lo que respecta a las notificaciones y a los paquetes de AutoSupport.



Existen dos opciones para seguir visualizando y configurando el sistema StorageGRID en caso de que falle un nodo de administración:

- Los clientes web pueden volver a conectarse 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 Grid Manager o al Tenant Manager usando la dirección IP virtual del grupo de alta disponibilidad. Consulta ["Gestiona grupos de alta disponibilidad"](#).



Cuando se utiliza un grupo de alta disponibilidad (HA), el acceso se interrumpe si el nodo de administración activo falla. Los usuarios deben volver a iniciar sesión después de que la dirección IP virtual del grupo de alta disponibilidad falle y pase a otro nodo de administración del grupo.

Algunas tareas de mantenimiento solo pueden realizarse mediante el nodo de administración principal. Si el

nodo de administración principal falla, debe recuperarse antes de que el sistema StorageGRID vuelva a estar plenamente operativo.

Identifica el nodo de administración principal en StorageGRID

El nodo de administración principal ofrece más funcionalidades 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, consulta "[¿Qué es un nodo de administración?](#)".

Antes de empezar

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

Pasos

1. Selecciona **Nodos**.
2. Escribe **primario** en el cuadro de búsqueda.

En los resultados de la búsqueda, identifica el nodo que aparece como "Primary Admin Node" en la columna Tipo. Debería aparecer un único Primary Admin Node.

Gestiona objetos con ILM

Administra objetos con ILM en StorageGRID

Las reglas de gestión del ciclo de vida de la información (ILM) en una política de ILM le indican a StorageGRID cómo crear y distribuir copias de los datos de los objetos y cómo gestionar 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 minuciosa. Debes conocer tus requisitos operativos, la topología de tu sistema StorageGRID, tus 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.

Sigue estas instrucciones para:

- Descubre más sobre StorageGRID ILM, incluida "[cómo funciona ILM a lo largo de la vida de un objeto](#)".
- Descubre cómo configurar "[grupos de almacenamiento](#)", "[Grupos de almacenamiento en la nube](#)" y "[Reglas de ILM](#)".
- Descubre cómo "[crear, simular y activar una política de ILM](#)" que protegerá los datos de objetos en uno o varios sitios.
- Descubre cómo "[gestionar objetos con S3 Object Lock](#)", lo que ayuda a garantizar que los objetos en buckets específicos de S3 no se eliminen ni se sobrescriban durante un periodo de tiempo determinado.

Más información

Para obtener más información, echa un vistazo a estos vídeos:

[Resumen de las reglas de ILM](#)

[Resumen de las políticas de ILM](#)

ILM y el ciclo de vida de los objetos

Cómo funciona ILM a lo largo de la vida de un objeto en StorageGRID

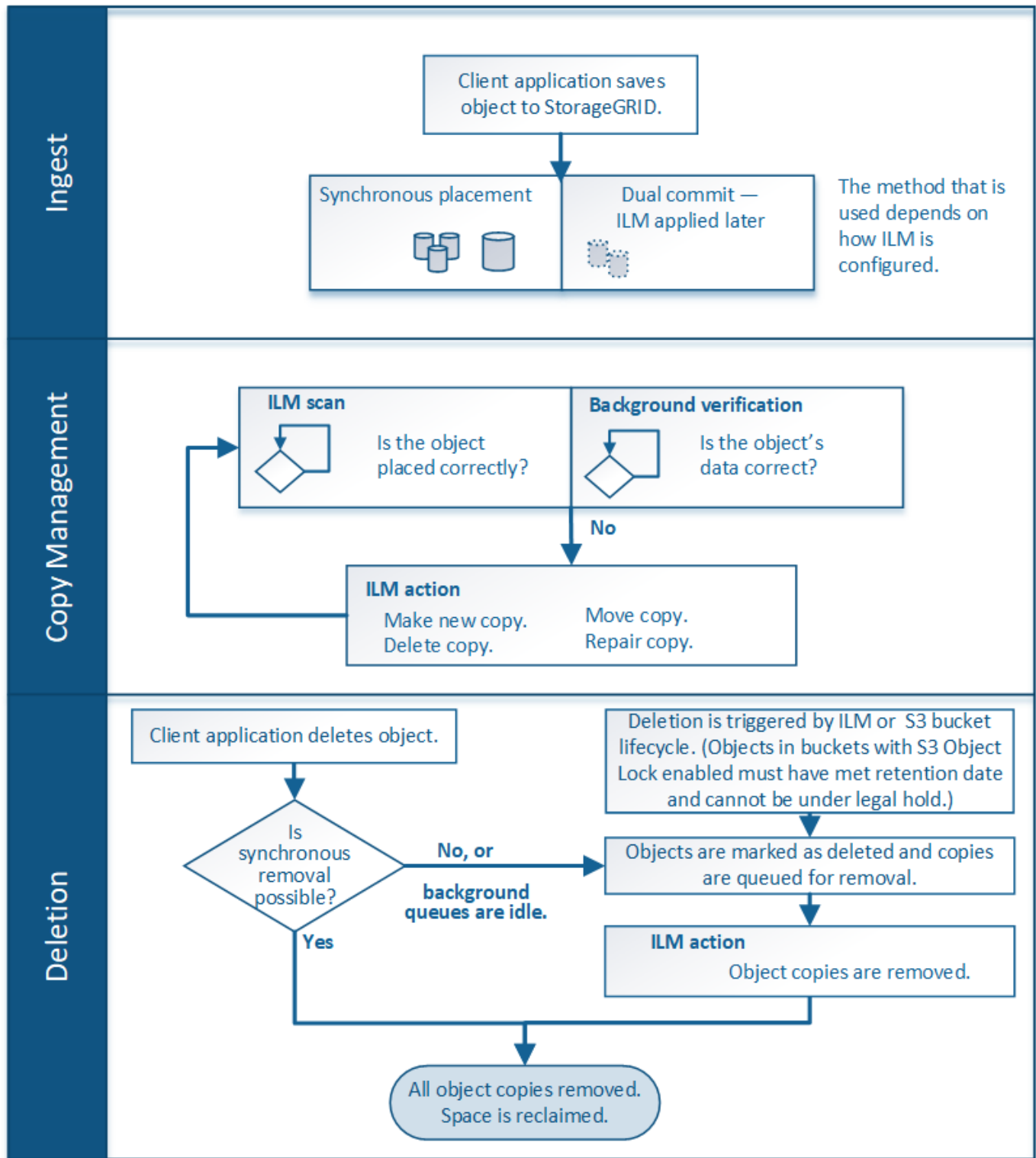
Comprender cómo StorageGRID utiliza ILM para gestionar los objetos en cada etapa de su ciclo de vida puede ayudarte a diseñar una política más eficaz.

- **Ingesta:** La ingesta comienza cuando una aplicación cliente de S3 establece una conexión para guardar un objeto en el sistema StorageGRID, y finaliza cuando StorageGRID devuelve al cliente un mensaje de «ingesta realizada con éxito». Los datos de los objetos quedan protegidos durante la ingesta, ya sea aplicando inmediatamente las instrucciones de ILM (colocación síncrona) o creando copias provisionales y aplicando ILM posteriormente (confirmación dual), en función de cómo se hayan especificado los requisitos de ILM.
- **Gestión de copias:** Después de crear el número y tipo de copias de objetos que se especifican en las instrucciones de ubicación del ILM, StorageGRID gestiona las ubicaciones de los objetos y los protege contra la pérdida.
 - **Análisis y evaluación de ILM:** StorageGRID analiza continuamente la lista de objetos almacenados en la red y comprueba si las copias actuales cumplen los requisitos de ILM. Cuando se requieren diferentes tipos, cantidades o ubicaciones de copias de los objetos, StorageGRID crea, elimina o desplaza copias según sea necesario.
 - **Verificación en segundo plano:** StorageGRID realiza continuamente verificaciones en segundo plano para comprobar la integridad de los datos de los objetos. Si se detecta algún problema, StorageGRID crea automáticamente una nueva copia del objeto o un fragmento de objeto sustitutivo con código de borrado en una ubicación que cumpla con los requisitos actuales de ILM. Consulta "[Verifica la integridad del objeto](#)".
- **Eliminación de objetos:** La gestión de un objeto finaliza cuando se eliminan todas sus copias del sistema StorageGRID. Los objetos pueden eliminarse como resultado de una solicitud de eliminación por parte de un cliente, de una eliminación realizada por ILM o de una eliminación causada por la expiración del ciclo de vida de un bucket de S3.



Los objetos de un bucket en el que se haya habilitado S3 Object Lock no se pueden eliminar si están sujetos a una retención legal o si se ha especificado una fecha límite de retención que aún no se haya alcanzado.

El diagrama resume cómo funciona ILM a lo largo del ciclo de vida de un objeto.



Cómo se ingieren los objetos

Opciones de ingestión de ILM en StorageGRID

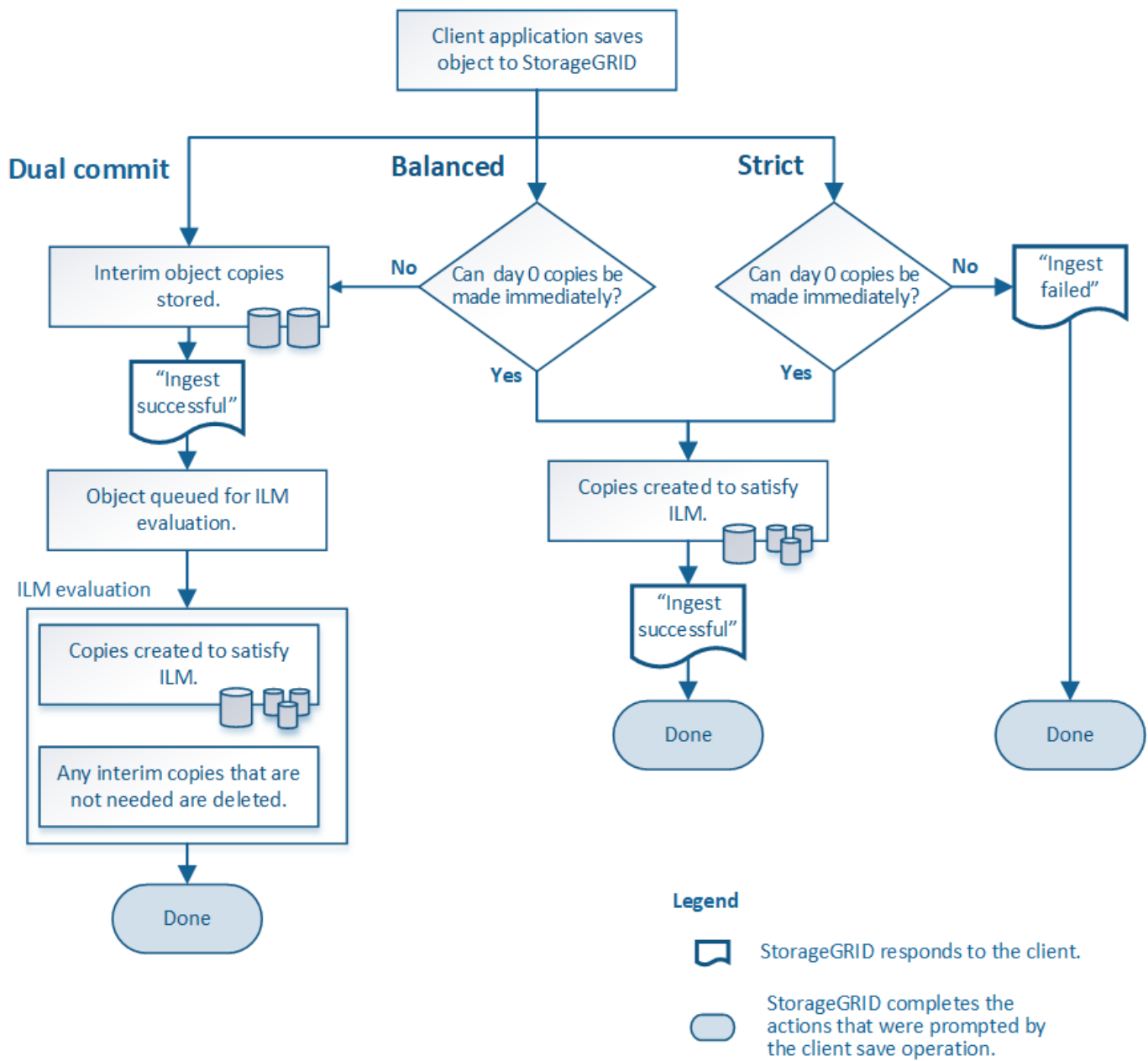
Cuando creas una regla de ILM, especificas una de tres opciones para proteger los objetos al momento de la ingesta: Dual commit, Strict o Balanced.

En función de la opción que elijas, StorageGRID crea copias provisionales y pone los objetos en cola para su

posterior evaluación ILM, o bien utiliza la colocación sincrónica y crea copias de inmediato para cumplir los requisitos ILM.

Diagrama de flujo de las opciones de ingestión

El diagrama de flujo muestra lo que ocurre cuando los objetos coinciden con una regla de ILM que utiliza cada una de las tres opciones de ingesta.



Confirmación doble

Al seleccionar la opción «Dual commit», StorageGRID crea inmediatamente copias provisionales del objeto en dos nodos de almacenamiento diferentes y devuelve al cliente un mensaje de «ingesta realizada con éxito». El objeto se pone en cola para su evaluación por parte de ILM, y las copias que cumplen con las instrucciones de ubicación de la regla se crean después. Si la política de ILM no se puede procesar inmediatamente después del dual commit, la protección contra la pérdida de un sitio podría tardar en lograrse.

Utiliza la opción Dual commit en cualquiera de estos casos:

- Estás utilizando reglas de ILM multisitio y la latencia en la ingesta de los clientes es tu principal consideración. Al utilizar Dual commit, debes asegurarte de que tu grid pueda realizar el trabajo adicional de crear y eliminar las copias de dual commit si no cumplen con ILM. En concreto:
 - La carga en la grid debe ser lo suficientemente baja como para evitar un retraso de ILM.
 - La red debe disponer de recursos de hardware de sobra (IOPS, CPU, memoria, ancho de banda de red, etc.).
- Estás utilizando reglas de ILM multisitio y la conexión WAN entre los sitios suele presentar una latencia elevada o un ancho de banda limitado. En este caso, usar la opción Dual commit puede ayudar a evitar los tiempos de espera de los clientes. Antes de elegir la opción Dual commit, deberías probar la aplicación cliente con cargas de trabajo realistas.

Equilibrado (predeterminado)

Al seleccionar la opción «Equilibrada», StorageGRID también utiliza la colocación sincrónica durante la ingesta y crea inmediatamente todas las copias especificadas en las instrucciones de colocación de la regla. A diferencia de la opción «Estricta», si StorageGRID no puede crear todas las copias de forma inmediata, utiliza en su lugar la confirmación dual. Si la política de ILM utiliza ubicaciones en varios sitios y no se puede lograr una protección inmediata contra la pérdida de un sitio, se activa la alerta **ILM placement unachievable**.

Utiliza la opción «Equilibrada» para conseguir la mejor combinación de protección de datos, rendimiento del grid y éxito en la ingesta. «Equilibrada» es la opción predeterminada en el asistente para crear reglas de ILM.

Estricto

Al seleccionar la opción Strict, StorageGRID utiliza la colocación sincrónica durante la ingesta y crea inmediatamente todas las copias del objeto especificadas en las instrucciones de colocación de la regla. La ingesta falla si StorageGRID no puede crear todas las copias, por ejemplo, porque una ubicación de almacenamiento necesaria no está disponible temporalmente. El cliente debe volver a intentar la operación.

Utiliza la opción Strict si tienes un requisito operativo o normativo que te obligue a almacenar inmediatamente los objetos únicamente en las ubicaciones especificadas en la regla de ILM. Por ejemplo, para cumplir un requisito normativo, es posible que tengas que utilizar la opción Strict y un filtro avanzado de Location Constraint para garantizar que los objetos nunca se almacenen en determinados centros de datos.

Consulta ["Ejemplo 5: normas y política de ILM para un comportamiento de ingesta estricto"](#).

Ventajas, desventajas y limitaciones de las opciones de ingesta de ILM en StorageGRID

Conocer las ventajas y desventajas de cada una de las tres opciones para proteger los datos en el momento de la ingesta (Balanced, Strict o Dual commit) puede ayudarte a decidir cuál elegir para una regla de ILM.

Para obtener una visión general de las opciones de ingestión, consulta ["Opciones de ingesta"](#).

Ventajas de las opciones Equilibrada y Estricta

En comparación con Dual commit, que crea copias provisionales durante la importación, las dos opciones de colocación sincrónica pueden ofrecer las siguientes ventajas:

- **Mayor seguridad de los datos:** Los datos de los objetos quedan protegidos de inmediato según lo especificado en las instrucciones de ubicación de la regla ILM, que pueden configurarse para proteger contra una amplia variedad de situaciones de fallo, incluido el fallo de más de una ubicación de almacenamiento. El dual commit solo puede proteger contra la pérdida de una única copia local.

- **Funcionamiento más eficiente de la red:** Cada objeto se procesa una sola vez, en el momento de su incorporación. Dado que el sistema StorageGRID no necesita realizar un seguimiento ni eliminar copias provisionales, la carga de procesamiento es menor y se consume menos espacio en la base de datos.
- **(Equilibrado) Recomendado:** La opción «Equilibrado» ofrece una eficiencia óptima de ILM. Se recomienda utilizar la opción «Equilibrado» salvo que se requiera un comportamiento de ingesta estricto o que la grid cumpla todos los criterios para utilizar Dual commit.
- **(Estricta) Certeza sobre la ubicación de los objetos:** La opción Estricta garantiza que los objetos se almacenen inmediatamente de acuerdo con las instrucciones de ubicación establecidas en la regla ILM.

Desventajas de las opciones «Balanced» y «Strict»

En comparación con Dual commit, las opciones Balanced y Strict presentan algunas desventajas:

- **Ingestas más largas por parte del cliente:** Las latencias de ingesta del cliente pueden ser mayores. Cuando usas las opciones "Balanced" o "Strict", no se devuelve al cliente un mensaje de "ingesta realizada con éxito" hasta que se hayan creado y almacenado todos los fragmentos con código de borrado o todas las copias replicadas. Sin embargo, es muy probable que los datos del objeto alcancen su ubicación definitiva mucho más rápido.
- **(Estricto) Mayores índices de fallos en la importación:** Con la opción «Estricto», la importación falla siempre que StorageGRID no pueda crear inmediatamente todas las copias especificadas en la regla de ILM. Es posible que veas altos índices de fallos en la importación si una ubicación de almacenamiento necesaria está temporalmente fuera de línea o si los problemas de red provocan retrasos en la copia de objetos entre sitios.
- **(Estricto) En algunas circunstancias, la ubicación de las subidas multiparte a S3 podría no ser la esperada:** con el modo «Estricto», esperas que los objetos se coloquen tal y como describe la regla de ILM o que la ingesta falle. Sin embargo, en una carga multiparte de S3, ILM se evalúa para cada parte del objeto a medida que se ingiere, y para el objeto en su conjunto cuando finaliza la carga multiparte. En las siguientes circunstancias, esto podría dar lugar a ubicaciones diferentes a las que esperas:
 - **Si el ILM cambia mientras se está realizando una subida multiparte a S3:** porque cada parte se almacena según la regla vigente en el momento de su ingesta, es posible que algunas partes del objeto no cumplan los requisitos actuales del ILM cuando finalice la subida multiparte. En estos casos, la ingesta del objeto no falla. En su lugar, cualquier parte que no se haya ubicado correctamente se pone en cola para una reevaluación de ILM y se traslada posteriormente a la ubicación correcta.
 - **Cuando las reglas de ILM filtran por tamaño:** Al evaluar ILM para una parte, StorageGRID filtra en función del tamaño de la parte, no del tamaño del objeto. Esto significa que las partes de un objeto pueden almacenarse en ubicaciones que no cumplen los requisitos de ILM para el objeto en su conjunto. Por ejemplo, si una regla especifica que todos los objetos de 10 GB o más se almacenan en DC1 mientras que todos los objetos más pequeños se almacenan en DC2, al ingerir, cada parte de 1 GB de una carga multiparte de 10 partes se almacena en DC2. Cuando se evalúa ILM para el objeto, todas las partes del objeto se trasladan a DC1.
- **(Estricto) La ingesta no falla cuando se actualizan las etiquetas o los metadatos de un objeto y no es posible realizar las nuevas ubicaciones requeridas:** Con Strict, esperas que los objetos se coloquen tal como lo describe la regla de ILM o que la ingesta falle. Sin embargo, cuando actualizas los metadatos o las etiquetas de un objeto que ya está almacenado en el grid, el objeto no se vuelve a ingerir. Esto significa que cualquier cambio en la ubicación del objeto provocado por la actualización no se realiza de inmediato. Los cambios de ubicación se realizan cuando ILM se vuelve a evaluar mediante los procesos normales de ILM en segundo plano. Si no es posible realizar los cambios de ubicación requeridos (por ejemplo, porque una ubicación recién requerida no está disponible), el objeto actualizado conserva su ubicación actual hasta que sea posible realizar los cambios de ubicación.

Limitaciones en la colocación de objetos con las opciones Balanced y Strict

Las opciones Equilibrada o Estricta no se pueden usar para las reglas de ILM que tengan cualquiera de estas instrucciones de ubicación:

- Ubicación en un Cloud Storage Pool el día 0.
- Asignaciones en un grupo de almacenamiento en la nube cuando la regla tiene como hora de referencia una hora de creación definida por el usuario.

Estas restricciones existen porque StorageGRID no puede realizar copias de forma sincrónica en un Cloud Storage Pool, y una hora de creación definida por el usuario podría corresponder al momento actual.

Cómo interactúan las reglas de ILM y la coherencia para afectar la protección de datos

Tanto la regla de ILM como la opción de consistencia que elijas influyen en la forma en que se protegen los objetos. Estos ajustes pueden interactuar.

Por ejemplo, el comportamiento de ingesta seleccionado para una regla de ILM afecta la ubicación inicial de las copias de los objetos, mientras que la consistencia utilizada al almacenar un objeto afecta la ubicación inicial de los metadatos del objeto. Porque StorageGRID requiere acceso tanto a los datos como a los 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 ofrecer una mejor protección inicial de los datos y respuestas del sistema más predecibles.

Aquí tienes un breve resumen de los valores de consistencia que están disponibles en StorageGRID:

- **Todos:** Todos los nodos reciben los metadatos del objeto de forma inmediata o la solicitud fallará.
- **Strong-global:** garantiza la consistencia de lectura después de escritura para todas las solicitudes de los clientes en todos los sitios. Cuando configuras la semántica de Quorum, se aplican los siguientes comportamientos:
 - Permite la tolerancia a fallos del sitio para las solicitudes de los clientes cuando los grids tienen tres o más sitios. Los grids de dos sitios no tendrán tolerancia a fallos del sitio.
 - Las siguientes operaciones de S3 no se podrán realizar si uno de los sitios está inactivo:
 - DeleteBucketEncryption
 - PutBucketBranch
 - PutBucketEncryption
 - PutBucketVersioning
 - PutObjectLegalHold
 - PutObjectLockConfiguration
 - PutObjectRetention

Si lo necesitas, puedes ["Configura la semántica de quórum de StorageGRID para una consistencia global fuerte"](#).

- **Sitio fuerte:** Los metadatos de los objetos se distribuyen inmediatamente a los demás nodos del sitio. Garantiza la consistencia de lectura tras escritura para todas las solicitudes de los clientes dentro de un sitio.
- **Read-after-new-write:** proporciona coherencia de lectura tras escritura para objetos nuevos y coherencia eventual para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.

- **Disponible:** Proporciona consistencia eventual tanto para los objetos nuevos como para las actualizaciones de objetos. Para los buckets de S3, utilízalo solo cuando sea necesario (por ejemplo, para un bucket que contenga valores de registro que rara vez se leen, o para operaciones HEAD o GET sobre claves que no existen). No es compatible con los buckets de S3 FabricPool.



Antes de seleccionar un valor de consistencia, "[Lee la descripción completa sobre la consistencia](#)". Debes entender los beneficios y las limitaciones antes de cambiar el valor predeterminado.

Ejemplo de cómo la coherencia y las reglas de ILM pueden interactuar

Supongamos que tienes una red de tres sitios con la siguiente regla de ILM y la siguiente consistencia:

- **Regla de ILM:** crea tres copias de objeto, una en el sitio local y otra en cada sitio remoto. Usa el comportamiento de ingesta Strict.
- **Consistencia:** Global fuerte (los metadatos de los objetos se distribuyen inmediatamente a varios sitios).

Cuando un cliente almacena un objeto en la grid, StorageGRID crea las tres copias del objeto y distribuye los metadatos a varios sitios antes de indicar al cliente que la operación se ha realizado con éxito.

El objeto queda totalmente protegido contra la pérdida en el momento en que se recibe el mensaje de ingesta correcta. Por ejemplo, si el sitio local se pierde poco después de la ingesta, siguen existiendo copias tanto de los datos del objeto como de los metadatos del objeto en los sitios remotos. El objeto se puede recuperar íntegramente desde los demás sitios.

Si, por el contrario, usaste la misma regla de ILM y la consistencia de sitio fuerte, el cliente podría recibir un mensaje de éxito después de que los datos del objeto se replican en los sitios remotos, 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. El objeto no se puede recuperar.

La interrelación entre la coherencia y las reglas de ILM puede ser compleja. Ponte en contacto con NetApp si necesitas ayuda.

Información relacionada

["Ejemplo 5: normas y política de ILM para un comportamiento de ingesta estricto"](#)

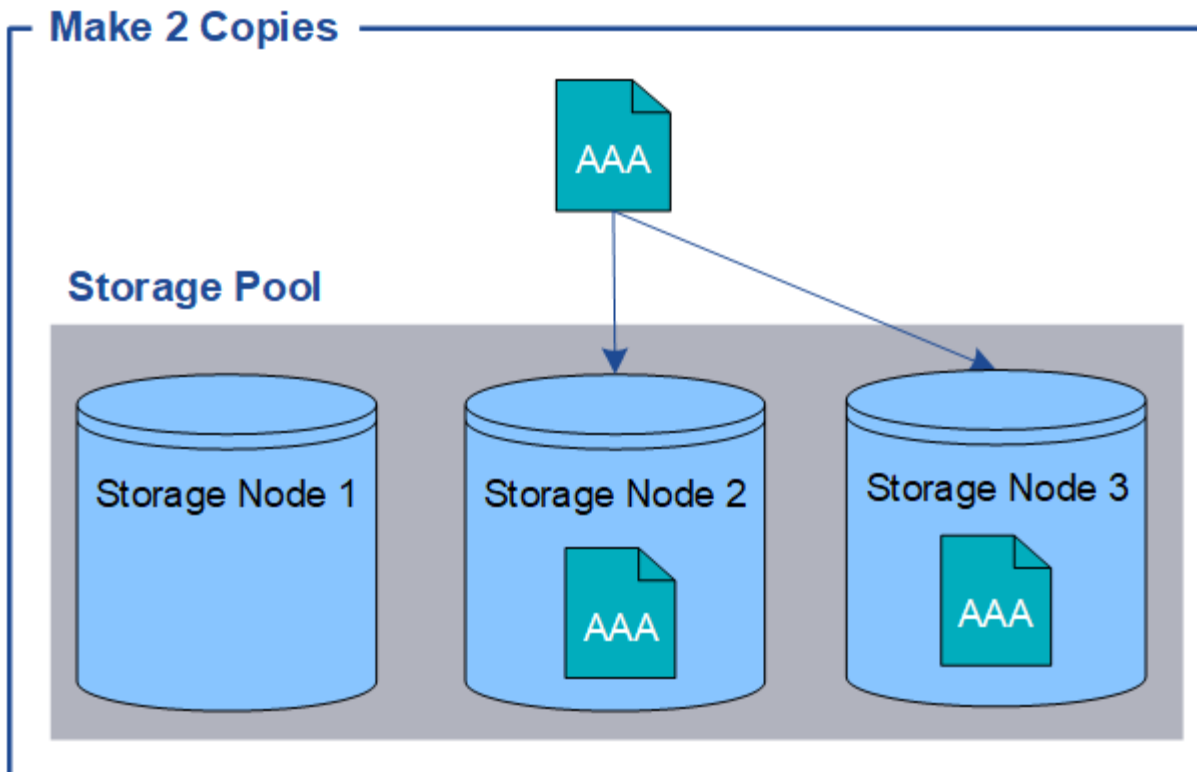
Cómo se almacenan los objetos (replicación o código de borrado)

Conoce la replicación en StorageGRID

La replicación es uno de los dos métodos que utiliza StorageGRID para almacenar datos de objetos (el otro método es el código de borrado). Cuando los objetos cumplen una regla de ILM que utiliza la replicación, el sistema crea copias exactas de los datos de los objetos y las almacena en Storage Nodes.

Al configurar una regla de ILM para crear copias replicadas, especificas cuántas copias deben crearse, dónde deben ubicarse y durante cuánto tiempo deben almacenarse en cada ubicación.

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



Cuando StorageGRID aplica esta regla a los objetos, crea dos copias del objeto y las almacena en dos nodos de almacenamiento distintos del grupo de almacenamiento. Las dos copias pueden ubicarse en cualquiera de los tres nodos de almacenamiento disponibles. En este caso, la regla ha ubicado las copias del objeto en los nodos de almacenamiento 2 y 3. Al haber dos copias, el objeto puede recuperarse si falla cualquiera de los nodos del grupo de almacenamiento.



StorageGRID solo puede almacenar una copia replicada de un objeto en cualquier nodo de almacenamiento. Si tu grid incluye tres nodos de almacenamiento y creas una regla ILM de 4 copias, solo se harán tres copias: una por cada nodo de almacenamiento. La alerta **ILM placement unachievable** se activa para indicar que la regla ILM no se pudo aplicar completamente.

Información relacionada

- ["¿Qué es el erasure coding?"](#)
- ["¿Qué es un storage pool?"](#)
- ["Activar la protección contra la pérdida de sitios mediante la replicación y el código de borrado"](#)

Riesgos de la replicación de una sola copia en StorageGRID

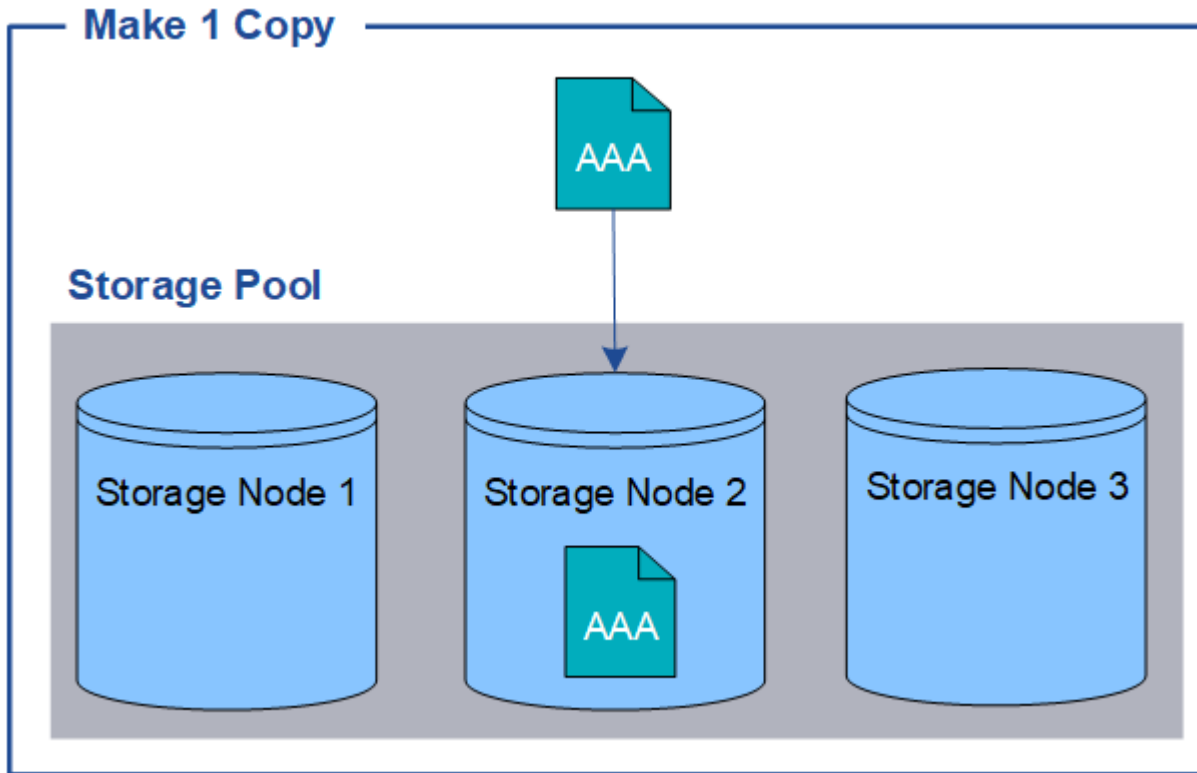
Al crear una regla de ILM para generar copias replicadas, siempre debes especificar al menos dos copias para cualquier periodo de tiempo en las instrucciones de ubicación.



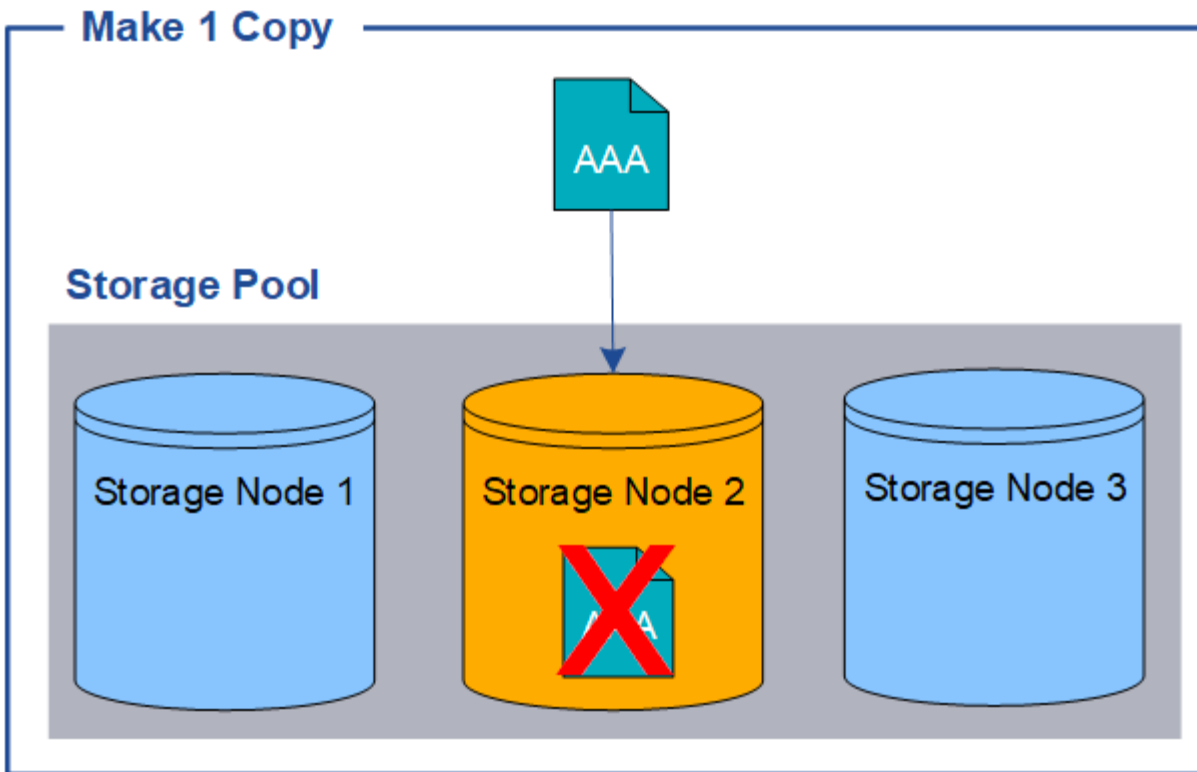
No utilices una regla de ILM que cree una sola copia replicada durante cualquier periodo de tiempo. Si solo existe una copia replicada de un objeto, ese objeto se pierde si un Storage Node falla o tiene un error importante. También perderás temporalmente el acceso al objeto durante procedimientos de mantenimiento como las actualizaciones.

En el siguiente ejemplo, la regla ILM «Make 1 Copy» especifica que se coloque una copia replicada de un

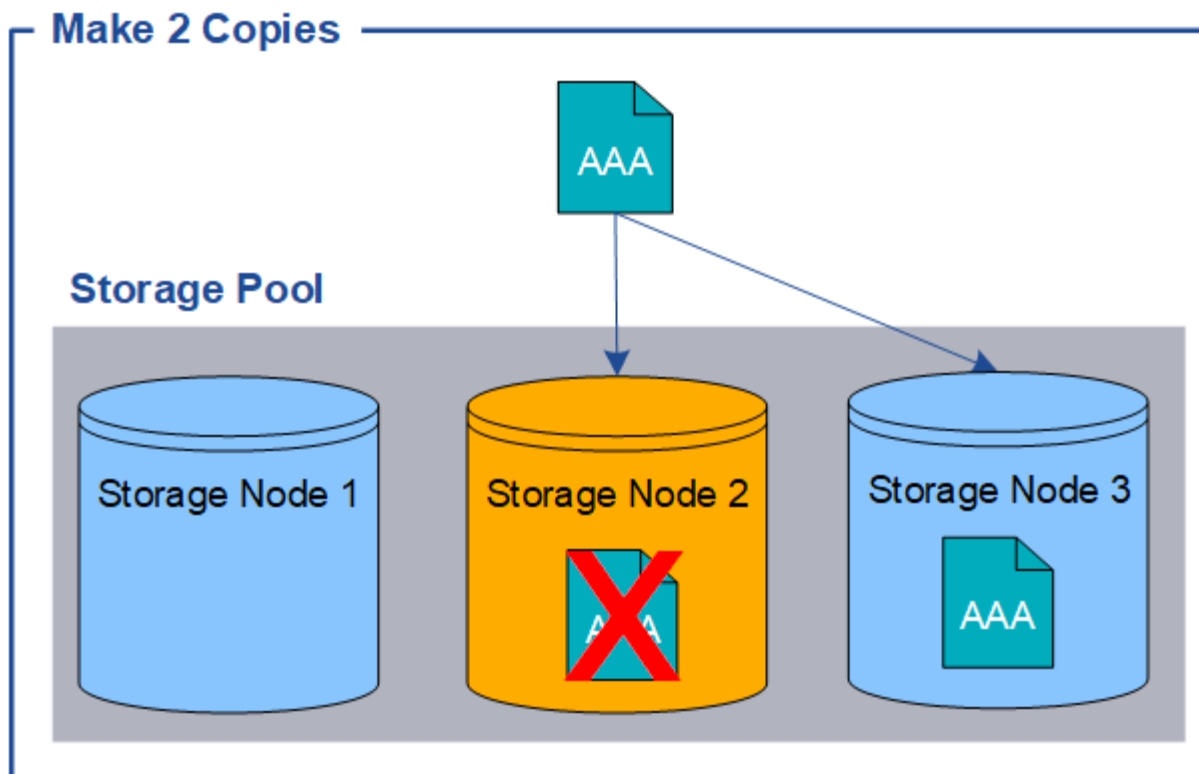
objeto en un grupo de almacenamiento que contiene tres Storage Nodes. Cuando se ingiere un objeto que coincide con esta regla, StorageGRID coloca una sola copia en solo un Storage Node.



Cuando una regla de 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, perderás temporalmente el acceso al objeto AAA cada vez que el nodo de almacenamiento 2 esté fuera de línea, como durante una actualización u otro procedimiento de mantenimiento. Perderás por completo el objeto AAA si el nodo de almacenamiento 2 falla.



Para evitar la pérdida de datos de los objetos, debes crear siempre al menos dos copias de todos los objetos que desees proteger mediante replicación. Si existen dos o más copias, puedes seguir accediendo al objeto si uno de los Storage Node falla o queda fuera de línea.



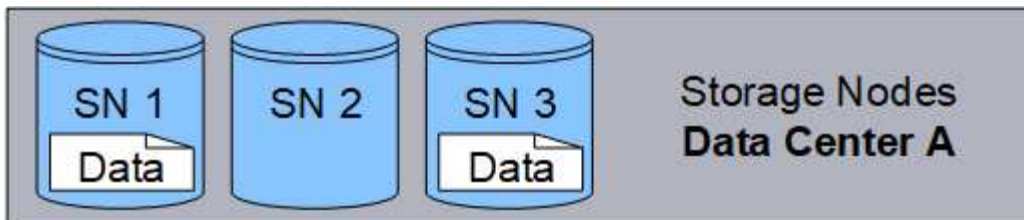
Aprende sobre el código de borrado en StorageGRID

El código 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 cumplen una regla de ILM que utiliza el código de borrado, esos objetos se dividen en fragmentos de datos, se calculan fragmentos de paridad adicionales y cada fragmento se almacena en un nodo de almacenamiento diferente.

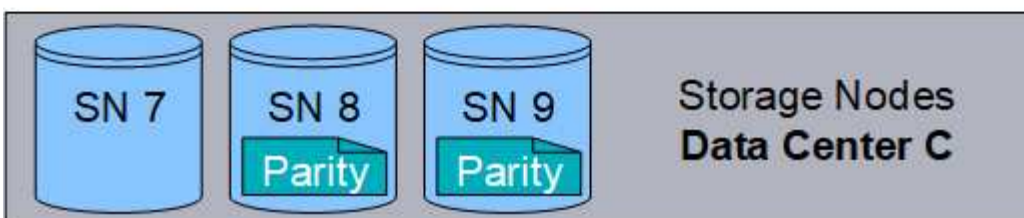
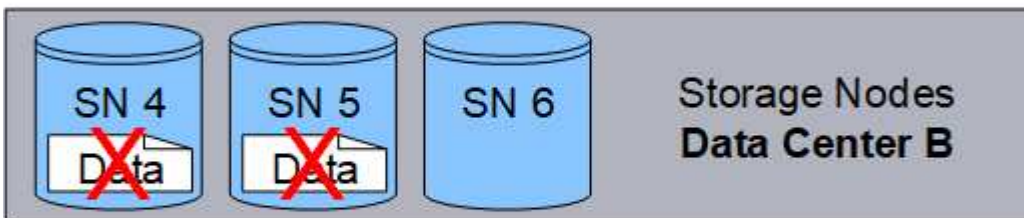
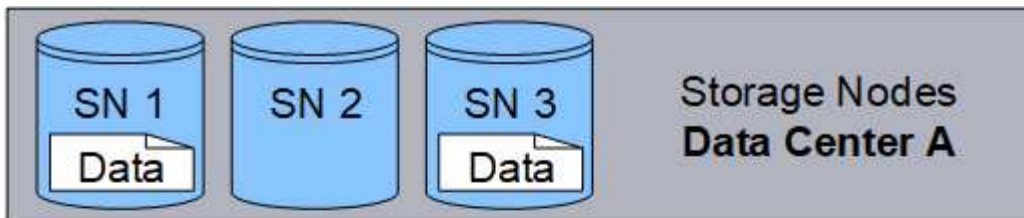
Cuando se accede a un objeto, este se vuelve a ensamblar utilizando los fragmentos almacenados. Si un fragmento de datos o de paridad se daña o se pierde, el algoritmo de código de borrado puede recrear ese fragmento utilizando un subconjunto de los fragmentos de datos y de paridad restantes.

A medida que creas reglas de ILM, StorageGRID crea perfiles de código de borrado compatibles con dichas reglas. Puedes consultar una lista de perfiles de código de borrado, ["cambiar el nombre de un perfil de código de borrado"](#), o ["desactivar un perfil de código de borrado si actualmente no se utiliza en ninguna regla de ILM"](#).

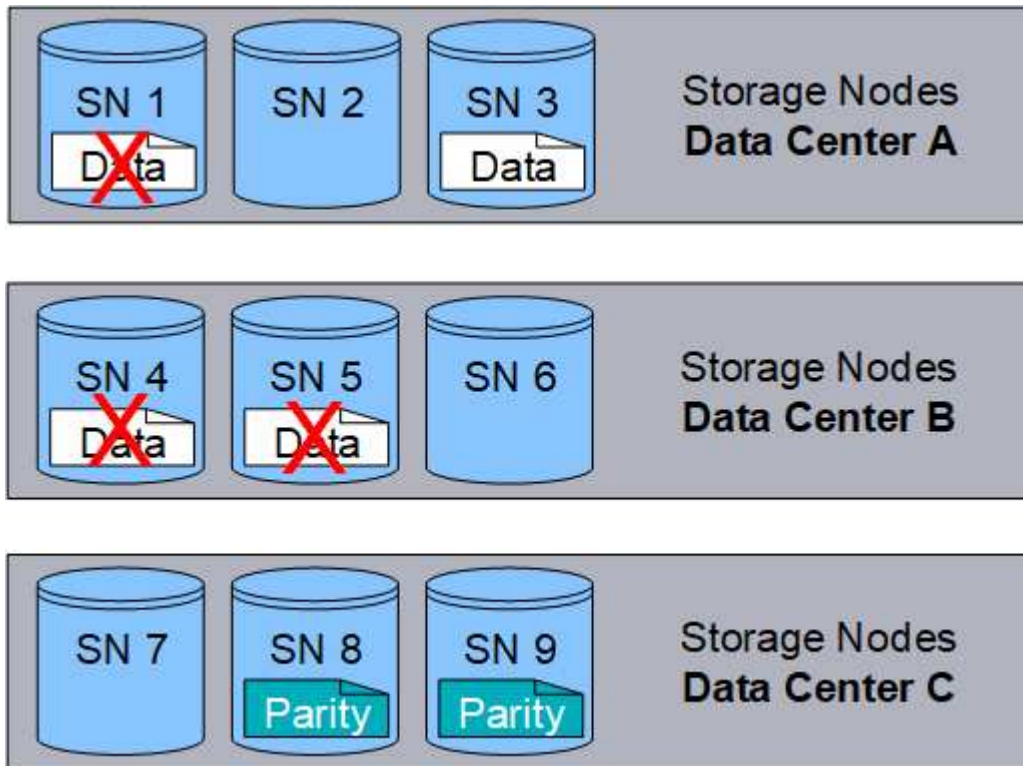
El siguiente ejemplo ilustra el uso de un algoritmo de codificación de borrado en los datos de un objeto. En este ejemplo, la regla ILM utiliza un esquema de codificación de borrado 4+2. Cada objeto se divide en cuatro fragmentos de datos iguales y se calculan dos fragmentos de paridad a partir de los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



El esquema de código de borrado 4+2 se puede configurar de diversas formas. Por ejemplo, puedes configurar un grupo de almacenamiento de un solo sitio que contenga seis nodos de almacenamiento. Para ["protección contra la pérdida del sitio"](#), puedes usar un grupo de almacenamiento que contenga tres sitios con tres nodos de almacenamiento en cada sitio. Puedes recuperar un objeto siempre que cualquiera de los cuatro de los seis fragmentos (de datos o de paridad) sigan disponibles. Se pueden perder hasta dos fragmentos sin perder los datos del objeto. Si se pierde un sitio completo, aún puedes recuperar o reparar el objeto, siempre que los demás fragmentos sigan siendo accesibles.



Si se pierden más de dos nodos de almacenamiento, el objeto no se puede recuperar.



Información relacionada

- ["¿Qué es la replicación?"](#)
- ["¿Qué es un storage pool?"](#)
- ["¿Qué son los esquemas de erasure coding?"](#)
- ["Cambiar el nombre de un perfil de código de borrado"](#)
- ["Desactivar un perfil de código de borrado"](#)

Conoce los esquemas de codificación de borrado en StorageGRID

Los esquemas de código de borrado controlan cuántos fragmentos de datos y cuántos fragmentos de paridad se crean para cada objeto.

Al crear o editar una regla de ILM, debes seleccionar un esquema de código de borrado disponible. StorageGRID crea automáticamente esquemas de código de borrado en función de cuántos nodos de almacenamiento y sitios forman el grupo de almacenamiento que planeas usar.

Protección de datos

El sistema StorageGRID utiliza el algoritmo de código de borrado Reed-Solomon. El algoritmo divide un objeto en k fragmentos de datos y calcula m fragmentos de paridad.

Los $k + m = n$ fragmentos se distribuyen entre n los nodos de almacenamiento para proporcionar protección de datos de la siguiente manera:

- Para recuperar o reparar un objeto, se necesitan fragmentos. k
- Un objeto puede soportar hasta m fragmentos perdidos o dañados. Cuanto mayor sea el valor de m , mayor

será la tolerancia a los fallos.

La mejor protección de datos la ofrece el esquema de código de borrado con mayor tolerancia a fallos de nodos o volúmenes dentro de un storage pool.

Sobrecarga de almacenamiento

La sobrecarga de almacenamiento de un esquema de codificación de borrado se calcula dividiendo el número de fragmentos de paridad (m) entre el número de fragmentos de datos (k). Puedes utilizar la sobrecarga de almacenamiento para calcular cuánto espacio en disco requiere cada objeto codificado mediante código de borrado:

$$\text{disk space} = \text{object size} + (\text{object size} * \text{storage overhead})$$

Por ejemplo, si almacenas un objeto de 10 MB utilizando el esquema 4+2 (que tiene una sobrecarga de almacenamiento del 50 %), el objeto ocupa 15 MB de almacenamiento en grid. Si almacenas el mismo objeto de 10 MB utilizando el esquema 6+2 (que tiene una sobrecarga de almacenamiento del 33 %), el objeto ocupa aproximadamente 13,3 MB.

Selecciona el esquema de código de borrado con el valor total más bajo de $k+m$ que se adapte a tus necesidades. Los esquemas de código de borrado con un número menor de fragmentos son más eficientes desde el punto de vista computacional porque:

- Se crean y distribuyen (o recuperan) menos fragmentos por objeto
- Ofrecen un mejor rendimiento porque el tamaño de los fragmentos es mayor
- Pueden requerir que se añadan menos nodos en un ["ampliación cuando se requiere más almacenamiento"](#)

Directrices para los grupos de almacenamiento

Al seleccionar el grupo de almacenamiento que se va a utilizar para una regla que creará una copia con código de borrado, sigue estas directrices relativas a los grupos de almacenamiento:

- El grupo de almacenamiento debe incluir tres o más emplazamientos, o exactamente un emplazamiento.



No puedes usar el código de borrado si el grupo de almacenamiento incluye dos sitios.

- [Esquemas de código de borrado para grupos de almacenamiento que contienen tres o más emplazamientos](#)
- [Esquemas de código de borrado para grupos de almacenamiento de un solo sitio](#)

- No utilices un grupo de almacenamiento que incluya el sitio All Sites.
- El grupo de almacenamiento debe incluir al menos $k+m + 1$ nodos de almacenamiento capaces de almacenar datos de objetos.



Los nodos de almacenamiento pueden configurarse durante la instalación para que contengan datos de objetos y metadatos (nodo de almacenamiento «combinado»), solo metadatos de objetos o solo datos de objetos. Para obtener más información, consulta ["Tipos de nodos de almacenamiento"](#).

El número mínimo de nodos de almacenamiento necesarios es $k+m$. Sin embargo, tener al menos un nodo de almacenamiento adicional puede ayudar a evitar fallos en la ingesta o retrasos en el ILM si un nodo de

almacenamiento necesario no está disponible temporalmente.

Esquemas de código de borrado para grupos de almacenamiento que contienen tres o más emplazamientos

La siguiente tabla describe los esquemas de código de borrado que admite actualmente StorageGRID para los grupos de almacenamiento que incluyen tres o más emplazamientos. Todos estos esquemas ofrecen protección frente a la pérdida de un emplazamiento. Se puede perder un emplazamiento y el objeto seguirá siendo accesible.

Para los esquemas de código de borrado que ofrecen protección frente a la pérdida de un sitio, el número recomendado de Storage Nodes en el storage pool supera $k+m + 1$ porque cada sitio requiere un mínimo de tres Storage Nodes.

Esquema de código 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 la pérdida del sitio?	Sobrecarga 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 usar el esquema 7+5, cada sitio requiere un mínimo de cuatro nodos de almacenamiento. Se recomienda usar cinco nodos de almacenamiento por sitio.

A la hora de seleccionar un esquema de código de borrado que ofrezca protección de sitio, hay que sopesar la importancia relativa de los siguientes factores:

- **Número de fragmentos:** Por lo general, el rendimiento y la flexibilidad de expansión son mejores cuando el número total de fragmentos es menor.
- **Tolerancia a fallos:** La tolerancia a fallos aumenta al disponer de más segmentos de paridad (es decir, cuando m tiene un valor más alto).

- **Tráfico de red:** Al recuperarse de fallos, usar un esquema con más fragmentos (es decir, un valor total más alto para $k+m$) genera más tráfico de red.
- **Sobrecarga de almacenamiento:** los esquemas con mayor sobrecarga requieren más espacio de almacenamiento por objeto.

Por ejemplo, a la hora de decidir entre un esquema 4+2 y uno 6+3 (ambos con una sobrecarga de almacenamiento del 50 %), elige el esquema 6+3 si se requiere una mayor tolerancia a fallos. Elige el esquema 4+2 si los recursos de red son limitados. Si todos los demás factores son iguales, elige el 4+2 porque tiene un número total de fragmentos menor.



Si no estás seguro de qué esquema debes utilizar, selecciona 4+2 o 6+3, o ponte en contacto con soporte técnico.

Esquemas de código de borrado para grupos de almacenamiento de un solo sitio

Un grupo de almacenamiento de un solo sitio es compatible con todos los esquemas de código de borrado definidos para tres o más sitios, siempre que dicho sitio cuente con suficientes nodos de almacenamiento.

El número mínimo de nodos de almacenamiento necesarios es $k+m$, pero se recomienda un grupo de almacenamiento con $k+m + 1$ nodos de almacenamiento. Por ejemplo, el esquema de código de borrado 2+1 requiere un grupo de almacenamiento con un mínimo de tres nodos de almacenamiento, pero se recomienda un grupo de cuatro nodos de almacenamiento.

Esquema de código de borrado ($k+m$)	Número mínimo de nodos de almacenamiento	Número recomendado de nodos de almacenamiento	Sobrecarga 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 para la codificación de borrado en StorageGRID

Antes de decidir si utilizar la replicación o el código de borrado para proteger los datos de objetos contra pérdidas, debes entender las ventajas, desventajas y los requisitos del

código de borrado.

Ventajas del código de borrado

En comparación con la replicación, el código de borrado ofrece una mayor fiabilidad, disponibilidad y eficiencia de almacenamiento.

- **Fiabilidad:** Se mide por el número de fallos simultáneos que se pueden soportar sin pérdida de datos.
 - Replicación: se almacenan varias copias idénticas de un objeto en distintos nodos y en diferentes emplazamientos.
 - Codificación de borrado: un objeto se codifica en fragmentos de datos y de paridad y se distribuye entre muchos nodos y sitios. Esta dispersión proporciona protección tanto frente a fallos de sitio como de nodo.
- **Disponibilidad:** La capacidad de obtener objetos si los nodos de almacenamiento fallan o se vuelven inaccesibles. En comparación con la replicación, el código de borrado ofrece una mayor disponibilidad con costes de almacenamiento similares.
- **Eficiencia de almacenamiento:** Para un nivel similar de disponibilidad y fiabilidad, los objetos con código de borrado ocupan menos espacio en disco que los objetos replicados. Por ejemplo, un objeto de 10 MB replicado en dos sitios ocupa 20 MB de espacio en disco (dos copias), mientras que un objeto codificado con código de borrado en tres sitios mediante un esquema 6+3 solo ocupa 15 MB de espacio en disco.



El espacio en disco para los objetos con código de borrado se calcula como el tamaño del objeto más la sobrecarga de almacenamiento. El porcentaje de sobrecarga de almacenamiento es el número de fragmentos de paridad dividido por el número de fragmentos de datos.

Desventajas del código de borrado

En comparación con la replicación, el código de borrado presenta las siguientes desventajas:

- Se recomienda aumentar el número de nodos de almacenamiento y de sitios, dependiendo del esquema de código de borrado. En cambio, si replicas datos de objetos, solo necesitas un nodo de almacenamiento por cada copia. Consulta ["Esquemas de código de borrado para grupos de almacenamiento que contienen tres o más emplazamientos"](#) y ["Esquemas de código de borrado para grupos de almacenamiento de un solo sitio"](#).
- Aumento del coste y la complejidad de las ampliaciones de almacenamiento. Para ampliar una implementación que utiliza replicación, tienes que añadir capacidad de almacenamiento en cada ubicación donde se crean copias de los objetos. Para ampliar una implementación que utiliza código de borrado, debes tener en cuenta tanto el esquema de código de borrado utilizado como el nivel de ocupación de los nodos de almacenamiento existentes. Por ejemplo, si esperas hasta que los nodos existentes estén al 100% de su capacidad, tienes que añadir al menos $k+m$ nodos de almacenamiento, pero si amplías cuando los nodos existentes están al 70% de su capacidad, puedes añadir dos nodos por sitio y seguir maximizando la capacidad de almacenamiento utilizable. Para más información, consulta ["Agrega capacidad de almacenamiento para objetos con código de borrado"](#).
- El uso del código de borrado en sitios distribuidos geográficamente conlleva un aumento de la latencia en la recuperación. Los fragmentos de un objeto codificado mediante código de borrado y distribuido entre sitios remotos tardan más en recuperarse a través de conexiones WAN que un objeto replicado y disponible localmente (en el mismo sitio al que se conecta el cliente).
- Cuando usas el código de borrado en sitios distribuidos geográficamente, hay un mayor uso de tráfico de red WAN para las recuperaciones y reparaciones, especialmente para los objetos que se recuperan con

frecuencia o para las reparaciones de objetos a través de conexiones de red WAN.

- Cuando se utiliza el código de borrado entre sitios, el rendimiento máximo de los objetos disminuye drásticamente a medida que aumenta la latencia de red entre los sitios. Esta disminución se debe a una reducción del rendimiento de la red TCP, lo que afecta a la rapidez con la que el sistema StorageGRID puede almacenar y recuperar fragmentos de objetos.
- Mayor uso de los recursos de computación.

Cuándo utilizar el código de borrado

Utiliza el código de borrado para los siguientes requisitos:

- Objetos de más de 1 MB de tamaño.



El código de borrado es más adecuado para objetos de más de 1 MB. No uses el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos muy pequeños codificados por borrado.

- Almacenamiento a largo plazo o en frío para contenido al que se accede con poca frecuencia.
- Alta disponibilidad y fiabilidad de los datos.
- Protección frente a fallos totales del sitio y de los nodos.
- Eficiencia de almacenamiento.
- Implementaciones en un único sitio que requieren una protección de datos eficaz con una sola copia codificada con código de borrado en lugar de múltiples copias replicadas.
- Implementaciones en varios sitios donde la latencia entre sitios es inferior a 100 ms.

Cómo StorageGRID determina la retención de objetos

StorageGRID ofrece opciones tanto a los administradores de grid como a los usuarios individuales de tenant para especificar durante cuánto tiempo almacenar los objetos. En general, cualquier instrucción de retención proporcionada por un usuario de tenant tiene prioridad sobre las instrucciones de retención proporcionadas por el administrador de grid.

Cómo los usuarios del inquilino controlan la retención de objetos

Los usuarios de Tenant pueden usar estos métodos para controlar cuánto tiempo se almacenan sus objetos en StorageGRID:

- Si la configuración global de S3 Object Lock está habilitada para la grid, los usuarios del tenant de S3 pueden crear buckets con S3 Object Lock habilitado y luego seleccionar un **período de retención predeterminado** para cada bucket.
- Si la configuración global de S3 Object Lock está habilitada para el grid, los usuarios de S3 tenant pueden crear buckets con S3 Object Lock habilitado y luego usar la API de REST de S3 para especificar retain-until-date y legal hold para cada versión de objeto añadida a ese bucket.
 - Una versión de objeto que está bajo retención legal no puede eliminarse por ningún método.
 - Antes de que se alcance la fecha límite de retención de una versión de un objeto, esa versión no puede eliminarse por ningún método.
 - Los objetos de los buckets en los que se ha habilitado S3 Object Lock se conservan «para siempre»

mediante ILM. Sin embargo, después de que se alcance la fecha de retención, una versión del objeto puede eliminarse mediante una solicitud del cliente o al expirar el ciclo de vida del bucket. Consulta ["Gestiona objetos con S3 Object Lock"](#).

- Los usuarios de un tenant de S3 pueden añadir una configuración de ciclo de vida a sus buckets en la que se especifique una acción de Expiration. Si existe un ciclo de vida para el bucket, StorageGRID almacena un objeto hasta que se alcance la fecha o el número de días especificados en la acción de Expiration, a menos que el cliente elimine el objeto antes. Consulta ["Crear configuración del ciclo de vida de S3"](#).
- Un cliente S3 puede enviar una solicitud de eliminación de un objeto. StorageGRID siempre da prioridad a las solicitudes de eliminación del cliente frente al ciclo de vida del bucket S3 o ILM al determinar si se debe eliminar o conservar un objeto.

Cómo controlan los administradores de grid la retención de objetos

Los administradores de la grid pueden utilizar estos métodos para controlar la retención de objetos:

- Establece un periodo máximo de retención de S3 Object Lock para cada tenant. Luego, los usuarios del tenant pueden establecer un periodo de retención predeterminado para cada uno de sus buckets. El periodo máximo de retención también se aplica a cualquier objeto nuevo que se incorpore a ese bucket (retain-until-date del objeto).
- Crea instrucciones de ubicación de ILM para controlar el tiempo que se almacenan los objetos. Cuando los objetos coinciden con una regla de ILM, StorageGRID almacena esos objetos hasta que haya transcurrido el último periodo de tiempo en la regla de ILM. Los objetos se conservan indefinidamente si se especifica "para siempre" en las instrucciones de ubicación.
- Independientemente de quién controle el tiempo de retención de los objetos, la configuración de ILM determina qué tipos de copias de los objetos (replicadas o con código de borrado) se almacenan y dónde se ubican dichas copias (Storage Nodes o Cloud Storage Pools).

Cómo interactúan el ciclo de vida de los buckets de S3 y la ILM

Cuando se configura el ciclo de vida de un bucket de S3, las acciones de caducidad del ciclo de vida prevalecen sobre la política de ILM para los objetos que coinciden con el filtro del ciclo de vida. Como resultado, un objeto podría mantenerse en el grid incluso después de que hayan expirado las instrucciones de ILM para ubicar el objeto.

Ejemplos de retención de objetos

Para comprender mejor las interacciones entre S3 Object Lock, la configuración del ciclo de vida de los buckets, las solicitudes de eliminación de los clientes y ILM, fíjate en los siguientes ejemplos.

Ejemplo 1: el ciclo de vida de un bucket de S3 conserva los objetos durante más tiempo que el ILM

ILM

Conservar dos copias durante 1 año (365 días)

Ciclo de vida de bucket

Los objetos caducan en 2 años (730 días)

Resultado

StorageGRID almacena el objeto durante 730 días. StorageGRID utiliza la configuración del ciclo de vida del bucket para determinar si se debe eliminar o conservar un objeto.



Si el ciclo de vida del bucket especifica que los objetos deben conservarse durante más tiempo del indicado por el ILM, StorageGRID sigue utilizando las instrucciones de ubicación del ILM al determinar el número y tipo de copias que se deben almacenar. En este ejemplo, dos copias del objeto seguirán almacenándose en StorageGRID desde el día 366 hasta el 730.

Ejemplo 2: el ciclo de vida del bucket de S3 expira los objetos antes que ILM

ILM

Conservar dos copias durante 2 años (730 días)

Ciclo de vida de bucket

Los objetos caducan en 1 año (365 días)

Resultado

StorageGRID elimina ambas copias del objeto después del día 365.

Ejemplo 3: la eliminación por parte del cliente anula el ciclo de vida del bucket y el ILM

ILM

Almacena dos copias en los Storage Nodes "para siempre"

Ciclo de vida de bucket

Los objetos caducan en 2 años (730 días)

Solicitud de eliminación de cliente

Publicado 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 de S3 anula la solicitud de eliminación del cliente

Bloqueo de objetos de S3

La fecha límite de conservación de una versión del objeto es el 31 de marzo de 2026. No hay ninguna retención legal en vigor.

Regla de ILM conforme

Almacena dos copias en los Storage Nodes "para siempre"

Solicitud de eliminación de cliente

Publicado el 31 de marzo de 2024

Resultado

StorageGRID no eliminará la versión del objeto porque aún faltan 2 años para la fecha límite de conservación.

Cómo StorageGRID borra 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

de S3 o de los requisitos de la política de ILM. Entender las diferentes formas en que se pueden eliminar los objetos y cómo StorageGRID maneja las solicitudes de eliminación puede ayudarte a gestionar los objetos de manera más eficaz.

StorageGRID puede utilizar uno de estos dos métodos para eliminar objetos:

- Eliminación sincrónica: Cuando StorageGRID recibe una solicitud de eliminación de un cliente, todas las copias del objeto se eliminan de inmediato. El cliente es informado de que la eliminación fue exitosa después de que se hayan eliminado las copias.
- Los objetos se colocan en cola para su eliminación: cuando StorageGRID recibe una solicitud de eliminación, el objeto se coloca en cola para su eliminación y se informa inmediatamente al cliente que la eliminación fue exitosa. Las copias de los objetos se eliminan más tarde mediante el procesamiento de 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 libre con mayor rapidez.

La tabla resume en qué casos StorageGRID utiliza cada método.

Método para realizar una eliminación	Cuando se utiliza
Los objetos se colocan en cola para su eliminación	Cuando cualquiera de las siguientes condiciones sea verdadera: • La eliminación automática de objetos se activó por uno de los siguientes eventos: ◦ Se ha alcanzado la fecha de caducidad o el número de días en la configuración del ciclo de vida de un bucket de S3. ◦ Vence el último plazo especificado en una regla de ILM. • Un cliente de S3 solicita una eliminación y se cumple una o varias de estas condiciones: ◦ Las copias no se pueden eliminar en los primeros 30 segundos porque, por ejemplo, la ubicación de un objeto no está disponible temporalmente. ◦ Las colas de eliminación en segundo plano están inactivas. Nota: Los objetos de un bucket en el que esté activada la función S3 Object Lock no se pueden eliminar si están sujetos a una retención legal o si se ha especificado una fecha límite de conservación que aún no se ha alcanzado.
Los objetos se eliminan de inmediato (eliminación sincrónica)	Cuando un cliente de S3 realiza una solicitud de eliminación y se cumplen todas las condiciones siguientes: • Todas las copias se pueden eliminar en 30 segundos. • Las colas de eliminación en segundo plano contienen objetos para procesar.

Cuando los clientes de S3 realizan solicitudes de eliminación, StorageGRID comienza añadiendo 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 a StorageGRID procesar las eliminaciones de manera más eficiente, especialmente para clientes con baja concurrencia, y ayuda a evitar acumulaciones de

solicitudes de eliminación de los clientes.

Tiempo necesario para eliminar objetos

La forma en que StorageGRID elimina los objetos puede influir en el rendimiento aparente del sistema:

- Cuando StorageGRID lleva a cabo una eliminación sincrónica, puede tardar hasta 30 segundos en devolver un resultado al cliente. Esto significa que la eliminación puede parecer más lenta, aunque en realidad las copias se eliminan más rápidamente que cuando StorageGRID pone los objetos en cola para su eliminación.
- Si estás supervisando de cerca el rendimiento de la eliminación durante una eliminación masiva, es posible que observes que la velocidad de eliminación parece reducirse una vez que se ha eliminado un determinado número de objetos. Este cambio se produce cuando StorageGRID pasa de poner los objetos en cola para su eliminación a realizar una eliminación sincrónica. La aparente reducción de la velocidad de eliminación no significa que las copias de los objetos se estén eliminando más lentamente. Al contrario, indica que, de media, ahora se libera espacio más rápidamente.

Si vas a eliminar un gran número de objetos y tu prioridad es obtener espacio libre rápidamente, plantéate utilizar una solicitud del cliente para eliminarlos en lugar de hacerlo mediante ILM u otros métodos. En general, el espacio libre se obtiene más rápidamente cuando la eliminación la realizan los clientes porque StorageGRID puede utilizar la eliminación sincrónica.

La cantidad de tiempo que se necesita para liberar espacio después de eliminar un objeto depende de varios factores:

- Si las copias de los objetos se eliminan de forma sincrónica o se ponen en cola para su eliminación posterior (para las solicitudes de eliminación de los clientes).
- Otros factores, como el número de objetos en el grid o la disponibilidad de recursos del grid cuando las copias de los objetos se ponen en cola para su eliminación (tanto en el caso de las eliminaciones realizadas por el cliente como en el de otros métodos).

Cómo se eliminan los objetos versionados de S3

Cuando se habilita el control de versiones para un bucket de S3, StorageGRID sigue el comportamiento de Amazon S3 cuando responde a las solicitudes de eliminación, ya sea que esas solicitudes provengan de un cliente de S3, del vencimiento del ciclo de vida de un bucket de S3 o de los requisitos de la política de ILM.

Cuando los objetos están versionados, las solicitudes de eliminación de objetos no eliminan la versión actual del objeto ni liberan espacio. En su lugar, una solicitud de eliminación de objetos crea un marcador de eliminación de cero bytes como versión actual del objeto, lo que hace que la versión anterior del objeto pase a ser "no actual". Un marcador de eliminación de objeto se convierte en un marcador de eliminación de objeto caducado cuando es la versión actual y no hay versiones no actuales.

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, como los datos del objeto no actual no se han eliminado, las solicitudes que especifiquen una versión no actual del objeto pueden tener éxito.

Si un cliente elimina una versión de un objeto con un identificador de versión de un "bucket de rama", StorageGRID oculta la existencia de la versión del objeto pero no crea un marcador de eliminación en el branch bucket. Si un cliente elimina un objeto sin identificador de versión de un branch bucket, StorageGRID crea un marcador de eliminación en el branch bucket según el comportamiento estándar de S3.

Para liberar espacio al eliminar objetos versionados o para eliminar los marcadores de eliminación, usa una de

las siguientes opciones:

- **Solicitud del cliente S3:** Especifica el ID de versión del objeto en la solicitud S3 DELETE Object (`DELETE /object?versionId=ID`). Ten en cuenta que esta solicitud solo elimina las copias del objeto correspondientes a la versión especificada (las demás versiones siguen ocupando espacio).
- **Ciclo de vida del bucket:** Usa la acción `NoncurrentVersionExpiration` en la configuración del ciclo de vida del bucket. Cuando se cumple el número de `NoncurrentDays` especificado, StorageGRID elimina permanentemente todas las copias de las versiones de objetos que ya no están vigentes. Estas versiones de objetos no se pueden recuperar.

La `NewerNoncurrentVersions` acción en la configuración del ciclo de vida del bucket especifica el número de versiones no actuales que se conservan en un bucket de S3 con control de versiones. Si hay más versiones no actuales de las que `NewerNoncurrentVersions` especifica, StorageGRID elimina las versiones más antiguas cuando ha transcurrido el valor de `NoncurrentDays`. El umbral de `NewerNoncurrentVersions` reemplaza las reglas del ciclo de vida proporcionadas por ILM, lo que significa que un objeto no actual con una versión dentro del umbral de `NewerNoncurrentVersions` se conserva si ILM solicita su eliminación.

Para eliminar los marcadores de eliminación de objetos caducados, usa la acción `Expiration` con una de las siguientes etiquetas: `ExpiredObjectDeleteMarker`, `Days` o `Date`.

- **ILM:** ["Clonar una política activa"](#) y añade dos reglas de ILM a la nueva política:
 - Primera regla: utiliza «Tiempo no actual» como tiempo de referencia para hacer coincidir las versiones no actuales del objeto. En ["Paso 1 \(Introducir datos\) del asistente para crear una regla de ILM"](#), selecciona **Sí** para la pregunta, «¿Aplicar esta regla solo a las versiones anteriores del objeto (en S3 buckets con control de versiones activado)?»
 - Segunda regla: Utiliza **Hora de ingesta** para hacer coincidir la versión actual. La regla «Hora no actual» debe aparecer en la política por encima de la regla **Hora de ingesta**.

Para eliminar los marcadores de eliminación de objetos caducados, utiliza una regla de **Hora de ingesta** 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 marcador de eliminación actual ha caducado (no hay versiones que no sean actuales).

- **Eliminar objetos de un depósito:** Usa el tenant manager 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 que se pueda eliminar un bucket versionado.

- Los marcadores de eliminación creados en StorageGRID 11.7 o versiones anteriores solo pueden eliminarse mediante solicitudes del cliente S3, no se eliminan mediante ILM, las reglas de ciclo de vida del bucket ni las operaciones de eliminación de objetos del bucket.
- Los marcadores de eliminación de un bucket creado en StorageGRID 11.8 o una versión posterior pueden eliminarse mediante ILM, las reglas del ciclo de vida del bucket, las operaciones de eliminación de objetos en el bucket o una eliminación explícita realizada por un cliente S3.

Información relacionada

- ["Usa la API de REST de S3"](#)
- ["Ejemplo 4: reglas y política de ILM para objetos versionados de S3"](#)

Crea y asigna grados de almacenamiento en StorageGRID

Los niveles de almacenamiento identifican el tipo de almacenamiento que utiliza un nodo de almacenamiento. Puedes crear niveles de almacenamiento si deseas que las reglas de ILM coloquen determinados objetos en determinados nodos de almacenamiento.

Antes de empezar

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

Acerca de esta tarea

Al instalar StorageGRID por primera vez, se asigna automáticamente el nivel de almacenamiento **Predeterminado** a todos los nodos de almacenamiento del sistema. Si es necesario, puedes definir opcionalmente niveles de almacenamiento personalizados y asignarlos a diferentes nodos de almacenamiento.

El uso de niveles de almacenamiento personalizados te permite crear grupos de almacenamiento ILM que contengan únicamente un tipo específico de nodo de almacenamiento. Por ejemplo, es posible que desees que determinados objetos se almacenen en tus nodos de almacenamiento más rápidos, como los dispositivos de almacenamiento all-flash de StorageGRID.



A los nodos de almacenamiento «solo metadatos» no se les puede asignar un nivel de almacenamiento. Para obtener más información, consulta ["Tipos de nodos de almacenamiento"](#).

Si el nivel de almacenamiento no es un factor relevante (por ejemplo, si todos los nodos de almacenamiento son idénticos), puedes omitir este procedimiento y utilizar la opción **incluye todos los niveles de almacenamiento** para el nivel de almacenamiento cuando ["crear grupos de almacenamiento"](#). Usar esta opción asegura que el grupo de almacenamiento incluya todos los nodos de almacenamiento del sitio, sin importar su nivel de almacenamiento.



No crees más niveles de almacenamiento de los necesarios. Por ejemplo, no crees un nivel de almacenamiento para cada Storage Node. En su lugar, asigna cada nivel de almacenamiento a dos o más nodos. Los niveles de almacenamiento asignados a un solo nodo pueden provocar atascos en ILM si ese nodo deja de estar disponible.

Pasos

1. Selecciona **ILM > Niveles de almacenamiento**.
2. Define grados de almacenamiento personalizados:
 - a. Para cada nivel de almacenamiento personalizado que quieras añadir, selecciona **Insert**  para añadir una fila.
 - b. Introduce 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. Selecciona **Aplicar cambios**.

d. Si lo deseas, si necesitas modificar una etiqueta guardada, selecciona **Editar** y selecciona **Aplicar cambios**.



No puedes eliminar los niveles de almacenamiento.

3. Asigna nuevos niveles de almacenamiento a los nodos de almacenamiento:

a. Busca el nodo de almacenamiento en la lista LDR y selecciona su icono **Editar** .

b. Selecciona el grado de almacenamiento adecuado 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



Asigna un nivel de almacenamiento a un Storage Node determinado solo una vez. Un Storage Node recuperado tras un fallo mantiene el nivel de almacenamiento asignado anteriormente. No cambies esta asignación después de que la política de ILM esté activada. Si se cambia la asignación, los datos se almacenan según el nuevo nivel de almacenamiento.

a. Selecciona **Aplicar cambios**.

Usa grupos de almacenamiento

Conoce los grupos de almacenamiento en StorageGRID

Un grupo de almacenamiento es una agrupación lógica de nodos de almacenamiento.

Al instalar StorageGRID, se crea automáticamente un grupo de almacenamiento por cada sitio. Puedes configurar grupos de almacenamiento adicionales según tus requisitos de almacenamiento.



Los nodos de almacenamiento pueden configurarse durante la instalación para que contengan datos de objetos y metadatos (nodo de almacenamiento «combinado»), solo metadatos de objetos o solo datos de objetos. Los nodos de almacenamiento que contienen únicamente metadatos no pueden utilizarse en grupos de almacenamiento. Para obtener más información, consulta "[Tipos de nodos de almacenamiento](#)".

Los grupos de almacenamiento tienen dos atributos:

- **Nivel de almacenamiento:** para los Storage Nodes, el rendimiento relativo del almacenamiento subyacente.
- **Ubicación:** el centro de datos donde se almacenarán los objetos.

Los grupos de almacenamiento se utilizan en las reglas de ILM para determinar dónde se almacenan los datos de los objetos y el tipo de almacenamiento que se utiliza. Cuando configuras las reglas de ILM para la replicación, seleccionas uno o varios grupos de almacenamiento.

Directrices para la configuración de storage pool en StorageGRID

Configura y utiliza grupos de almacenamiento para protegerte contra la pérdida de datos distribuyéndolos entre varias ubicaciones. Las copias replicadas y las copias con código de borrado requieren diferentes configuraciones de grupos de almacenamiento.

Consulta ["Ejemplos de cómo habilitar la protección contra la pérdida de sitios mediante la replicación y el código de borrado"](#).

Directrices para todos los grupos de almacenamiento

- Mantén las configuraciones de los grupos de almacenamiento lo más sencillas posible. No crees más grupos de almacenamiento de los necesarios.
- Crea grupos de almacenamiento con el mayor número posible de nodos. Cada grupo de almacenamiento debe contener dos o más nodos. Un grupo de almacenamiento con un número insuficiente de nodos puede provocar atascos en el ILM si un nodo deja de estar disponible.
- Evita crear o utilizar grupos de almacenamiento que se solapen (que contengan uno o más de los mismos nodos). Si los grupos de almacenamiento se solapan, es posible que se guarde más de una copia de los datos de los objetos en el mismo nodo.
- En general, no utilices el grupo de almacenamiento All Storage Nodes (StorageGRID 11.6 y versiones anteriores) ni el sitio All Sites. Estos elementos se actualizan automáticamente para incluir cualquier sitio nuevo que añadas en una ampliación, lo que quizá no sea el comportamiento que desees.

Directrices para los grupos de almacenamiento utilizados para copias replicadas

- Para la protección contra la pérdida de un sitio mediante ["replicación"](#), especifica uno o varios grupos de almacenamiento específicos del sitio en ["instrucciones de colocación para cada regla del 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 replicadas de los objetos se almacenen exactamente donde esperas (por ejemplo, una copia de cada objeto en cada sitio para protegerte ante la pérdida de un sitio).

- Si añades un sitio en una ampliación, crea un nuevo grupo de almacenamiento que contenga únicamente el nuevo sitio. Luego, ["Actualizar las reglas de ILM"](#) para controlar qué objetos se almacenan en el nuevo sitio.
- Si el número de copias es inferior al número de grupos de almacenamiento, el sistema distribuye las copias para equilibrar el uso del disco entre los grupos.
- Si los grupos de almacenamiento se solapan (contienen los mismos nodos de almacenamiento), es posible que todas las copias del objeto se guarden únicamente en un solo sitio. Debes asegurarte de que los grupos de almacenamiento seleccionados no contengan los mismos nodos de almacenamiento.

Directrices para los grupos de almacenamiento usados para copias con código de borrado

- Para la protección contra la pérdida de sitios mediante ["codificación de borrado"](#), crea grupos de almacenamiento que consten de al menos tres sitios. Si un grupo de almacenamiento incluye solo dos sitios, no puedes usar ese grupo de almacenamiento para el código de borrado. No hay esquemas de código de borrado disponibles para un grupo de almacenamiento que tenga dos sitios.
- El número de nodos de almacenamiento y de emplazamientos que componen el grupo de almacenamiento determina qué ["esquemas de codificación de borrado"](#) están disponibles.

- Si es posible, un grupo de almacenamiento debería incluir más que el número mínimo de nodos de almacenamiento requerido para el esquema de código de borrado que elijas. Por ejemplo, si utilizas un esquema de código de borrado 6+3, debes tener al menos nueve nodos de almacenamiento. Sin embargo, se recomienda tener al menos un nodo de almacenamiento adicional por sitio.
- Distribuye los nodos de almacenamiento entre los distintos emplazamientos de la forma más uniforme posible. Por ejemplo, para admitir un esquema de código de borrado 6+3, configura un grupo de almacenamiento que incluya al menos tres nodos de almacenamiento en tres emplazamientos.
- Si tienes requisitos de rendimiento elevados, 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 reducción del rendimiento de la red TCP.

La disminución del rendimiento afecta las velocidades máximas alcanzables de ingesta y recuperación de objetos (cuando se seleccionan los comportamientos de ingesta Balanced o Strict) o podría provocar atascos en las colas de ILM (cuando se selecciona el comportamiento de ingesta Dual commit). Consulta ["Comportamiento de ingesta según la regla ILM"](#).



Si tu grid incluye solo un sitio, no podrás utilizar el grupo de almacenamiento All Storage Nodes (StorageGRID 11.6 y versiones anteriores) ni el sitio All Sites en un perfil de código de borrado. Este comportamiento evita que el perfil deje de ser válido si se añade un segundo sitio.

Protección contra pérdida de sitios con pools de almacenamiento en StorageGRID

Si tu implementación de StorageGRID incluye más de un sitio, puedes utilizar la replicación y el código de borrado con grupos de almacenamiento configurados adecuadamente para habilitar la protección frente a la pérdida de un sitio.

La replicación y el código de borrado requieren diferentes configuraciones del grupo de almacenamiento:

- Para utilizar la replicación como protección frente a la pérdida de un sitio, utiliza los grupos de almacenamiento específicos de cada sitio que se crean automáticamente durante la instalación de StorageGRID. Luego crea reglas de ILM con ["instrucciones de colocación"](#) que especifiquen varios grupos de almacenamiento para que se coloque una copia de cada objeto en cada sitio.
- Para utilizar el código de borrado como protección frente a la pérdida de un sitio, ["crear grupos de almacenamiento que consten de varios sitios"](#). Luego crea reglas de ILM que usen un grupo de almacenamiento compuesto por varios sitios y cualquier esquema de código de borrado disponible.



Al configurar tu implementación de StorageGRID para la protección frente a la pérdida de un sitio, también debes tener en cuenta los efectos de ["opciones de ingesta"](#) y ["coherencia"](#).

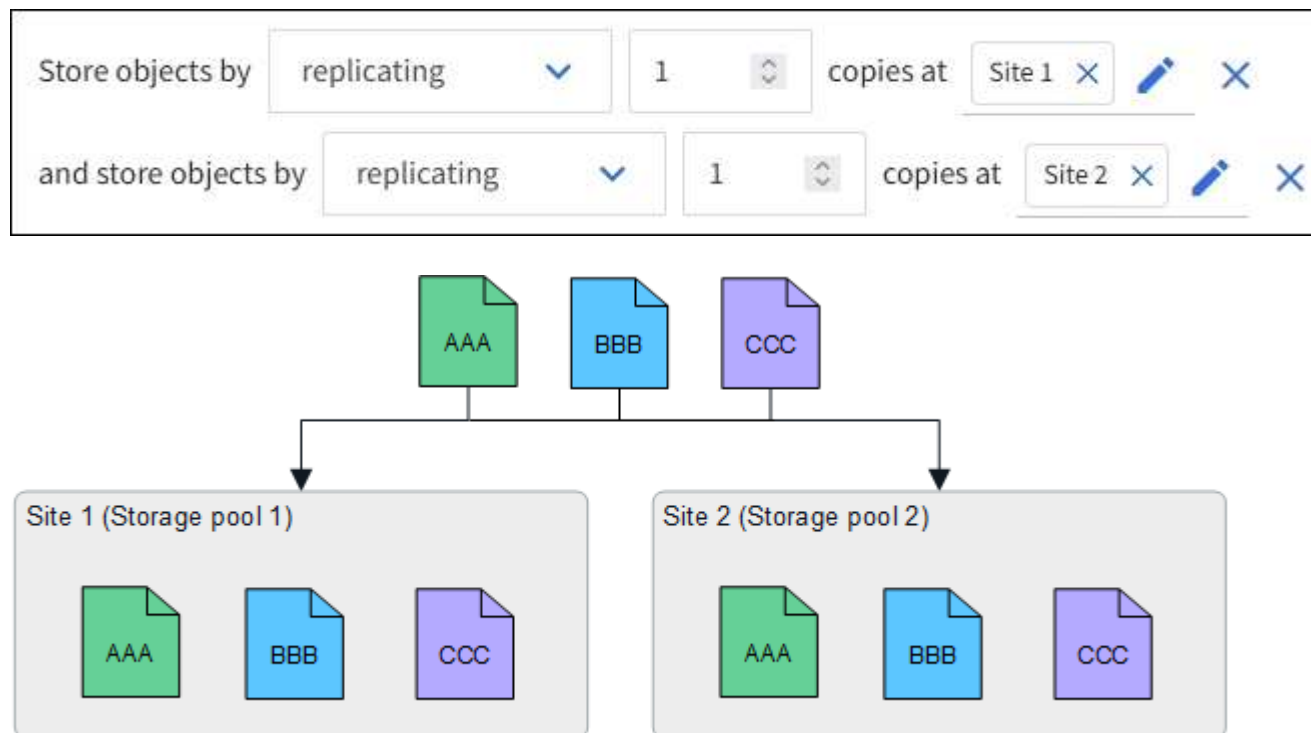
Ejemplo de replicación

De forma predeterminada, durante la instalación de StorageGRID se crea un grupo de almacenamiento para cada sitio. Disponer de grupos de almacenamiento formados por un único sitio permite configurar reglas de ILM que utilicen la replicación como protección ante la pérdida de un sitio. En este ejemplo:

- El pool de almacenamiento 1 contiene Site 1
- El grupo de almacenamiento 2 contiene Site 2
- La regla ILM contiene dos ubicaciones:

- Almacena objetos replicando 1 copia en el sitio 1
- Almacena objetos replicando 1 copia en el sitio 2

Ubicaciones de las reglas de ILM:



Si se pierde una de las sedes, se dispone de copias de los objetos en la otra sede.

Ejemplo de erasure coding

Disponer de grupos de almacenamiento que consten de más de un sitio por grupo permite configurar reglas de ILM que utilicen el código de borrado para la protección frente a la pérdida de un sitio. En este ejemplo:

- El grupo de almacenamiento 1 contiene los sitios 1 al 3
- La regla ILM contiene una ubicación: almacenar objetos mediante el código de borrado utilizando un esquema EC 4+2 en Storage pool 1, que contiene tres sitios

Ubicaciones de las reglas de ILM:



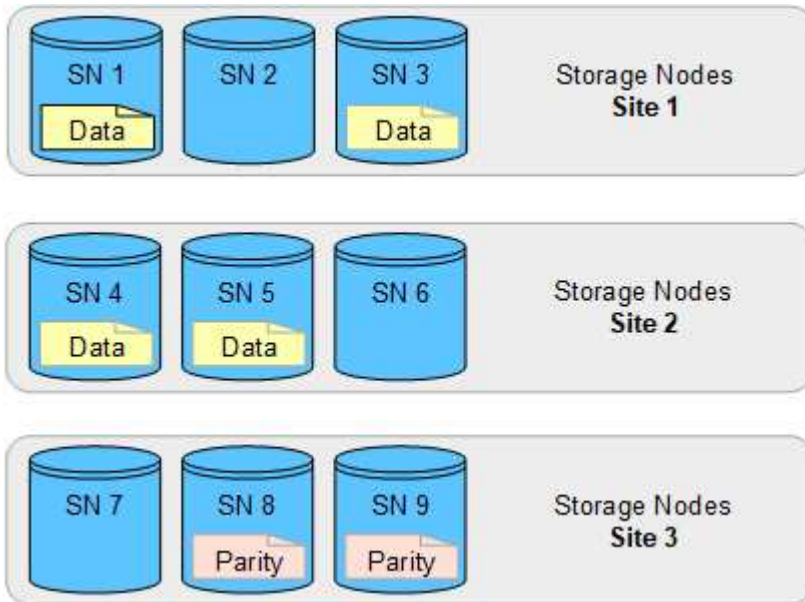
En este ejemplo:

- La regla ILM utiliza un esquema de código de borrado 4+2.
- Cada objeto se divide en cuatro fragmentos de datos iguales, y a partir de los datos del objeto se calculan dos fragmentos de paridad.
- Cada uno de los seis fragmentos se almacena en un nodo diferente repartido entre tres centros de datos para proporcionar protección de datos ante fallos de nodo o pérdida de sitio.

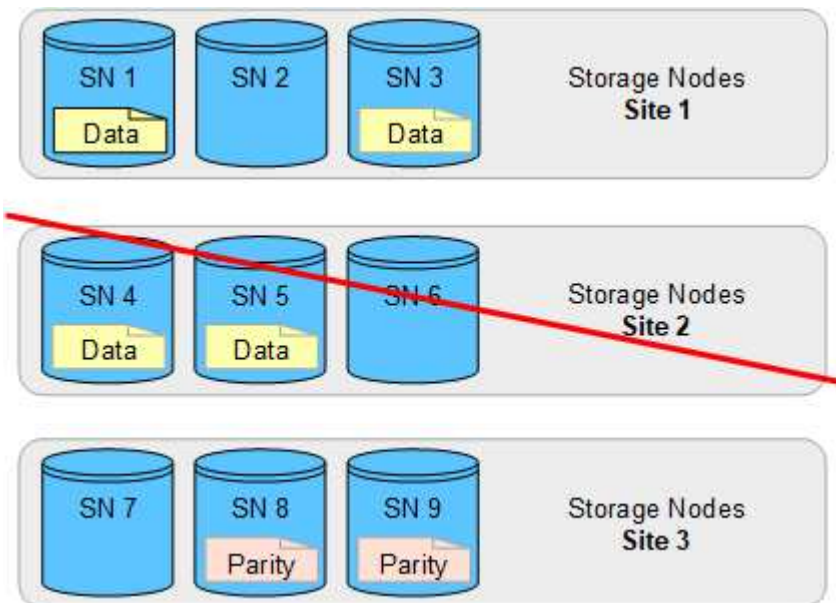


El código de borrado está permitido en los grupos de almacenamiento que contienen cualquier número de sitios *excepto* dos sitios.

Regla ILM que utiliza el esquema de código de borrado 4+2:



Si se pierde un sitio, los datos aún se pueden recuperar:



Crea un pool de almacenamiento en StorageGRID

Creas grupos de almacenamiento para determinar dónde almacena el sistema StorageGRID los datos de los objetos y el tipo de almacenamiento que se usa. Cada grupo de almacenamiento incluye uno o varios sitios y uno o varios niveles de almacenamiento.



Al instalar StorageGRID 12.0 en una nueva grid, se crean automáticamente grupos de almacenamiento para cada sitio. Sin embargo, si inicialmente instalaste StorageGRID 11.6 o una versión anterior, los grupos de almacenamiento no se crean automáticamente para cada sitio.

Si deseas crear Cloud Storage Pools para almacenar datos de objetos fuera de tu sistema StorageGRID, consulta la ["Información sobre el uso de Cloud Storage Pools"](#).

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).
- Ya has consultado las directrices para crear grupos de almacenamiento.

Acerca de esta tarea

Los grupos de almacenamiento determinan dónde se almacenan los datos de los objetos. El número de grupos de almacenamiento que necesitas depende del número de sitios en tu grid y de los tipos de copias que quieres: replicadas o con código de borrado.

- Para la replicación y el código de borrado en un único sitio, crea un grupo de almacenamiento para cada sitio. Por ejemplo, si deseas almacenar copias replicadas de objetos en tres sitios, crea tres grupos de almacenamiento.
- Para el código de borrado en tres o más sitios, crea un grupo de almacenamiento que incluya una entrada para cada sitio. Por ejemplo, si quieres aplicar el código de borrado a objetos en tres sitios, crea un solo grupo de almacenamiento.



No incluyas el sitio «All Sites» en un grupo de almacenamiento que se vaya a utilizar en un perfil de código de borrado. En su lugar, añade una entrada independiente al grupo de almacenamiento para cada sitio que vaya a almacenar datos con código de borrado. Consulta [este paso](#) para ver un ejemplo.

- Si tienes más de un nivel de almacenamiento, no crees un grupo de almacenamiento que incluya diferentes niveles de almacenamiento en un solo sitio. Consulta el ["Directrices para la creación de grupos de almacenamiento"](#).

Pasos

1. Selecciona **ILM > Storage pools**.

La pestaña «Grupos de almacenamiento» muestra todos los grupos de almacenamiento definidos.



En las nuevas instalaciones de StorageGRID 11.6 o versiones anteriores, el grupo de almacenamiento All Storage Nodes se actualiza automáticamente cada vez que añades nuevas sedes de centro de datos. No utilices este grupo en las reglas de ILM.

2. Para crear un nuevo grupo de almacenamiento, selecciona **Crear**.
3. Introduce un nombre único para el grupo de almacenamiento. Elige un nombre que resulte fácil de identificar a la hora de configurar perfiles de código de borrado y reglas de ILM.
4. En la lista desplegable **Sitio**, selecciona un sitio para este grupo de almacenamiento.

Al seleccionar un sitio, el número de nodos de almacenamiento en la tabla se actualiza automáticamente.

En general, no utilices el sitio All Sites en ningún grupo de almacenamiento. Las reglas de ILM que utilizan un grupo de almacenamiento All Sites colocan los objetos en cualquier sitio disponible, lo que te da menos control sobre la ubicación de los objetos. Además, un grupo de almacenamiento All Sites utiliza inmediatamente los Storage Nodes de un nuevo sitio, lo que podría no ser el comportamiento que esperas.

5. En la lista desplegable **Storage grade**, selecciona el tipo de almacenamiento que se usará si una regla de ILM utiliza este grupo de almacenamiento.

El nivel de almacenamiento, *incluye todos los niveles de almacenamiento*, abarca todos los Storage Nodes del emplazamiento seleccionado. Si has creado niveles de almacenamiento adicionales para los Storage Nodes de tu grid, aparecerán en el menú desplegable.

6. Si deseas utilizar el grupo de almacenamiento en un perfil de código de borrado multisitio, selecciona **Add more nodes** para añadir una entrada para cada sitio al grupo de almacenamiento.



Se te avisará si añades más de una entrada con distintos grados de almacenamiento para un sitio.

Para eliminar una entrada, selecciona el icono de eliminación .

7. Cuando estés satisfecho con tus selecciones, selecciona **Guardar**.

El nuevo grupo de almacenamiento se añade a la lista.

Ver detalles del pool de almacenamiento en StorageGRID

Puedes consultar los detalles de un grupo de almacenamiento para determinar dónde se utiliza dicho grupo y ver qué nodos y niveles de almacenamiento incluye.

Antes de empezar

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

Pasos

1. Selecciona **ILM > Storage pools**.

La tabla «Grupos de almacenamiento» incluye la siguiente información para cada grupo de almacenamiento que incluye nodos de almacenamiento:

- **Nombre:** El nombre de visualización único del storage pool.
- **Número de nodos:** el número de nodos en el grupo de almacenamiento.
- **Uso del almacenamiento:** El porcentaje del espacio total utilizable que se ha utilizado para los datos de objetos en este nodo. Este valor no incluye los metadatos de los objetos.
- **Capacidad total:** El tamaño del grupo de almacenamiento, que equivale a la cantidad total de espacio utilizable para los datos de los objetos de todos los nodos del grupo de almacenamiento.
- **Uso de ILM:** Cómo se está utilizando actualmente el grupo de almacenamiento. Un grupo de almacenamiento puede estar sin utilizar o puede estar siendo utilizado en una o varias reglas de ILM, perfiles de código de borrado o en ambos.

2. Para ver los detalles de un grupo de almacenamiento concreto, selecciona su nombre.

Aparece la página de detalles del grupo de almacenamiento.

3. Accede a la pestaña **Nodos** para obtener información sobre los Storage Nodes incluidos en el grupo de almacenamiento.

La tabla incluye la siguiente información para cada nodo:

- Nombre de nodo
- Nombre del sitio
- Nivel de almacenamiento
- Uso del almacenamiento: el porcentaje del espacio total utilizable para 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 objetos» para cada Storage Node (selecciona **Nodos > Storage Node > Storage**).

4. Consulta la pestaña **Uso de ILM** para determinar si el grupo de almacenamiento se está utilizando actualmente en alguna regla de ILM o en algún perfil de código de borrado.
5. Opcionalmente, ve a la **página de reglas de ILM** para conocer y gestionar cualquier regla que use el grupo de almacenamiento.

Consulta el "[Instrucciones para trabajar con reglas de ILM](#)".

Edita un pool de almacenamiento en StorageGRID

Puedes editar un grupo de almacenamiento para cambiar su nombre o para actualizar los sitios y los niveles de almacenamiento.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tienes "[permisos de acceso específicos](#)".
- Has revisado la "[Directrices para la creación de grupos de almacenamiento](#)".
- Si planeas editar un grupo de almacenamiento que está siendo usado por una regla en la política de ILM activa, ya has considerado cómo tus cambios afectarán la ubicación de los datos de los objetos.

Acerca de esta tarea

Si añades un nuevo emplazamiento o un nuevo nivel de almacenamiento a un grupo de almacenamiento que se utiliza en la política de ILM activa, ten en cuenta que los nodos de almacenamiento del nuevo emplazamiento o nivel de almacenamiento no se utilizarán automáticamente. Para forzar a StorageGRID a utilizar un nuevo emplazamiento o nivel de almacenamiento, debes activar una nueva política de ILM tras guardar el grupo de almacenamiento editado.

Pasos

1. Selecciona **ILM > Storage pools**.
2. Marca la casilla correspondiente al storage pool que deseas editar.

No puedes editar el grupo de almacenamiento All Storage Nodes (StorageGRID 11.6 y versiones anteriores).

3. Selecciona **Editar**.
4. Según sea necesario, cambia el nombre del grupo de almacenamiento.
5. Según sea necesario, selecciona otros sitios y niveles de almacenamiento.

No puedes cambiar la ubicación o el nivel de almacenamiento si el grupo de almacenamiento se usa en un perfil de código de borrado y el cambio haría que el esquema de código de borrado dejara de ser válido. Por ejemplo, si un grupo de almacenamiento usado en un perfil de código de borrado incluye actualmente un nivel de almacenamiento con solo una ubicación, no puedes usar un nivel de almacenamiento con dos ubicaciones porque el cambio haría que el esquema de código de borrado dejara de ser válido.



Añadir o eliminar sitios de un grupo de almacenamiento existente no moverá ningún dato existente codificado por borrado. Si quieres mover los datos existentes del sitio, debes crear un nuevo grupo de almacenamiento y un perfil de EC para volver a codificar los datos.

6. Selecciona **Guardar**.

Después de que termines

Si añadiste un nuevo sitio o un nuevo nivel de almacenamiento a un grupo de almacenamiento usado en la política de ILM activa, activa una nueva política de ILM para obligar a StorageGRID a usar el nuevo sitio o nivel de almacenamiento. Por ejemplo, clona tu política de ILM existente y luego activa la copia. Consulta ["Trabaja con reglas y políticas de ILM"](#).

Eliminar un pool de almacenamiento en StorageGRID

Puedes eliminar un grupo de almacenamiento que no se está utilizando.

Antes de empezar

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

Pasos

1. Selecciona **ILM > Storage pools**.
2. Consulta la columna «Uso de ILM» de la tabla para determinar si puedes eliminar el grupo de almacenamiento.

No puedes eliminar un grupo de almacenamiento si se está utilizando en una regla de ILM o en un perfil de código de borrado. Según sea necesario, selecciona **storage pool name > ILM usage** para determinar dónde se utiliza el grupo de almacenamiento.

3. Si el grupo de almacenamiento que quieres eliminar no se está utilizando, selecciona la casilla.
4. Selecciona **Eliminar**.
5. Selecciona **Aceptar**.

Usa grupos de almacenamiento en la nube

Conoce los Cloud Storage Pools en StorageGRID

Un grupo de almacenamiento en la nube te permite utilizar ILM para trasladar datos de objetos fuera de tu sistema StorageGRID. Por ejemplo, podrías querer trasladar objetos

a los que se accede con poca frecuencia a un almacenamiento en la nube de menor coste, como Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o el nivel de acceso Archive en el almacenamiento de blobs de Microsoft Azure. O quizá quieras mantener una copia de seguridad en la nube de los objetos de StorageGRID para mejorar la recuperación ante desastres.

Desde el punto de vista de ILM, un grupo de almacenamiento en la nube es similar a un grupo de almacenamiento. Para almacenar objetos en cualquiera de estas ubicaciones, seleccionas el grupo al crear las instrucciones de ubicación para una regla de ILM. Sin embargo, mientras que los grupos de almacenamiento están formados por nodos de almacenamiento dentro del sistema StorageGRID, un grupo de almacenamiento en la nube está formado por un bucket externo (S3) o un contenedor (Azure Blob storage).

La tabla compara los grupos de almacenamiento con los Cloud Storage Pools y muestra las similitudes y diferencias a grandes rasgos.

	Pool de almacenamiento	Grupo de almacenamiento en la nube
¿Cómo se crea?	Utilizando la opción ILM > Grupos de almacenamiento en Grid Manager.	Utilizando la opción ILM > Storage pools > Cloud Storage Pools en Grid Manager. Debes configurar el bucket o contenedor externo antes de poder crear el Cloud Storage Pool.
¿Cuántos grupos puedes crear?	Ilimitado.	Hasta 10.
¿Dónde se almacenan los objetos?	En uno o varios nodos de almacenamiento de StorageGRID.	En un bucket de Amazon S3, un contenedor de Azure Blob storage o en Google Cloud que es externo al sistema StorageGRID. Si el Cloud Storage Pool es un bucket de Amazon S3: • Si lo deseas, puedes configurar el ciclo de vida de un bucket para trasladar los objetos a un almacenamiento a largo plazo y de bajo coste, 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 de S3 RestoreObject. • Puedes crear Cloud Storage Pools para utilizarlos con AWS Commercial Cloud Services (C2S), que son compatibles con AWS Secret Region. Si el Cloud Storage Pool es un contenedor de Azure Blob storage, StorageGRID traslada el objeto al nivel Archive. Nota: En general, no configures la gestión del ciclo de vida del almacenamiento de blobs de Azure para el contenedor utilizado para un Cloud Storage Pool. Las operaciones RestoreObject en objetos en el Cloud Storage Pool pueden verse afectadas por el ciclo de vida configurado.

	Pool de almacenamiento	Grupo de almacenamiento en la nube
¿Qué determina la ubicación de los objetos?	Una regla de ILM en las políticas de ILM activas.	Una regla de ILM en las políticas de ILM activas.
¿Qué método de protección de datos se utiliza?	Replicación o codificación de borrado.	Replicación.
¿Cuántas copias de cada objeto se permiten?	Varios.	Una copia en el grupo de almacenamiento en la nube y, opcionalmente, una o más copias en StorageGRID. Nota: No puedes almacenar un objeto en más de un Cloud Storage Pool a la vez.
¿Cuáles son las ventajas?	Los objetos son accesibles rápidamente en cualquier momento.	Almacenamiento económico. Nota: Los datos de FabricPool no se pueden clasificar por niveles en Cloud Storage Pools.

Ciclo de vida de un objeto Cloud Storage Pool en StorageGRID

Antes de implementar Cloud Storage Pools, revisa el ciclo de vida de los objetos almacenados en cada tipo de Cloud Storage Pool.

S3: ciclo de vida de un objeto del Cloud Storage Pool

Estos pasos describen las fases del ciclo de vida de un objeto almacenado en un S3 Cloud Storage Pool.



El término «Glacier» hace referencia tanto a la clase de almacenamiento Glacier como a la clase de almacenamiento Glacier Deep Archive, con una excepción: la clase de almacenamiento Glacier Deep Archive no admite el nivel de restauración Expedited. Solo se admite la recuperación Bulk o Standard.



Google Cloud Platform (GCP) permite recuperar objetos del almacenamiento a largo plazo sin necesidad de realizar una operación POST Restore.

1. Objeto almacenado en StorageGRID

Para iniciar el ciclo de vida, una aplicación cliente almacena un objeto en StorageGRID.

2. Objeto trasladado al grupo de almacenamiento en la nube S3

- Cuando el objeto coincide con una regla de ILM que utiliza un grupo de almacenamiento en la nube S3 como ubicación de almacenamiento, StorageGRID mueve el objeto al bucket S3 externo especificado por el Cloud Storage Pool.

- Cuando el objeto se ha movido al grupo de almacenamiento en la nube S3, la aplicación cliente puede recuperarlo usando una solicitud S3 GetObject desde StorageGRID, a menos que el objeto haya sido trasladado al almacenamiento Glacier.

3. Objeto transferido a Glacier (estado no recuperable)

- Opcionalmente, el objeto puede trasladarse al almacenamiento Glacier. Por ejemplo, el bucket externo de S3 podría utilizar la configuración del ciclo de vida para trasladar un objeto al almacenamiento Glacier de forma inmediata o tras un determinado número de días.



Si deseas realizar la transición de objetos, debes crear una configuración de ciclo de vida para el bucket externo de S3 y debes usar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y sea compatible con la API RestoreObject de S3.

- Durante la transición, la aplicación cliente puede usar una solicitud S3 HeadObject para supervisar el estado del objeto.

4. Objeto recuperado del almacenamiento de Glacier

Si un objeto se ha trasladado al almacenamiento Glacier, la aplicación cliente puede enviar una solicitud S3 RestoreObject para restaurar una copia recuperable en el grupo de almacenamiento en la nube de S3. La solicitud especifica durante cuántos días debe estar disponible la copia en el grupo de almacenamiento en la nube y el nivel de acceso a los datos que se utilizará para la operación de restauración (Expedited, Standard o Bulk). Cuando se alcanza la fecha de caducidad de la copia recuperable, esta vuelve automáticamente a un estado no recuperable.



Si también existen una o más copias del objeto en los nodos de almacenamiento de StorageGRID, no es necesario restaurar el objeto desde Glacier mediante una solicitud RestoreObject. En su lugar, la copia local se puede recuperar directamente mediante una solicitud GetObject.

5. Objeto recuperado

Una vez que se ha restaurado un objeto, la aplicación cliente puede enviar una solicitud de GetObject para recuperar el objeto restaurado.

Azure: ciclo de vida de un objeto de un Cloud Storage Pool

Estos pasos describen las fases 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 trasladado al grupo de almacenamiento en la nube de Azure

Cuando el objeto coincide con una regla de ILM que utiliza un grupo de almacenamiento en la nube de Azure como ubicación de almacenamiento, StorageGRID mueve el objeto al contenedor externo de Azure Blob storage especificado por el Cloud Storage Pool.

3. Objeto trasladado al nivel de archivo (estado no recuperable)

Inmediatamente después de trasladar el objeto al grupo de almacenamiento en la nube de Azure,

StorageGRID traslada automáticamente el objeto al nivel de archivo de Azure Blob storage.

4. Objeto recuperado del nivel Archive

Si un objeto se ha trasladado al nivel Archive, la aplicación cliente puede enviar una solicitud S3 RestoreObject para restaurar una copia recuperable en el Azure Cloud Storage Pool.

Cuando StorageGRID recibe la RestoreObject, traslada temporalmente el objeto al nivel Cool del almacenamiento de blobs de Azure. En cuanto se alcanza la fecha de caducidad en la solicitud RestoreObject, StorageGRID traslada el objeto de nuevo al nivel Archive.



Si también existen una o más copias del objeto en los nodos de almacenamiento de StorageGRID, no es necesario restaurar el objeto desde el nivel de acceso Archive mediante una solicitud RestoreObject. En su lugar, la copia local se puede recuperar directamente mediante una solicitud GetObject.

5. Objeto recuperado

Una vez que se ha restaurado un objeto en el grupo de almacenamiento en la nube de Azure, la aplicación cliente puede enviar una solicitud de GetObject para recuperar el objeto restaurado.

Información relacionada

["Usa la API de REST de S3"](#)

Casos de uso de Cloud Storage Pool en StorageGRID

Con los Cloud Storage Pools, puedes hacer backup o clasificar datos por niveles en una ubicación externa. Además, puedes hacer backup o clasificar datos por niveles en más de una nube.

Haz una copia de seguridad de los datos de StorageGRID en una ubicación externa

Puedes utilizar un Cloud Storage Pool para hacer backup de los objetos de StorageGRID en una ubicación externa.

Si no se puede acceder a las copias de StorageGRID, se pueden utilizar los datos de los objetos del Cloud Storage Pool para atender las solicitudes de los clientes. No obstante, es posible que tengas que enviar una solicitud S3 RestoreObject para acceder a la copia de backup del objeto en el Cloud Storage Pool.

Los datos de los objetos de un Cloud Storage Pool también pueden utilizarse para recuperar datos perdidos de StorageGRID debido a un fallo en un volumen de almacenamiento o en un Storage Node. Si la única copia restante de un objeto está en un Cloud Storage Pool, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el Storage Node recuperado.

Para implementar una solución de backup:

1. Crea un único Cloud Storage Pool.
2. Configura una regla de ILM que almacene simultáneamente copias de objetos en Storage Nodes (como copias replicadas o con código de borrado) y una única copia de objeto en el Cloud Storage Pool.
3. Añade la regla a tu política de ILM. Luego, simula y activa la política.

Transfiere datos de niveles de StorageGRID a una ubicación externa

Puedes utilizar un grupo de almacenamiento en la nube para almacenar objetos fuera del sistema StorageGRID. Por ejemplo, supón que tienes un gran número de objetos que necesitas conservar, pero esperas acceder a esos objetos rara vez, si es que alguna vez lo haces. Puedes utilizar un grupo de almacenamiento en la nube para trasladar los objetos a un almacenamiento de menor coste y liberar espacio en StorageGRID.

Para implementar una solución de tiering:

1. Crea un único Cloud Storage Pool.
2. Configura una regla de ILM que traslade los objetos que se utilizan con poca frecuencia de los Storage Nodes al Cloud Storage Pool.
3. Añade la regla a tu política de ILM. Luego, simula y activa la política.

Gestiona múltiples puntos de conexión en la nube

Puedes configurar varios endpoints de Cloud Storage Pool si quieres clasificar por niveles o hacer backup de los datos de objetos en más de una nube. Los filtros en tus reglas de ILM te permiten especificar qué objetos se almacenan en cada Cloud Storage Pool. Por ejemplo, podrías querer almacenar objetos de algunos tenants o buckets en Amazon S3 Glacier y objetos de otros tenants o buckets en Azure Blob storage. O podrías querer mover datos entre Amazon S3 Glacier y Azure Blob storage.



Quando utilices varios puntos de conexión de Cloud Storage Pool, ten en cuenta que un objeto solo puede almacenarse en un Cloud Storage Pool a la vez.

Para implementar varios puntos de conexión en la nube:

1. Crea hasta 10 Cloud Storage Pools.
2. Configura las reglas de ILM para almacenar los datos de objetos adecuados en el momento adecuado en cada Cloud Storage Pool. Por ejemplo, almacena objetos del bucket A en Cloud Storage Pool A y objetos del bucket B en Cloud Storage Pool B. O bien, almacena objetos en Cloud Storage Pool A durante un tiempo y luego muévelos a Cloud Storage Pool B.
3. Añade las reglas a tu política de ILM. Luego, simula y activa la política.

Requisitos y límites de Cloud Storage Pool en StorageGRID

Si tienes previsto usar un Cloud Storage Pool para mover objetos fuera del sistema StorageGRID, debes revisar las consideraciones para configurar y usar Cloud Storage Pools.

Consideraciones generales

- En general, el almacenamiento de archivo en la nube, como Amazon S3 Glacier o Azure Blob storage, es una opción económica para almacenar datos de objetos. Sin embargo, los costes de recuperar datos del almacenamiento de archivo en la nube son relativamente elevados. Para lograr el menor coste total, debes tener en cuenta cuándo y con qué frecuencia accederás a los objetos en el Cloud Storage Pool. Se recomienda usar un Cloud Storage Pool solo para contenido que esperas acceder con poca frecuencia.
- No se admite el uso de Cloud Storage Pools con FabricPool debido a la latencia adicional para recuperar un objeto del destino de Cloud Storage Pool.
- Los objetos con S3 Object Lock habilitado no se pueden colocar en Cloud Storage Pools.

- Las siguientes combinaciones de plataforma, autenticación y protocolo con S3 Object lock no son compatibles para Cloud Storage Pools:
 - **Plataformas:** Google Cloud Platform y Azure
 - **Tipos de autenticación:** Acceso anónimo
 - **Protocolo:** HTTP

Consideraciones para los puertos utilizados para Cloud Storage Pools

Para garantizar que las reglas de ILM puedan mover objetos hacia y desde el Cloud Storage Pool especificado, debes configurar la red o redes que contienen los Storage Nodes de tu sistema. Debes asegurarte de que los siguientes puertos puedan comunicarse con el Cloud Storage Pool.

De forma predeterminada, los grupos de almacenamiento en la nube utilizan los siguientes puertos:

- **80:** Para los URI de puntos finales que comienzan con http
- **443:** Para los URI de endpoint que comienzan con https

Puedes especificar un puerto diferente cuando creas o editas un Cloud Storage Pool.

Si utilizas un proxy no transparente, también debes ["configurar un proxy de almacenamiento"](#) para permitir el envío de mensajes a puntos finales externos, como un punto final en internet.

Consideraciones para los costes

El acceso al almacenamiento en la nube usando un Cloud Storage Pool requiere conectividad de red con la nube. Debes tener en cuenta el coste de la infraestructura de red que vas a utilizar para acceder a la nube y aprovisionarla adecuadamente, según la cantidad de datos que esperas mover entre StorageGRID y la nube usando el Cloud Storage Pool.

Cuando StorageGRID se conecta al punto final externo del Cloud Storage Pool, envía varias solicitudes para supervisar la conectividad y asegurarse de que puede realizar las operaciones necesarias. Aunque estas solicitudes conllevan algunos costes adicionales, el coste de supervisar un Cloud Storage Pool solo debería ser una pequeña fracción del coste total de almacenar objetos en S3 o Azure.

Podrían generarse costes más elevados si necesitas trasladar objetos desde un endpoint externo de Cloud Storage Pool de vuelta a StorageGRID. Los objetos podrían trasladarse de vuelta a StorageGRID en cualquiera de estos casos:

- La única copia del objeto se encuentra en un Cloud Storage Pool y decides almacenarlo en StorageGRID en su lugar. En este caso, reconfiguras tus reglas y políticas de ILM. Cuando se lleva a cabo la evaluación de ILM, StorageGRID envía varias solicitudes para recuperar el objeto del Cloud Storage Pool. Luego, StorageGRID crea localmente el número especificado de copias replicadas o con código de borrado. Después de que el objeto se traslada de nuevo a StorageGRID, se elimina la copia en el Cloud Storage Pool.
- Los objetos se pierden debido a un fallo del nodo de almacenamiento. Si la única copia restante de un objeto se encuentra en un Cloud Storage Pool, StorageGRID restaura temporalmente el objeto y crea una nueva copia en el nodo de almacenamiento recuperado.



Cuando se devuelven objetos a StorageGRID desde un Cloud Storage Pool, StorageGRID envía varias solicitudes al endpoint del Cloud Storage Pool por cada objeto. Antes de mover un gran número de objetos, ponte en contacto con soporte técnico para que te ayuden a estimar el plazo y los costes asociados.

S3: permisos necesarios para el depósito del Cloud Storage Pool

Las políticas del bucket externo de S3 utilizado para un Cloud Storage Pool deben conceder a StorageGRID permiso para mover un objeto al bucket, obtener el estado de un objeto, restaurar un objeto desde el almacenamiento de Glacier cuando sea necesario y más. Lo ideal es que StorageGRID tenga acceso con control total al bucket (`s3:*`); sin embargo, si esto no es posible, la política del bucket debe conceder los siguientes permisos de 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 bucket externo

El movimiento de objetos entre StorageGRID y el bucket externo de S3 especificado en el Cloud Storage Pool se controla mediante las reglas de ILM y las políticas de ILM activas en StorageGRID. Por el contrario, la transición de objetos desde el bucket externo de S3 especificado en el Cloud Storage Pool a Amazon S3 Glacier o S3 Glacier Deep Archive (o a una solución de almacenamiento que implemente la clase de almacenamiento Glacier) se controla mediante la configuración del ciclo de vida de ese bucket.

Si deseas trasladar objetos desde el Cloud Storage Pool, debes crear la configuración de ciclo de vida adecuada en el bucket externo de S3 y debes usar una solución de almacenamiento que implemente la clase de almacenamiento Glacier y sea compatible con la API S3 `RestoreObject`.

Por ejemplo, supongamos que quieres que todos los objetos que se trasladen desde StorageGRID al Cloud Storage Pool pasen inmediatamente al almacenamiento Amazon S3 Glacier. Deberías crear una configuración de ciclo de vida en el bucket externo de S3 que especifique una única acción (**Transition**) 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 los buckets a Amazon S3 Glacier el mismo 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 bucket externo, nunca utilices acciones de **Expiration** para definir cuándo expiran los objetos. Las acciones de Expiration hacen que el sistema de almacenamiento externo elimine los objetos expirados. Si más adelante intentas acceder a un objeto expirado desde StorageGRID, el objeto eliminado no se encontrará.

Si deseas trasladar los objetos del Cloud Storage Pool a S3 Glacier Deep Archive (en lugar de a Amazon S3 Glacier), especifica `<StorageClass>DEEP_ARCHIVE</StorageClass>` en el ciclo de vida del bucket. Sin embargo, ten en cuenta que no puedes usar el tier `Expedited` para restaurar objetos desde S3 Glacier Deep Archive.

Azure: consideraciones sobre el nivel de acceso

Al configurar una cuenta de almacenamiento de Azure, puedes establecer el nivel de acceso predeterminado en Hot o Cool. Al crear una cuenta de almacenamiento para usarla con un Cloud Storage Pool, debes usar el nivel Hot como nivel predeterminado. Aunque StorageGRID establece inmediatamente el nivel en Archive al mover objetos al Cloud Storage Pool, usar la configuración predeterminada Hot asegura que no se te cobre una tarifa por eliminación anticipada por los objetos eliminados del nivel Cool antes del mínimo de 30 días.

Azure: no se admite la gestión del ciclo de vida

No utilices la gestión del ciclo de vida del almacenamiento de blobs de Azure para el contenedor que se utiliza con un Cloud Storage Pool. Las operaciones del ciclo de vida podrían interferir con las operaciones de Cloud Storage Pool.

Información relacionada

["Crear un grupo de almacenamiento en la nube"](#)

Cloud Storage Pools y replicación CloudMirror en StorageGRID

Al empezar 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 CloudMirror de StorageGRID.

	Grupo de almacenamiento en la nube	Servicio de replicación de CloudMirror
¿Cuál es el objetivo principal?	Actúa como destino de archivo. La copia del objeto en el Cloud Storage Pool puede ser la única copia del objeto o puede ser una copia adicional. Es decir, en lugar de conservar dos copias en las instalaciones, puedes conservar una copia en StorageGRID y enviar una copia al Cloud Storage Pool.	Permite a un inquilino replicar automáticamente objetos desde un bucket en StorageGRID (origen) a un bucket externo de S3 (destino). Crea una copia independiente de un objeto en una infraestructura independiente de S3.

	Grupo de almacenamiento en la nube	Servicio de replicación de CloudMirror
¿Cómo se configura?	Se definen de la misma forma que los grupos de almacenamiento, usando Grid Manager o la Grid Management API. Se pueden seleccionar como ubicación de colocación en una regla de ILM. Mientras que un grupo de almacenamiento está formado por un conjunto de Storage Nodes, un Cloud Storage Pool se define usando un endpoint remoto de S3 o Azure (dirección IP, credenciales, y así sucesivamente).	Un usuario de un inquilino "configura la replicación de CloudMirror" definiendo un punto final CloudMirror (dirección IP, credenciales, etc.) mediante el Gestor de inquilinos o la API de S3. Una vez configurado el punto final CloudMirror, cualquier depósito que pertenezca a esa cuenta de inquilino se puede configurar para que apunte al punto final CloudMirror.
¿Quién se encarga de configurarlo?	Normalmente, un administrador de la grid	Normalmente, un usuario de tenant
¿Cuál es el destino?	• Cualquier infraestructura S3 compatible (incluido Amazon S3) • Nivel de archivo de Azure Blob • Google Cloud Platform (GCP)	• Cualquier infraestructura S3 compatible (incluido Amazon S3) • Google Cloud Platform (GCP)
¿Qué hace que los objetos se trasladen al destino?	Una o varias reglas de ILM en las políticas de ILM activas. Las reglas de ILM definen qué objetos StorageGRID mueve al Cloud Storage Pool y cuándo se mueven los objetos.	La acción de ingerir un nuevo objeto en un bucket de origen que se haya configurado con un endpoint CloudMirror. Los objetos que existían en el bucket de origen antes de que el bucket se configurara con el endpoint CloudMirror no se replican, a menos que se modifiquen.
¿Cómo se recuperan los objetos?	Las aplicaciones deben enviar solicitudes a StorageGRID para recuperar objetos que se hayan trasladado a un Cloud Storage Pool. Si la única copia de un objeto se ha trasladado al almacenamiento de archivo, StorageGRID gestiona el proceso de restauración del objeto para que pueda recuperarse.	Dado que la copia duplicada en el bucket de destino es una copia independiente, las aplicaciones pueden recuperar el objeto enviando solicitudes tanto a StorageGRID como al destino S3. Por ejemplo, supongamos que usas la replicación de CloudMirror para duplicar objetos en una organización asociada. La organización asociada puede usar sus propias aplicaciones para leer o actualizar objetos directamente desde el destino S3. No es necesario usar StorageGRID.
¿Puedes leer directamente desde el destino?	No. Los objetos trasladados a un Cloud Storage Pool son gestionados por StorageGRID. Las solicitudes de lectura deben dirigirse a StorageGRID (y StorageGRID será responsable de recuperarlos del Cloud Storage Pool).	Sí, porque la copia reflejada es una copia independiente.

	Grupo de almacenamiento en la nube	Servicio de replicación de CloudMirror
¿Qué ocurre si se elimina un objeto de la fuente?	El objeto también se elimina del Cloud Storage Pool.	La acción de eliminación no se replica. Un objeto eliminado deja de existir en el depósito de StorageGRID, pero sigue existiendo en el depósito de destino. Del mismo modo, los objetos del depósito de destino pueden eliminarse sin afectar al de origen.
¿Cómo accedes a los objetos después de un desastre (cuando el sistema StorageGRID no está operativo)?	Los nodos de StorageGRID que hayan fallado deben recuperarse. Durante este proceso, es posible que se restauren copias de objetos replicados utilizando las copias en el Cloud Storage Pool.	Las copias de los objetos en el destino CloudMirror son independientes de StorageGRID, así que puedes acceder a ellas directamente antes de que se recuperen los nodos de StorageGRID.

Crea un Cloud Storage Pool en StorageGRID

Un grupo de almacenamiento en la nube especifica un único bucket externo de Amazon S3, otro proveedor compatible con S3 o un contenedor de almacenamiento de blobs de Azure.

Al crear un grupo de almacenamiento en la nube, debes especificar el nombre y la ubicación del bucket o contenedor externo que StorageGRID utilizará 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 bucket o contenedor externo.

StorageGRID valida el Cloud Storage Pool en cuanto lo guardas, así que debes asegurarte de que el bucket o contenedor especificado en el Cloud Storage Pool exista y sea accesible.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["permisos de acceso necesarios"](#).
- Has revisado la ["Consideraciones para Cloud Storage Pools"](#).
- El bucket o contenedor externo al que hace referencia el Cloud Storage Pool ya existe, y tienes el [información sobre el endpoint del servicio](#).
- Para acceder al bucket o al contenedor, tienes la [información de la cuenta para el tipo de autenticación](#) que elijas.

Pasos

1. Selecciona **ILM > Storage pools > Cloud Storage Pools**.
2. Selecciona **Crear** y luego introduce la siguiente información:

Campo	Descripción
Nombre del Cloud Storage Pool	Un nombre que describa brevemente el Cloud Storage Pool y su finalidad. Utiliza un nombre que resulte fácil de identificar a la hora de configurar las reglas de ILM.
Tipo de proveedor	¿Qué proveedor de servicios en la nube vas a utilizar para este Cloud Storage Pool: • Amazon S3/GCP: Selecciona esta opción para Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) u otro proveedor compatible con S3. • Azure Blob Storage
Bucket o contenedor	El nombre del bucket externo de S3 o del contenedor de Azure. No puedes cambiar este valor después de guardar el Cloud Storage Pool.

3. En función del tipo de proveedor que hayas seleccionado, introduce la información del punto final del servicio.

Amazon S3/GCP

- a. Para el protocolo, selecciona HTTPS o HTTP.



No utilices conexiones HTTP para datos confidenciales.

- b. Introduce el nombre de host. Ejemplo:

`s3-aws-region.amazonaws.com`

- c. Selecciona el estilo de la URL:

Opción	Descripción
Detección automática	Intenta detectar automáticamente qué estilo de URL usar, basándose en la información proporcionada. Por ejemplo, si especificas una dirección IP, StorageGRID usará una URL de tipo path. Selecciona esta opción solo si no sabes qué estilo específico usar.
Estilo de alojamiento virtual	Utiliza una URL de tipo «host virtual» para acceder al bucket. Las URL de tipo «host virtual» incluyen el nombre del bucket como parte del nombre de dominio. Ejemplo: <code>https://bucket-name.s3.company.com/key-name</code>
Estilo path	Utiliza una URL de tipo path para acceder al bucket. Las URL de tipo path incluyen el nombre del bucket al final. Ejemplo: <code>https://s3.company.com/bucket-name/key-name</code> Nota: No se recomienda utilizar la opción de URL de tipo «path» y dejará de estar disponible en una futura versión de StorageGRID.

- d. Si lo deseas, introduce el número de puerto o utiliza el puerto predeterminado: 443 para HTTPS o 80 para HTTP.

Almacenamiento de blobs de Azure

- a. Introduce el URI del endpoint del servicio utilizando uno de los siguientes formatos.

- `https://host:port`
- `http://host:port`

Ejemplo: `https://myaccount.blob.core.windows.net:443`

Si no especificas un puerto, por defecto se usa el puerto 443 para HTTPS y el puerto 80 para HTTP.

4. Selecciona **Continuar**. Luego selecciona el tipo de autenticación e introduce la información necesaria para el endpoint del Cloud Storage Pool:

Clave de acceso

Para Amazon S3/GCP u otros proveedores compatibles con S3

- a. **ID de la clave de acceso:** Introduce el ID de la clave de acceso de la cuenta propietaria del bucket externo.
- b. **Clave de acceso secreta:** introduce la clave de acceso secreta.

IAM Roles Anywhere

Para el servicio AWS IAM Roles Anywhere

StorageGRID utiliza el Servicio de tokens de seguridad (STS) de AWS para generar dinámicamente un token de corta duración que permite acceder a los recursos de AWS.

- a. **Región de AWS IAM Roles Anywhere:** Selecciona la región para el Cloud Storage Pool. Por ejemplo, `us-east-1`.
- b. **URN del ancla de confianza:** Introduce el URN del ancla de confianza que valida las solicitudes de credenciales STS de corta duración. Puede ser una CA raíz o intermedia.
- c. **URN del perfil:** Introduce el URN del perfil de IAM Roles Anywhere que enumera los roles que puede asumir cualquier persona de confianza.
- d. **URN del rol:** Introduce el URN del rol de IAM que pueda asumir cualquier persona de confianza.
- e. **Duración de la sesión:** Introduce la duración de las credenciales de seguridad temporales y de la sesión de rol. Introduce un valor de al menos 15 minutos y no más de 12 horas.
- f. **Certificado de CA del servidor** (opcional): uno o varios certificados de CA de confianza, en formato PEM, para verificar el servidor de IAM Roles Anywhere. Si no se incluye, el servidor no se verificará.
- g. **Certificado de entidad final:** La clave pública, en formato PEM, del certificado X509 firmado por el trust anchor. AWS IAM Roles Anywhere utiliza esta clave para emitir un token STS.
- h. **Clave privada de la entidad final:** la clave privada del certificado de la entidad final.

CAP (portal de acceso C2S)

Para el servicio S3 de Commercial Cloud Services (C2S)

- a. **URL de credenciales temporales:** Introduce la URL completa que StorageGRID utilizará para obtener credenciales temporales del servidor CAP, incluyendo todos los parámetros de API obligatorios y opcionales asignados a tu cuenta C2S.
- b. **Certificado de CA del servidor:** Selecciona **Examinar** y carga el certificado de CA que StorageGRID utilizará para verificar el servidor CAP. El certificado debe estar codificado en formato PEM y haber sido emitido por una autoridad de certificación (CA) gubernamental adecuada.
- c. **Certificado de cliente:** Selecciona **Examinar** y carga el certificado que StorageGRID utilizará para identificarse ante el servidor CAP. El certificado de cliente debe estar codificado en formato PEM, emitido por una autoridad de certificación (CA) gubernamental adecuada y tener acceso a tu cuenta de C2S.
- d. **Clave privada del cliente:** Selecciona **Examinar** y carga la clave privada codificada en formato PEM para el certificado de cliente.
- e. Si la clave privada del cliente está cifrada, introduce la frase de contraseña para descifrar la clave privada del cliente. En caso contrario, deja en blanco el campo **Frase de contraseña de la clave**

privada del cliente.



Si el certificado de cliente va a estar cifrado, utiliza el formato tradicional para el cifrado. No se admite el formato cifrado PKCS #8.

Almacenamiento de blobs de Azure

Solo para Azure Blob Storage, clave compartida

- Nombre de la cuenta:** Introduce el nombre de la cuenta de almacenamiento que es propietaria del contenedor externo
- Clave de la cuenta:** Ingresa la clave secreta para la cuenta de almacenamiento

Puedes utilizar el portal de Azure para encontrar estos valores.

Anónimo

No se requiere información adicional.

5. Selecciona **Continuar**. Luego elige el tipo de verificación del servidor que quieres usar:

Opción	Descripción
Usa certificados de CA raíz en el sistema operativo del nodo de almacenamiento	Utiliza los certificados CA de Grid instalados en el sistema operativo para proteger las conexiones.
Usa un certificado de CA personalizado	Utiliza un certificado de CA personalizado. Selecciona Examinar y sube el certificado codificado en formato PEM.
No verificar el certificado	Seleccionar esta opción significa que las conexiones TLS al Cloud Storage Pool no son seguras.

6. Selecciona **Guardar**.

Al guardar un grupo de almacenamiento en la nube, StorageGRID realiza lo siguiente:

- Comprueba que el bucket o contenedor y el punto final del servicio existan y que se pueda acceder a ellos utilizando las credenciales que hayas especificado.
- Escribe un archivo de marcador en el bucket o contenedor para identificarlo como un Cloud Storage Pool. Nunca elimines este archivo, que se llama `x-ntap-sgws-cloud-pool-uuid`.

Si falla la validación del Cloud Storage Pool, recibirás un mensaje de error que explica por qué falló la validación. Por ejemplo, podría aparecer un error si hay un problema con el certificado o si el bucket o contenedor que especificaste no existe todavía.

7. Si se produce un error, consulta la "[Instrucciones para solucionar problemas de Cloud Storage Pools](#)", resuelve cualquier problema y luego intenta guardar el Cloud Storage Pool de nuevo.

Ver detalles de Cloud Storage Pool en StorageGRID

Puedes consultar los detalles de un Cloud Storage Pool para determinar dónde se utiliza

y ver qué nodos y niveles de almacenamiento incluye.

Antes de empezar

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

Pasos

1. Selecciona **ILM > Storage pools > Cloud Storage Pools**.

La tabla «Cloud Storage Pools» incluye la siguiente información para cada Cloud Storage Pool que incluye Storage Nodes:

- **Nombre:** El nombre de visualización único del pool.
- **URI:** El identificador uniforme de recursos del Cloud Storage Pool.
- **Tipo de proveedor:** qué proveedor de cloud se utiliza para este Cloud Storage Pool.
- **Contenedor:** El nombre del bucket utilizado para el Cloud Storage Pool.
- **Uso de ILM:** cómo se está utilizando actualmente el pool. Un Cloud Storage Pool puede estar sin usar o puede estar siendo usado en una o varias reglas de ILM, perfiles de erasure-coding o ambos.
- **Último error:** El último error detectado durante una comprobación de estado de este Cloud Storage Pool.

2. Para ver los detalles de un Cloud Storage Pool específico, selecciona su nombre.

Aparece la página de detalles del pool.

3. Accede a la pestaña **Autenticación** para conocer el tipo de autenticación de este Cloud Storage Pool y para modificar los datos de autenticación.
4. Accede a la pestaña **Verificación del servidor** para consultar los detalles de la verificación, editar la verificación, descargar un nuevo certificado o copiar el certificado PEM.
5. Consulta la pestaña **Uso de ILM** para determinar si el Cloud Storage Pool se está utilizando actualmente en alguna regla de ILM o en algún perfil de código de borrado.
6. Si lo deseas, ve a la **página de reglas de ILM** para ["conocer y gestionar cualquier norma"](#) que usan el Cloud Storage Pool.

Edita un Cloud Storage Pool en StorageGRID

Puedes editar un grupo de almacenamiento en la nube para cambiar su nombre, el punto final del servicio u otros detalles; sin embargo, no puedes cambiar el S3 bucket ni el Azure container de un grupo de almacenamiento en la nube.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).
- Has revisado la ["Consideraciones para Cloud Storage Pools"](#).

Pasos

1. Selecciona **ILM > Storage pools > Cloud Storage Pools**.

La tabla «Cloud Storage Pools» muestra los Cloud Storage Pools existentes.

2. Marca la casilla correspondiente al Cloud Storage Pool que quieras editar y, a continuación, selecciona **Actions > Edit**.

También puedes seleccionar el nombre del Cloud Storage Pool y luego seleccionar **Editar**.

3. Según sea necesario, cambia el nombre del Cloud Storage Pool, el service endpoint, las credenciales de autenticación o el método de verificación de certificados.



No puedes cambiar el tipo de proveedor, ni el bucket de S3 ni el contenedor de Azure para un Cloud Storage Pool.

Si ya has subido un certificado de servidor o de cliente, puedes desplegar el acordeón **Detalles del certificado** para consultar el certificado que se está utilizando actualmente.

4. Selecciona **Guardar**.

Al guardar un grupo de almacenamiento en la nube, StorageGRID comprueba que el depósito o contenedor y el punto final del servicio existan, y que se pueda acceder a ellos utilizando las credenciales que hayas especificado.

Si falla la validación del grupo de almacenamiento en la nube, se muestra un mensaje de error. Por ejemplo, podría aparecer un error si hay un error de certificado.

Consulta las instrucciones de "[Solución de problemas de Cloud Storage Pools](#)", resuelve el problema y luego intenta guardar el Cloud Storage Pool de nuevo.

Eliminar un Cloud Storage Pool en StorageGRID

Puedes eliminar un grupo de almacenamiento en la nube si no se usa en una regla de ILM y no contiene datos de objetos.

Antes de empezar

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

Si es necesario, utiliza ILM para mover los datos de los objetos

Si el Cloud Storage Pool que deseas eliminar contiene datos de objetos, debes utilizar ILM para trasladar los datos a otra ubicación. Por ejemplo, puedes trasladar los datos a Storage Nodes en tu grid o a otro Cloud Storage Pool.

Pasos

1. Selecciona **ILM > Storage pools > Cloud Storage Pools**.
2. Consulta la columna de uso de ILM en la tabla para determinar si puedes eliminar el Cloud Storage Pool.

No puedes eliminar un Cloud Storage Pool si se está usando en una regla de ILM o en un perfil de erasure-coding.
3. Si se está utilizando el Cloud Storage Pool, selecciona **cloud storage pool name > ILM usage**.
4. "[Clona cada regla de ILM](#)" que actualmente coloca objetos en el Cloud Storage Pool que quieres eliminar.
5. Decide a dónde quieres mover los objetos existentes gestionados por cada regla que clonaste.

Puedes utilizar uno o varios grupos de almacenamiento o un Cloud Storage Pool diferente.

6. Edita cada una de las reglas que clonaste.

En el paso 2 del asistente para crear una regla de ILM, selecciona la nueva ubicación en el campo **copias en**.

7. "[Crear una nueva política de ILM](#)" y sustituye cada una de las reglas antiguas por una regla clonada.

8. Activa la nueva política.

9. Espera a que ILM elimine los objetos del Cloud Storage Pool y los coloque en la nueva ubicación.

Eliminar Cloud Storage Pool

Cuando el grupo de almacenamiento en la nube está vacío y no se usa en ninguna regla de ILM, puedes eliminarlo.

Antes de empezar

- Has eliminado todas las reglas de ILM que pudieran haber utilizado el pool.
- Has confirmado que el bucket de S3 o el contenedor de Azure no contiene ningún objeto.

Se produce un error si intentas eliminar un grupo de almacenamiento en la nube que contenga objetos. Consulta "[Soluciona problemas de los grupos de almacenamiento en la nube](#)".



Al crear 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 elimines este archivo, que se llama `x-ntap-sgws-cloud-pool-uuid`.

Pasos

1. Selecciona **ILM > Storage pools > Cloud Storage Pools**.
2. Si la columna «Uso de ILM» indica que no se está utilizando Cloud Storage Pool, marca la casilla.
3. Selecciona **Acciones > Eliminar**.
4. Selecciona **Aceptar**.

Soluciona problemas de los Cloud Storage Pools en StorageGRID

Sigue estos pasos de resolución de problemas para solucionar los errores que puedas encontrar al crear, editar o eliminar un Cloud Storage Pool.

Determina si se ha producido un error

StorageGRID realiza una sencilla comprobación de estado en cada Cloud Storage Pool leyendo el objeto conocido `x-ntap-sgws-cloud-pool-uuid` para garantizar que se puede acceder al Cloud Storage Pool y que está funcionando correctamente. Cuando StorageGRID detecta un error en el endpoint, realiza una comprobación de estado cada minuto desde cada Storage Node. Cuando se resuelve el error, las comprobaciones de estado se detienen. Si una comprobación de estado detecta un problema, se muestra un mensaje en la columna Last error de la tabla Cloud Storage Pools en la página Storage pools.

La tabla muestra el error más reciente detectado para cada Cloud Storage Pool e indica hace cuánto ocurrió el error.

Además, se activa una alerta de **Cloud Storage Pool connectivity error** si la comprobación de estado detecta que se han producido uno o más errores nuevos en Cloud Storage Pool en los últimos 5 minutos. Si recibes una notificación por correo electrónico sobre esta alerta, ve a la página Storage pools (selecciona **ILM > Storage pools**), revisa los mensajes de error en la columna Last error y consulta las pautas de resolución de problemas que aparecen a continuación.

Comprueba si se ha solucionado un error

Después de resolver cualquier problema subyacente, puedes comprobar si el error se ha solucionado. En la página Cloud Storage Pool, selecciona el endpoint y selecciona **Borrar error**. Un mensaje de confirmación indica que StorageGRID ha borrado el error del Cloud Storage Pool.

Si se ha resuelto el problema subyacente, el mensaje de error ya no aparecerá. Sin embargo, si el problema subyacente no se ha solucionado (o si se produce un error diferente), el mensaje de error aparecerá en la columna Last error en unos minutos.

Error: Fallo en la comprobación de estado. Error del endpoint

Es posible que te encuentres con este error al habilitar S3 Object Lock con la retención predeterminada para tu bucket de Amazon S3 después de empezar a usar este bucket para un Cloud Storage Pool. Este error se produce cuando la operación PUT no incluye un encabezado HTTP con un valor de suma de comprobación de la carga útil, como `Content-MD5`. Este valor de encabezado es obligatorio para AWS en las operaciones PUT en buckets con S3 Object Lock habilitado.

Para solucionar este problema, sigue los pasos que se indican en ["Editar un Cloud Storage Pool"](#) sin realizar ningún cambio. Esta acción activa la validación de la configuración del Cloud Storage Pool, que detecta y actualiza automáticamente la bandera S3 Object Lock en la configuración del endpoint del Cloud Storage Pool.

Error: Este grupo de almacenamiento en la nube contiene contenido inesperado

Es posible que te encuentres con este error al intentar crear, editar o eliminar un grupo de almacenamiento en la nube. Este error se produce si el bucket o el 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, este error solo aparecerá si estás creando un nuevo Cloud Storage Pool y ya hay otra instancia de StorageGRID utilizando ese mismo Cloud Storage Pool.

Prueba a seguir uno de estos pasos para solucionar el problema:

- Si estás configurando un nuevo grupo de almacenamiento en la nube y el bucket contiene el archivo `x-ntap-sgws-cloud-pool-uuid` y claves de objetos adicionales similares al siguiente ejemplo, crea un bucket nuevo y usa este bucket nuevo en su lugar.

Ejemplo de una clave de objeto adicional: `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- Si el archivo `x-ntap-sgws-cloud-pool-uuid` es el único objeto en el bucket, elimina este archivo.

Si estos pasos no se ajustan a tu caso, ponte en contacto con soporte técnico.

Error: No se pudo crear ni actualizar el Cloud Storage Pool. Error del endpoint

Es posible que te encuentres con este error en las siguientes circunstancias:

- Cuando intentas crear o editar un Cloud Storage Pool.
- Cuando seleccionas una combinación de plataforma, autenticación o protocolo no compatible con S3 Object Lock durante la configuración de un nuevo Cloud Storage Pool. Consulta ["Aspectos a tener en cuenta sobre los grupos de almacenamiento en la nube"](#).

Este error indica que un problema de conectividad o de configuración impide que StorageGRID escriba en el Cloud Storage Pool.

Para solucionar el problema, revisa el mensaje de error del endpoint.

- Si el mensaje de error incluye `Get url: EOF`, comprueba que el punto final del servicio utilizado para el Cloud Storage Pool no utilice HTTP para un contenedor o bucket que requiera HTTPS.
- Si el mensaje de error incluye `Get url: net/http: request canceled while waiting for connection`, comprueba que la configuración de red permita que los Storage Nodes accedan al endpoint del servicio usado para el Cloud Storage Pool.
- Si el error se debe a una plataforma, autenticación o protocolo no compatibles, cambia a una configuración compatible con S3 Object Lock e intenta guardar de nuevo el nuevo Cloud Storage Pool.
- Para el resto de mensajes de error del punto final, prueba una o varias de las siguientes opciones:
 - Crea un contenedor o bucket externo con el mismo nombre que ingresaste para el Cloud Storage Pool e intenta guardar el nuevo Cloud Storage Pool otra vez.
 - Corrige el nombre del contenedor o del bucket que has especificado para el Cloud Storage Pool e intenta guardar de nuevo el nuevo Cloud Storage Pool.

Error: No se pudo analizar el certificado de CA

Es posible que te encuentres con este error al intentar crear o editar un Cloud Storage Pool. El error se produce si StorageGRID no pudo analizar el certificado que introdujiste al configurar el Cloud Storage Pool.

Para solucionar el problema, comprueba si el certificado de la CA que has proporcionado presenta algún problema.

Error: No se ha encontrado ningún Cloud Storage Pool con este ID

Es posible que te encuentres con este error al intentar editar o eliminar un grupo de almacenamiento en la nube. Este error se produce si el endpoint devuelve una respuesta 404, lo que puede significar cualquiera de las siguientes situaciones:

- Las credenciales utilizadas para el Cloud Storage Pool no tienen permiso de lectura para el bucket.
- El bucket utilizado para el Cloud Storage Pool no incluye el archivo marcador `x-ntap-sgws-cloud-pool-uuid`.

Prueba uno o varios de estos pasos para corregir el problema:

- Comprueba que el usuario asociado a la clave de acceso configurada disponga de los permisos necesarios.
- Edita el Cloud Storage Pool con credenciales que cuenten con los permisos necesarios.
- Si los permisos son correctos, ponte en contacto con soporte.

Error: No se pudo comprobar el contenido del Cloud Storage Pool. Error del endpoint

Es posible que te encuentres con este error al intentar eliminar un Cloud Storage Pool. Este error indica que algún tipo de problema de conectividad o de configuración impide que StorageGRID lea el contenido del bucket del Cloud Storage Pool.

Para solucionar el problema, revisa el mensaje de error del endpoint.

Error: Ya hay objetos en este bucket

Es posible que te encuentres con este error al intentar eliminar un Cloud Storage Pool. No puedes eliminar un Cloud Storage Pool si contiene datos que fueron trasladados allí por ILM, datos que ya estaban en el bucket antes de configurar el Cloud Storage Pool, o datos que se pusieron en el bucket desde otra fuente después de que se creó el Cloud Storage Pool.

Prueba uno o varios de estos pasos para corregir el problema:

- Sigue las instrucciones para devolver los objetos a StorageGRID en «Ciclo de vida de un objeto de un Cloud Storage Pool».
- Si estás seguro de que los objetos restantes no fueron colocados en el Cloud Storage Pool por ILM, elimina manualmente los objetos del bucket.



Nunca elimines manualmente objetos de un Cloud Storage Pool que puedan haber sido colocados allí por ILM. Si más adelante intentas acceder a un objeto eliminado manualmente desde StorageGRID, el objeto eliminado no se encontrará.

Error: El proxy encontró un error externo al intentar acceder al Cloud Storage Pool

Es posible que aparezca este error si has configurado un proxy de almacenamiento no transparente entre los nodos de almacenamiento y el endpoint S3 externo utilizado para el Cloud Storage Pool. Este error se produce si el servidor proxy externo no puede acceder al endpoint del Cloud Storage Pool. Por ejemplo, es posible que el servidor DNS no pueda resolver el nombre de host o que haya un problema de red externo.

Prueba uno o varios de estos pasos para corregir el problema:

- Comprueba la configuración del Cloud Storage Pool (**ILM > Storage pools**).
- Comprueba la configuración de red del servidor proxy de almacenamiento.

Error: el certificado X.509 está fuera del período de validez

Es posible que aparezca este error al intentar eliminar un Cloud Storage Pool. Este error se produce cuando la autenticación requiere un certificado X.509 para garantizar que se valida correctamente el Cloud Storage Pool externo y que este está vacío antes de eliminar la configuración del Cloud Storage Pool.

Sigue estos pasos para solucionar el problema:

- Actualiza el certificado configurado para la autenticación en el Cloud Storage Pool.
- Asegúrate de que se resuelva cualquier alerta de caducidad de certificados en este Cloud Storage Pool.

Información relacionada

["Ciclo de vida de un objeto del grupo de almacenamiento en la nube"](#)

Administra los perfiles de código de borrado en StorageGRID

Puedes consultar los detalles de un perfil de código de borrado y cambiarle el nombre si es necesario. Puedes desactivar un perfil de código de borrado si actualmente no se utiliza en ninguna regla de ILM.

Antes de empezar

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

Ver los detalles del perfil de código de borrado

Puedes consultar los detalles de un perfil de código de borrado para conocer su estado, el esquema de código de borrado utilizado y otra información.

Pasos

1. Selecciona **Configuración > Sistema > Erasure coding**.
2. Selecciona el perfil. Aparece la página de detalles del perfil.
3. Opcionalmente, consulta la pestaña de reglas de ILM para ver una lista de las reglas de ILM que usan el perfil y las políticas de ILM que usan esas reglas.
4. Si lo deseas, consulta la pestaña Storage Nodes para ver detalles sobre cada Storage Node en el grupo de almacenamiento del perfil, como el sitio donde se encuentra y el uso de almacenamiento.

Cambiar el nombre de un perfil de código de borrado

Quizá te interese cambiar el nombre de un perfil de código de borrado para que quede más claro qué hace dicho perfil.

Pasos

1. Selecciona **Configuración > Sistema > Erasure coding**.
2. Selecciona el perfil al que quieras cambiar el nombre.
3. Selecciona **Renombrar**.
4. Introduce un nombre único para el perfil de código de borrado.

El nombre del perfil de código de borrado se añade al nombre del grupo de almacenamiento en la instrucción de ubicación de una regla de ILM.



Los nombres de los perfiles de código de borrado deben ser únicos. Se produce un error de validación si usas el nombre de un perfil existente, incluso si ese perfil ha sido desactivado.

5. Selecciona **Guardar**.

Desactivar un perfil de código de borrado

Puedes desactivar un perfil de código de borrado si ya no tienes previsto utilizarlo y si dicho perfil no se está utilizando actualmente en ninguna regla de ILM.



Confirma que no haya ninguna operación de reparación de datos con código de borrado ni ningún procedimiento de descomisionado en curso. Se muestra un mensaje de error si intentas desactivar un perfil de codificación de borrado mientras cualquiera de estas operaciones está en curso.

Acerca de esta tarea

StorageGRID no te permite desactivar un perfil de código de borrado si se cumple alguna de las siguientes condiciones:

- El perfil de código de borrado se utiliza actualmente en una regla de ILM.
- El perfil de código de borrado ya no se utiliza en ninguna regla de ILM, pero los datos de los objetos y los fragmentos de paridad para el perfil siguen existiendo.

Pasos

1. Selecciona **Configuración > Sistema > Erasure coding**.
2. En la pestaña **Activo**, revisa la columna **Estado** para confirmar que el perfil de código de borrado que quieres desactivar no se usa en ninguna regla de ILM.

No puedes desactivar un perfil de código de borrado si se usa en alguna regla de ILM. En el ejemplo, el perfil 2+1 Data Center 1 se usa en al menos una regla de ILM.

☐	Profile name ?	Status ?	Storage pool ?	Erasure-coding scheme ?
☐	2+1 Data Center 1	Used in 5 rules	Data Center 1	2+1
☐	New profile	Deactivated	Data Center 1	2+1

3. Si el perfil se utiliza en una regla de ILM, sigue estos pasos:
 - a. Selecciona **ILM > Reglas**.
 - b. Selecciona cada regla y revisa el diagrama de retención para determinar si la regla utiliza el perfil de código de borrado que deseas desactivar.
 - c. Si la regla de ILM utiliza el perfil de código de borrado que deseas desactivar, comprueba si la regla se usa en alguna política de ILM.
 - d. Completa los pasos adicionales que aparecen en la tabla, según dónde se use el perfil de código de borrado.

¿Dónde se ha utilizado el perfil?	Pasos adicionales que hay que realizar antes de desactivar el perfil	Consulta estas instrucciones adicionales
Nunca se ha utilizado en ninguna regla de ILM	No es necesario realizar ningún paso adicional. Continúa con este procedimiento.	Ninguno

¿Dónde se ha utilizado el perfil?	Pasos adicionales que hay que realizar antes de desactivar el perfil	Consulta estas instrucciones adicionales
En una regla de ILM que nunca se ha usado en ninguna política de ILM	i. Modifica o elimina todas las reglas de ILM afectadas. Si modificas la regla, elimina todas las ubicaciones que utilicen el perfil de código de borrado. ii. Continúa con este procedimiento.	"Trabaja con reglas y políticas de ILM"
En una regla de ILM que está actualmente en una política de ILM activa	i. Clona la política. ii. Elimina la regla de ILM que utiliza el perfil de código de borrado. iii. Agrega una o más reglas ILM nuevas para asegurarte de que los objetos estén protegidos. iv. Guarda, simula y activa la nueva política. v. Espera a que se aplique la nueva política y a que los objetos existentes se trasladen a nuevas ubicaciones según las nuevas reglas que añadiste. Nota: Dependiendo del número de objetos y del tamaño de tu sistema StorageGRID, las operaciones de ILM podrían tardar semanas o incluso meses en trasladar los objetos a nuevas ubicaciones, según las nuevas reglas de ILM. Aunque puedes intentar desactivar sin problemas un perfil de código de borrado mientras siga asociado a datos, la operación de desactivación fallará. Un mensaje de error te informará si el perfil aún no está listo para ser desactivado. vi. Edita o elimina la regla que eliminaste de la política. Si editas la regla, elimina todas las ubicaciones que usan el perfil de código de borrado. vii. Continúa con este procedimiento.	"Crear una política de ILM" "Trabaja con reglas y políticas de ILM"

¿Dónde se ha utilizado el perfil?	Pasos adicionales que hay que realizar antes de desactivar el perfil	Consulta estas instrucciones adicionales
En una regla de ILM que actualmente está en una política de ILM	i. Edita la política. ii. Elimina la regla de ILM que utiliza el perfil de código de borrado. iii. Agrega una o más reglas nuevas de ILM para asegurarte de que todos los objetos estén protegidos. iv. Guarda la directiva. v. Edita o elimina la regla que eliminaste de la política. Si editas la regla, elimina todas las ubicaciones que usan el perfil de código de borrado. vi. Continúa con este procedimiento.	"Crear una política de ILM" "Trabaja con reglas y políticas de ILM"

e. Actualiza la página «Perfiles de código de borrado» para asegurarte de que el perfil no se utilice en una regla de ILM.

4. Si el perfil no se utiliza en ninguna regla de ILM, selecciona el botón de opción y selecciona **Desactivar**. Aparece el cuadro de diálogo Desactivar perfil de código de borrado.



Puedes seleccionar varios perfiles para desactivarlos al mismo tiempo, siempre y cuando cada perfil no se use en ninguna regla.

5. Si estás seguro de que quieres desactivar el perfil, selecciona **Desactivar**.

Resultados

- Si StorageGRID puede desactivar el perfil de erasure-coding, su estado es desactivado. Ya no puedes seleccionar este perfil para ninguna regla de ILM. No puedes volver a activar un perfil desactivado.
- Si StorageGRID no puede desactivar el perfil, aparece un mensaje de error. Por ejemplo, aparece un mensaje de error si todavía hay datos de objetos asociados a este perfil. Es posible que tengas que esperar varias semanas antes de volver a intentar el proceso de desactivación.

Configura las regiones de S3 para StorageGRID

Las reglas de ILM permiten filtrar objetos en función de las regiones opcionales en las que se crean los buckets de S3, lo que te permite almacenar objetos de diferentes regiones en distintas ubicaciones de almacenamiento.

Si quieres utilizar la región de un bucket de S3 como filtro en una regla, primero debes crear las regiones que puedan utilizar los buckets de tu sistema.



No puedes cambiar la región de un bucket después de que el bucket ha sido creado.

Antes de empezar

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

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

Acerca de esta tarea

Al crear un depósito de S3, puedes especificar que se cree en una región concreta. Especificar una región permite que el depósito esté geográficamente cerca de sus usuarios, lo que puede ayudar a optimizar la latencia, minimizar los costes y cumplir los requisitos normativos.

Cuando creas una regla de ILM, puede que quieras usar la región asociada con un bucket de S3 como filtro avanzado. Por ejemplo, puedes diseñar una regla que se aplique solo a los objetos en buckets de S3 creados en la región `us-west-2`. Luego puedes especificar que las copias de esos objetos se coloquen en Storage Nodes en un sitio de centro de datos dentro de esa región para optimizar la latencia.

A la hora de configurar las regiones, sigue estas directrices:

- Por defecto, se considera que todos los buckets pertenecen a la región `us-east-1`.
- Debes crear las regiones usando el Grid Manager antes de poder especificar una región no predeterminada al crear buckets con el Tenant Manager o la Tenant Management API, o con el elemento de solicitud `LocationConstraint` para las solicitudes S3 PUT Bucket API. Se produce un error si una solicitud PUT Bucket usa una región que no se ha definido en StorageGRID.
- Debes utilizar el nombre exacto de la región al crear el bucket de S3. Los nombres de las regiones distinguen mayúsculas de minúsculas. Los caracteres válidos son números, letras y guiones.



«EU» no se considera un alias de «eu-west-1». Si quieres utilizar la región «EU» o «eu-west-1», debes utilizar el nombre exacto.

- No puedes eliminar ni modificar una región si se utiliza en una regla asignada a cualquier política (activa o inactiva).
- Si utilizas una región no válida como filtro avanzado en una regla de ILM, no puedes añadir esa regla a una política.

Puede producirse una región no válida si utilizas una región como filtro avanzado en una regla de ILM y luego eliminas esa región, o si usas la Grid Management API para crear una regla y especificas una región que aún no has definido.

- Si eliminas una región después de haberla utilizado para crear un bucket de S3, tendrás que volver a añadir la región si en algún momento quieres usar el filtro avanzado de Location Constraint para encontrar objetos en ese bucket.

Pasos

1. Selecciona **ILM > Regiones**.

Aparece la página «Regiones».

2. Selecciona la pestaña **Todas las regiones** o **Región predeterminada**.

Todas las regiones

La pestaña **Todas las regiones** muestra las regiones definidas actualmente, incluida la región predeterminada.



No puedes eliminar ni modificar la región predeterminada en la pestaña **Todas las regiones**. Usa la pestaña **Región predeterminada** para cambiar la región predeterminada.

- Para añadir una región, selecciona **Add another region**.
- Introduce el nombre de una región que quieres usar al crear buckets de S3.

Debes utilizar este nombre exacto de la región como el elemento de solicitud LocationConstraint cuando crees el bucket de S3 correspondiente.

- Para eliminar una región que no se utilice, selecciona el icono de eliminación

Aparece un mensaje de error si intentas eliminar una región que se está utilizando actualmente en alguna política (activa o inactiva).

- Cuando hayas terminado de realizar los cambios, selecciona **Guardar**.

Ahora puedes seleccionar estas regiones en la sección «Filtros avanzados» del paso 1 del asistente para crear reglas de ILM. Consulta "[Usa filtros avanzados en las reglas de ILM](#)".

Región predeterminada

La pestaña **Región predeterminada** muestra la región predeterminada definida actualmente, que puedes modificar.

- Para cambiar la región predeterminada, selecciona el nombre de la región entre las opciones disponibles en la lista desplegable **Región predeterminada**.
- Selecciona **Guardar**.

Crear regla de ILM

Conoce las reglas ILM en StorageGRID

Para gestionar los objetos, creas un conjunto de reglas de gestión del ciclo de vida de la información (ILM) y las organizas en una política de ILM.

Cada objeto que se introduce en el sistema se evalúa en función de la política activa. Cuando una regla de la política coincide con los metadatos de un objeto, las instrucciones de la regla determinan qué acciones toma StorageGRID para copiar y almacenar ese objeto.



Los metadatos de los objetos no se gestionan mediante reglas de ILM. En su lugar, los metadatos de los objetos se almacenan en una base de datos 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 de la pérdida.

Elementos de una regla ILM

Una regla de ILM consta de tres elementos:

- **Criterios de filtrado:** Los filtros básicos y avanzados de una regla definen a qué objetos se aplica dicha regla. Si un objeto cumple todos los filtros, StorageGRID aplica la regla y crea las copias del objeto especificadas en las instrucciones de ubicación de la regla.
- **Instrucciones de ubicación:** Las instrucciones de ubicación de una regla definen el número, el tipo y la ubicación de las copias de los objetos. Cada regla puede incluir una secuencia de instrucciones de ubicación para modificar el número, el tipo y la ubicación de las copias de los objetos a lo largo del tiempo. Cuando expira el periodo de tiempo de una ubicación, las instrucciones de la siguiente ubicación se aplican automáticamente en la siguiente evaluación de ILM.
- **Comportamiento de ingesta:** El comportamiento de ingesta de una regla te permite elegir cómo se protegen los objetos filtrados por la regla a medida que se ingieren (cuando un cliente S3 guarda un objeto en el grid).

Filtrado de reglas ILM

Cuando creas una regla de ILM, especificas filtros para identificar a qué objetos se aplica la regla.

En el caso más sencillo, una regla podría no usar ningún filtro. Cualquier regla que no use filtros se aplica a todos los objetos, así que debe ser la última (por defecto) en una política de ILM. La regla por defecto proporciona instrucciones de almacenamiento para los objetos que no coinciden con los filtros de otra regla.

- Los filtros básicos te permiten aplicar diferentes reglas a grupos grandes y diferenciados de objetos. Estos filtros te permiten aplicar una regla a cuentas de inquilino específicas, buckets de S3 específicos o ambos.

Los filtros básicos te ofrecen una forma sencilla de aplicar diferentes reglas a un gran número de objetos. Por ejemplo, es posible que los registros financieros de tu empresa deban almacenarse para cumplir con los requisitos normativos, mientras que los datos del departamento de marketing quizá deban almacenarse para facilitar las operaciones diarias. Tras crear cuentas de inquilino independientes para cada departamento o tras segregar los datos de los distintos departamentos en buckets de S3 separados, puedes 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 te ofrecen un control muy preciso. Puedes crear filtros para seleccionar objetos en función de las siguientes propiedades de objeto:
 - Tiempo de ingesta
 - Último tiempo de 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)

Puedes filtrar los objetos según criterios muy específicos. Por ejemplo, los objetos almacenados por el departamento de diagnóstico por imagen de un hospital pueden utilizarse con frecuencia cuando tienen menos de 30 días de antigüedad y con poca frecuencia después, mientras que los objetos que contienen información sobre las visitas de los pacientes pueden necesitar copiarse al departamento de facturación en la sede central de la red sanitaria. Puedes crear filtros que identifiquen cada tipo de objeto según el nombre del objeto, el tamaño, las etiquetas de objetos S3 o cualquier otro criterio relevante, y luego crear reglas

independientes para almacenar cada conjunto de objetos de forma adecuada.

Puedes combinar filtros según sea necesario en una sola regla. Por ejemplo, el departamento de marketing podría querer almacenar archivos de imagen grandes de manera diferente a los registros de sus proveedores, mientras que el departamento de Recursos Humanos podría necesitar almacenar los expedientes del personal en una ubicación geográfica específica y la información sobre políticas de forma centralizada. En este caso, puedes crear reglas que filtren por cuenta de inquilino para separar los registros de cada departamento, mientras usas filtros en cada regla para identificar el tipo específico de objetos al que se aplica la regla.

Instrucciones para la 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 varias instrucciones de ubicación. Cada instrucción de ubicación se aplica a un único periodo de tiempo.

Al crear instrucciones de colocación:

- Lo primero que tienes que hacer es especificar la hora de referencia, que determina cuándo comienzan las instrucciones de ubicación. La hora de referencia puede ser el momento en que se ingresa un objeto, cuando se accede a él, cuando un objeto versionado deja de estar vigente o una hora definida por el usuario.
- A continuación, especificas cuándo se aplicará la ubicación, en relación con el momento de referencia. Por ejemplo, una ubicación podría comenzar el día 0 y continuar durante 365 días, en relación con el momento en que se incorporó el objeto.
- Por último, especificas el tipo de copias (replicación o código de borrado) y la ubicación donde se almacenan las copias. Por ejemplo, podrías querer almacenar dos copias replicadas en dos sitios diferentes.

Cada regla puede definir varias ubicaciones para un mismo periodo de tiempo y ubicaciones diferentes para distintos periodos de tiempo.

- Para situar objetos en varias ubicaciones durante un mismo periodo de tiempo, selecciona **Add other type or location** para añadir más de una línea para ese periodo.
- Para situar objetos en diferentes ubicaciones en distintos periodos de tiempo, selecciona **Add another time period** para añadir el siguiente periodo. Luego, especifica una o más líneas dentro de ese periodo.

El ejemplo muestra dos instrucciones de ubicación en la página Definir ubicaciones del asistente para crear reglas 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

1

Add other type or location

Time period 2
From Day 365 store forever

Store objects by replicating 2 copies at Data Center 3

2

Add other type or location

La primera instrucción de asignación 1 tiene dos líneas para el primer año:

- La primera línea crea dos copias replicadas del objeto en dos 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 asignación 2 crea dos copias al cabo de un año y las conserva indefinidamente.

Al definir el conjunto de instrucciones de ubicación para una regla, debes asegurarte de que al menos una instrucción de ubicación comience en el día 0, que no haya huecos entre los periodos de tiempo que hayas definido y que la última instrucción de ubicación continúe indefinidamente o hasta que ya no necesites más copias de ningún objeto.

A medida que vence cada período de la regla, se aplican las instrucciones de ubicación de contenido para el siguiente período. Se crean nuevas copias del objeto y se eliminan las copias que no sean necesarias.

Comportamiento de ingesta según la regla ILM

El comportamiento de ingesta determina si las copias de los objetos se colocan inmediatamente según las instrucciones de la regla o si se crean copias provisionales y las instrucciones de colocación se aplican más tarde. Los siguientes comportamientos de ingesta están disponibles para las reglas de ILM:

- **Equilibrado:** StorageGRID intenta crear todas las copias especificadas en la regla ILM en el momento de la ingesta; si esto no es posible, se crean copias provisionales y se devuelve un mensaje de éxito al cliente. Las copias especificadas en la regla ILM se crean cuando es posible.
- **Estricta:** Todas las copias especificadas en la regla de ILM deben crearse antes de que se devuelva un mensaje de éxito al cliente.
- **Confirmación doble:** StorageGRID crea inmediatamente copias provisionales del objeto y devuelve éxito al cliente. Las copias especificadas en la regla ILM se crean cuando es posible.

Información relacionada

- ["Opciones de ingesta"](#)
- ["Ventajas, desventajas y limitaciones de las opciones de ingesta"](#)
- ["Cómo interactúan la coherencia y las reglas de ILM para influir en la protección de datos"](#)

Ejemplo de regla ILM

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

- Aplícalo únicamente a los objetos que pertenecen a Tenant A.
- Crea dos copias replicadas de esos objetos y almacena cada copia en una ubicación diferente.
- Conservar las dos copias «para siempre», lo que significa que StorageGRID no las eliminará automáticamente. En su lugar, StorageGRID conservará estos objetos hasta que sean eliminados mediante una solicitud de eliminación del cliente o hasta que expire el ciclo de vida del bucket.
- Utiliza la opción Equilibrada para el comportamiento de ingesta: la instrucción de distribución en dos sitios se aplica en cuanto Tenant A guarda un objeto en StorageGRID, a menos que no sea posible crear inmediatamente ambas copias requeridas.

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

Información relacionada

- ["¿Qué es un storage pool?"](#)
- ["¿Qué es un grupo de almacenamiento en la nube?"](#)

Accede al asistente para crear una regla ILM en StorageGRID

Las reglas de ILM te permiten gestionar la ubicación de los datos de los objetos a lo largo del tiempo. Para crear una regla de ILM, usas el asistente Crear una regla de ILM.



Si deseas crear la regla ILM predeterminada para una política, sigue la ["Instrucciones para crear una regla ILM predeterminada"](#) en su lugar.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).
- Si quieres especificar a qué cuentas de inquilino se aplica esta regla, tienes la ["Permisos de las cuentas de inquilinos"](#) o sabes el ID de cada cuenta.
- Si quieres que la regla filtre los objetos según los metadatos del tiempo de acceso, debes habilitar las actualizaciones del tiempo de acceso en el bucket de S3.
- Ya has configurado los grupos de almacenamiento en la nube que tienes previsto utilizar. Consulta ["Crear Cloud Storage Pool"](#).
- Seguro que conoces el ["opciones de ingesta"](#).
- Si necesitas crear una regla que cumpla con los requisitos para su uso con S3 Object Lock, ya conoces el ["Requisitos para S3 Object Lock"](#).

- Opcionalmente, has visto el vídeo:

[Resumen de las reglas de ILM](#)

Acerca de esta tarea

Al crear reglas de ILM:

- Ten en cuenta la topología y las configuraciones de almacenamiento del sistema StorageGRID.
- Piensa qué tipos de copias de objetos quieres crear (replicadas o con código de borrado) y el número de copias de cada objeto que se requieren.
- Determina qué tipos de metadatos de objetos se utilizan en las aplicaciones que se conectan al sistema StorageGRID. Las reglas de ILM filtran los objetos en función de sus metadatos.
- Piensa dónde quieres que se coloquen las copias de los objetos a lo largo del tiempo.
- Decide qué opción de ingesta quieres utilizar (Balanced, Strict o Dual commit).

Pasos

1. Selecciona **ILM > Reglas**.
2. Selecciona **Crear**. "[Paso 1 \(Introducir datos\)](#)" de la pantalla del asistente para crear una regla de ILM aparece.

Ingresa detalles y filtros para una regla StorageGRID ILM

El paso **Introducir detalles** del asistente para crear una regla de ILM te permite introducir un nombre y una descripción para la regla y definir filtros para la regla.

Introducir una descripción y definir filtros para la regla es opcional.

Acerca de esta tarea

Al evaluar un objeto según una "[Regla de ILM](#)" regla, StorageGRID compara los metadatos del objeto con los filtros de la regla. Si los metadatos del objeto coinciden con todos los filtros, StorageGRID usa la regla para colocar el objeto. Puedes diseñar una regla para que se aplique a todos los objetos, o puedes especificar filtros básicos, como una o más cuentas de tenant o nombres de buckets, o filtros avanzados, como el tamaño del objeto o los metadatos de usuario.

Pasos

1. Introduce un nombre único para la regla en el campo **Nombre**.
2. Si lo deseas, introduce una breve descripción para la regla en el campo **Descripción**.

Deberías describir el propósito o la función de la regla para que puedas reconocerla después.

3. Si lo deseas, selecciona una o más cuentas de inquilino de S3 a las que se aplique esta regla. Si esta regla se aplica a todos los inquilinos, deja este campo en blanco.

Si no dispones ni del permiso de acceso Root ni del permiso de cuentas de Tenant, no puedes seleccionar tenants de la lista. En su lugar, introduce el tenant ID o varios IDs como una cadena separada por comas.

4. Si lo deseas, especifica los buckets de S3 a los que se aplica esta regla.

Si se selecciona **aplica a todos los buckets** (predeterminado), la regla se aplica a todos los buckets de S3.

5. Para los inquilinos de S3, puedes seleccionar **Sí** para aplicar la regla solo a las versiones anteriores de los objetos en los buckets de S3 que tengan habilitado el versionado.

Si seleccionas **Sí**, se seleccionará automáticamente «Hora no actual» como hora de referencia en "[Paso 2 del asistente para crear una regla de ILM](#)".



El tiempo no actual solo se aplica a los objetos S3 en buckets con control de versiones habilitado. Consulta "[Operaciones en los buckets, PutBucketVersioning](#)" y "[Gestiona objetos con S3 Object Lock](#)".

Puedes usar esta opción para reducir el impacto en el almacenamiento de los objetos versionados filtrando las versiones de objetos no actuales. Consulta "[Ejemplo 4: reglas y política de ILM para objetos versionados de S3](#)".

6. Si lo deseas, selecciona **Add an advanced filter** para especificar filtros adicionales.

Si no configuras 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, consulta [Usa filtros avanzados en las reglas de ILM](#) y [Especifica varios tipos y valores de metadatos](#).

7. Selecciona **Continuar**. "[Paso 2 \(Definir ubicaciones\)](#)" de la pantalla del asistente para crear una regla ILM aparece.

Usa filtros avanzados en las reglas de ILM

El filtrado avanzado te permite crear reglas de ILM que se aplican únicamente a objetos específicos en función de sus metadatos. Al configurar el filtrado avanzado para una regla, seleccionas el tipo de metadatos con el que quieres hacer la coincidencia, eliges un operador y especificas un valor de metadatos. Cuando se evalúan los objetos, la regla de ILM se aplica solo a aquellos objetos que tienen metadatos que coinciden con el filtro avanzado.

La tabla muestra los tipos de metadatos que puedes especificar en los filtros avanzados, los operadores que puedes usar 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 de • es en o antes de • es después de • es a partir de	Fecha y hora en que se ingirió el objeto. Nota: Para evitar problemas con los recursos al activar una nueva política de ILM, puedes utilizar el filtro avanzado «Hora de ingesta» en cualquier regla que pueda modificar la ubicación de un gran número de objetos existentes. Establece la «Hora de ingesta» en un valor mayor o igual a la hora aproximada en la que la nueva política entrará en vigor para garantizar que los objetos existentes no se muevan innecesariamente.

Tipo de metadatos	Operadores compatibles	Valor de metadatos
Clave	• es igual a • no es igual a • contiene • no contiene • comienza con • no empieza por • termina con • no termina con	Todo o parte de la clave única de un objeto S3. Por ejemplo, quizá quieras buscar objetos que terminen con <code>.txt</code> o que empiecen con <code>test-object/</code>.
Último tiempo de acceso	• es • no es • es antes de • es en o antes de • es después de • es a partir de	Fecha y hora de la última vez que se recuperó (leyó o visualizó) el objeto. Nota: Si tienes pensado usar "usar el tiempo de acceso más reciente" como filtro avanzado, debes habilitar las actualizaciones del tiempo de acceso más reciente para el bucket de S3.
Restricción de ubicación (solo S3)	• es igual a • no es igual a	La región en la que se creó un bucket de S3. Utiliza ILM > Regiones para definir las regiones que se muestran. Nota: El valor «us-east-1» coincidirá con los objetos de los buckets creados en la región us-east-1, así como con los objetos de los buckets que no tengan especificada ninguna región. Consulta "Configurar regiones de S3".
Tamaño del objeto	• es igual a • no es igual a • menos de • menor o igual que • mayor que • mayor o igual que	El tamaño del objeto. El código de borrado es más adecuado para objetos de más de 1 MB. No uses el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos muy pequeños codificados por borrado.

Tipo de metadatos	Operadores compatibles	Valor de metadatos
Metadatos del usuario	• contiene • termina con • es igual a • existe • comienza con • no contiene • no termina con • no es igual a • no existe • no empieza por	Par clave-valor, donde User metadata name es la clave y Metadata value es el valor. Por ejemplo, para filtrar objetos que tengan metadatos de usuario <code>color=blue</code>, especifica <code>color</code> para User metadata name, <code>equals</code> para el operador y <code>blue</code> para Metadata value. Nota: Los nombres de los metadatos de usuario no distinguen mayúsculas de minúsculas; los valores de los metadatos de usuario sí distinguen mayúsculas de minúsculas.
Etiqueta de objeto (solo S3)	• contiene • termina con • es igual a • existe • comienza con • no contiene • no termina con • no es igual a • no existe • no empieza por	Par clave-valor, donde Object tag name es la clave y Object tag value es el valor. Por ejemplo, para filtrar objetos que tengan una etiqueta de objeto de <code>Image=True</code>, especifica <code>Image</code> para Nombre de la etiqueta de objeto, <code>equals</code> para el operador y <code>True</code> para Valor de la etiqueta de objeto. Nota: Los nombres y valores de las etiquetas de los objetos distinguen mayúsculas de minúsculas. Debes introducir estos elementos exactamente tal y como se definieron para el objeto.

Especifica varios tipos y valores de metadatos

Al definir un filtrado avanzado, puedes especificar varios tipos de metadatos y varios valores de metadatos. Por ejemplo, si quieres que una regla coincida con objetos entre 10 MB y 100 MB de tamaño, debes seleccionar el tipo de metadatos **Object size** y especificar dos valores de metadatos.

- El primer valor de metadatos especifica los objetos mayores o iguales a 10 MB.
- El segundo valor de metadatos especifica los objetos de un tamaño igual o menor 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 entradas múltiples te permite controlar con precisión qué objetos se seleccionan. En el siguiente ejemplo, la regla se aplica a los objetos que tienen Brand A o Brand B como valor del metadato de usuario `camera_type`. Sin embargo, la regla solo se aplica a aquellos objetos Brand B que sean menores de 10 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule:

User metadata (dropdown) camera_type (text) equals (dropdown) Brand A (text) [X]

[Add another advanced filter](#)

or **Filter group 2** Objects with all of following metadata will be evaluated by this rule:

User metadata (dropdown) camera_type (text) equals (dropdown) Brand B (text) [X]

and Object size (dropdown) less than or equal to (dropdown) 10 (text) MB (dropdown) [X]

[Add another advanced filter](#)

Define instrucciones de colocación para una regla de StorageGRID ILM

El paso **Definir ubicaciones** del asistente para crear reglas de ILM te permite definir las instrucciones de ubicación que determinan cuánto tiempo se almacenan los objetos, el tipo de copias (replicadas o con código de borrado), la ubicación de almacenamiento y el número de copias.



Las capturas de pantalla que se muestran son ejemplos. Tus resultados pueden variar en función de tu versión de StorageGRID.

Acerca de esta tarea

Una regla ILM puede incluir una o varias instrucciones de ubicación. Cada instrucción de ubicación se aplica a un único periodo de tiempo. Cuando usas más de una instrucción, los periodos de tiempo deben ser contiguos y al menos una instrucción debe comenzar en el día 0. Las instrucciones pueden continuar para siempre o hasta que ya no necesites copias de ningún objeto.

Cada instrucción de colocación puede constar de varias líneas si deseas crear diferentes tipos de copias o usar diferentes ubicaciones durante ese periodo de tiempo.

En este ejemplo, la regla de ILM almacena una copia replicada en el sitio 1 y otra en el sitio 2 durante el primer año. Después de un año, se crea una copia con código de borrado 2+1 y se guarda únicamente en un sitio.

Time period 1
From Day
0
store
for
365
days

Store objects by
replicating
1
copies at
Site 1

and store objects by
replicating
1
copies at
Site 2

Add other type or location

Time period 2
From Day
365
store
forever

Store objects by
erasure coding
using
2+1 EC scheme at Site 3

Add other type or location

Pasos

1. Para **Hora de referencia**, selecciona el tipo de hora que quieres usar al calcular la hora de inicio de una instrucción de asignación.

Opción	Descripción
Tiempo de ingesta	El momento en que se ingirió el objeto.
Último tiempo de acceso	El momento en que se recuperó (leyó o visualizó) el objeto por última vez. Para utilizar esta opción, deben estar habilitadas las actualizaciones del tiempo de acceso para el bucket de S3. Consulta "Usa el tiempo de acceso en las reglas de ILM".
Hora de creación definida por el usuario	Una hora especificada en los metadatos definidos por el usuario.
Tiempo no corriente	La opción «Tiempo no actual» se selecciona automáticamente si seleccionaste Sí en la pregunta «¿Aplicar esta regla solo a versiones antiguas de objetos (en S3 buckets con versioning habilitado)?» en "Paso 1 del asistente para crear una regla de ILM" .

Si quieres crear una regla *conforme*, debes seleccionar **Hora de ingesta**. Consulta ["Gestiona objetos con S3 Object Lock"](#).

2. En la sección **Periodo de tiempo y asignaciones**, introduce una hora de inicio y una duración para el primer periodo de tiempo.

Por ejemplo, es posible que quieras especificar dónde almacenar los objetos durante el primer año (*A partir del día 0, almacénalos durante 365 días*). Al menos una instrucción debe comenzar en el día 0.

3. Si quieres crear copias replicadas:

- a. En la lista desplegable **Almacenar objetos por**, selecciona **replicando**.
- b. Selecciona el número de copias que desees hacer.

Aparece una advertencia si cambias el número de copias a 1. Una regla de ILM que crea solo una copia replicada para cualquier periodo de tiempo pone los datos en riesgo de pérdida permanente. Consulta ["Por qué no debes utilizar la replicación de copia única"](#).

Para evitar el riesgo, haz una o más de las siguientes acciones:

- Aumenta el número de copias para el periodo de tiempo.
- Agrega copias a otros pools de almacenamiento o a un Cloud Storage Pool.
- Selecciona **código de borrado** en lugar de **replicación**.

Puedes ignorar esta advertencia sin problema si esta regla ya crea varias copias para todos los periodos.

- c. En el campo **copias en**, selecciona los grupos de almacenamiento que quieras añadir.

Si solo especificas un grupo de almacenamiento, ten en cuenta que StorageGRID solo puede almacenar una copia replicada de un objeto en cada nodo de almacenamiento. Si tu grid incluye tres nodos de almacenamiento y seleccionas 4 como número de copias, solo se crearán tres copias—una copia por cada nodo de almacenamiento.

Se activa la alerta **ILM placement unachievable** para indicar que no se ha podido aplicar completamente la regla de ILM.

Si especificas más de un grupo de almacenamiento, ten en cuenta las siguientes reglas:

- El número de copias no puede ser mayor que el número de grupos de almacenamiento.
- Si el número de copias es igual al número de grupos de almacenamiento, se almacena una copia del objeto en cada grupo de almacenamiento.
- Si el número de copias es inferior al número 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 de almacenamiento, asegurando que ningún sitio reciba más de una copia de un objeto.
- Si los grupos de almacenamiento se solapan (contienen los mismos Storage Nodes), es posible que todas las copias del objeto se guarden únicamente en un sitio. Por este motivo, no especifiques el grupo de almacenamiento All Storage Nodes (StorageGRID 11.6 y versiones anteriores) junto con otro grupo de almacenamiento.

4. Si quieres crear una copia con código de borrado:

- a. En la lista desplegable **Almacenar objetos por**, selecciona **código de borrado**.



El código de borrado es más adecuado para objetos de más de 1 MB. No uses el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos muy pequeños codificados por borrado.

- b. Si no has añadido un filtro de «Tamaño del objeto» para un valor superior a 200 KB, selecciona **Anterior** para volver al paso 1. Luego, selecciona **Añadir un filtro avanzado** y configura un filtro de «Tamaño del objeto» con cualquier valor superior a 200 KB.

- c. Selecciona el grupo de almacenamiento que quieras añadir y el esquema de código de borrado que quieras utilizar.

La ubicación de almacenamiento de una copia con código de borrado incluye el nombre del esquema de código de borrado, seguido del nombre del grupo de almacenamiento.

Los esquemas de código de borrado disponibles están limitados por el número de nodos de almacenamiento del grupo de almacenamiento que selecciones. Aparece una insignia de **Recommended** junto a los esquemas que ofrecen ya sea el ["la mejor protección o la menor sobrecarga de almacenamiento"](#).

5. Opcionalmente:

- a. Selecciona **Add other type or location** para crear copias adicionales en distintas ubicaciones.
- b. Selecciona **Add another time period** para añadir diferentes periodos.



La eliminación de objetos se realiza según los siguientes ajustes:

- Los objetos se eliminan automáticamente al finalizar el último periodo de tiempo, a menos que otro periodo de tiempo termine con **forever**.
- Según ["Configuración del periodo de retención de buckets y de inquilinos"](#), es posible que los objetos no se eliminen aunque finalice el periodo de retención de ILM.

6. Si quieres almacenar objetos en un grupo de almacenamiento en la nube:

- a. En la lista desplegable **Almacenar objetos por**, selecciona **replicating**.
- b. Selecciona el campo **copias en**, luego selecciona un Cloud Storage Pool.

Cuando uses Cloud Storage Pools, ten en cuenta estas reglas:

- No puedes seleccionar más de un Cloud Storage Pool en una sola instrucción de ubicación. Del mismo modo, no puedes seleccionar un Cloud Storage Pool y un storage pool en la misma instrucción de ubicación.
- Solo puedes almacenar una sola copia de un objeto en cualquier Cloud Storage Pool. Aparece un mensaje de error si configuras **Copias** en 2 o más.
- No puedes almacenar más de una copia de un objeto en cualquier Cloud Storage Pool al mismo tiempo. Aparece un mensaje de error si varias ubicaciones que usan un Cloud Storage Pool tienen fechas que se solapan o si varias líneas de la misma ubicación usan un Cloud Storage Pool.
- Puedes almacenar un objeto en un Cloud Storage Pool al mismo tiempo que dicho objeto se almacena como copias replicadas o con código de borrado en StorageGRID. Sin embargo, debes incluir más de una línea en la instrucción de ubicación para ese periodo de tiempo, de modo que puedas especificar el número y los tipos de copias para cada ubicación.

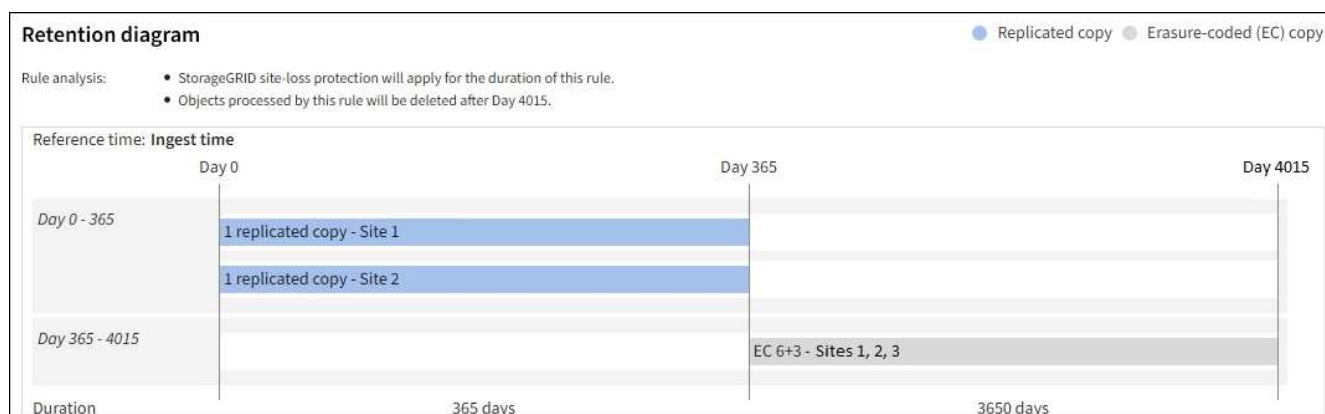
7. En el diagrama de retención, comprueba tus instrucciones de colocación.

En este ejemplo, la regla de ILM almacena una copia replicada en el Site 1 y otra copia replicada en el Site 2 durante el primer año. Después de un año y durante 10 años adicionales, se guardará una copia con código de borrado 6+3 en tres sites. Después de 11 años en total, los objetos se eliminarán de StorageGRID.

La sección de análisis de reglas del diagrama de retención dice:

- La protección contra la pérdida de un sitio de StorageGRID se aplicará mientras esté vigente esta regla.
- Los objetos procesados por esta regla se eliminarán después del día 4015.

Consulta ["Activa la protección contra la pérdida del sitio."](#)



8. Selecciona **Continuar**. ["Paso 3 \(Selecciona el comportamiento de ingesta\)"](#) del asistente para crear una regla ILM aparece.

Usa el tiempo de último acceso en las reglas ILM de StorageGRID

Puedes usar el tiempo de acceso como la hora de referencia en una regla de ILM. Por ejemplo, podrías querer dejar los objetos que se han visto en los últimos tres meses en los nodos de almacenamiento locales, mientras que los objetos que no se han visto recientemente se muevan a una ubicación externa. También puedes usar el tiempo de acceso como un filtro avanzado si quieres que una regla de 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 el tiempo de acceso en una regla de ILM, ten en cuenta las siguientes consideraciones:

- Cuando uses el tiempo de acceso como fecha de referencia, ten en cuenta que cambiar el tiempo de acceso de un objeto no activa una evaluación inmediata de ILM. En su lugar, se evalúan las ubicaciones del objeto y este se mueve según sea necesario cuando ILM en segundo plano evalúa el objeto. Esto podría tardar dos semanas o más después de que se accede al objeto.

Ten en cuenta esta latencia al crear reglas de ILM basadas en el tiempo de acceso y evita las ubicaciones que utilicen periodos de tiempo cortos (menos de un mes).

- Si utilizas el tiempo de acceso más reciente como filtro avanzado o como hora de referencia, debes habilitar las actualizaciones del tiempo de acceso más reciente para los buckets de S3. Puedes usar el ["Administrador de inquilinos"](#) o el ["API de gestión de inquilinos"](#).



Las actualizaciones del tiempo de acceso están desactivadas por defecto para los buckets de S3.



Ten en cuenta que habilitar las actualizaciones del tiempo de acceso puede reducir el rendimiento, especialmente en sistemas con objetos pequeños. El impacto en el rendimiento ocurre porque StorageGRID debe actualizar los objetos con nuevas marcas de tiempo cada vez que se recuperan.

La siguiente tabla resume si el tiempo de acceso se actualiza para todos los objetos del bucket según los distintos tipos de solicitudes.

Tipo de solicitud	Si se actualiza el tiempo de acceso más reciente cuando las actualizaciones del tiempo de acceso están desactivadas	Si el tiempo de acceso más reciente se actualiza cuando están activadas las actualizaciones del tiempo de acceso más reciente
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 bucket a otro	• No, para la copia original • Sí, para la copia de destino	• Sí, para la copia original • Sí, para la copia de destino
Solicitud para completar una subida en varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Selecciona el comportamiento de ingesta para una regla StorageGRID ILM

El paso **Seleccionar comportamiento de incorporación** del asistente para crear reglas de ILM te permite elegir cómo se protegen los objetos filtrados por esta regla en el momento de su incorporación.

Acerca de esta tarea

StorageGRID puede crear copias provisionales y poner los objetos en cola para su posterior evaluación según el ILM, o puede crear copias de inmediato para cumplir con las instrucciones de ubicación de la regla.

Pasos

1. Selecciona el ["comportamiento de ingesta"](#) que quieres usar.

Para más información, consulta ["Ventajas, desventajas y limitaciones de las opciones de ingesta"](#).



No puedes utilizar la opción «Equilibrada» o «Estricta» si la regla utiliza una de estas ubicaciones:

- Un Cloud Storage Pool desde el día 0
- Un Cloud Storage Pool cuando la regla utiliza una hora de creación definida por el usuario como hora de referencia

Consulta ["Ejemplo 5: normas y política de ILM para un comportamiento de ingesta estricto"](#).

2. Selecciona **Crear**.

Se ha creado la regla ILM. La regla no se activa hasta que se añade a una ["Política de ILM"](#) y esa política se activa.

Para ver los detalles de la regla, selecciona el nombre de la regla en la página de reglas de ILM.

Crea una regla ILM predeterminada en StorageGRID

Antes de crear una política de ILM, debes crear una regla predeterminada para incluir en la política cualquier objeto que no se ajuste a otra regla. La regla predeterminada no puede utilizar ningún filtro. Debe aplicarse a todos los inquilinos, todos los buckets y todas las versiones de los objetos.

Antes de empezar

- Has 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 de 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 de la política.

En esta política de ejemplo, la primera regla se aplica únicamente 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 tenant.

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, ten en cuenta estos requisitos:

- La regla predeterminada se colocará automáticamente como la última regla cuando la añadas a una política.
- La regla predeterminada no puede utilizar ningún filtro básico ni avanzado.
- La regla por defecto debe aplicarse a todas las versiones de los objetos.
- La regla predeterminada debería crear copias replicadas.



No utilices una regla que cree copias con código de borrado como regla predeterminada de una política. Las reglas de código de borrado deben usar un filtro avanzado para evitar que los objetos más pequeños se codifiquen con código de borrado.

- En general, la regla por defecto debería conservar los objetos para siempre.
- Si estás utilizando (o tienes previsto activar) la configuración global de S3 Object Lock, la regla predeterminada debe ser compatible.

Pasos

1. Selecciona **ILM > Reglas**.
2. Selecciona **Crear**.

Aparece el paso 1 (Introducir datos) del asistente para crear una regla de ILM.

3. Introduce un nombre único para la regla en el campo **Nombre de la regla**.
4. Si lo deseas, introduce una breve descripción para la regla en el campo **Descripción**.
5. Deja en blanco el campo **Tenant accounts**.

La regla predeterminada debe aplicarse a todas las cuentas de inquilino.

6. Deja el menú desplegable «Nombre del bucket» en la opción **se aplica a todos los buckets**.

La regla predeterminada debe aplicarse a todos los buckets de S3.

7. Mantén la respuesta predeterminada, **No**, para la pregunta, «¿Aplicar esta regla solo a las versiones anteriores de los objetos (en buckets de S3 con control de versiones activado)?»
8. No añadas filtros avanzados.

La regla predeterminada no puede especificar ningún filtro.

9. Selecciona **Siguiente**.

Aparece el paso 2 (Definir ubicaciones).

10. Para Hora de referencia, selecciona cualquier opción.

Si has mantenido la respuesta predeterminada, **No**, para la pregunta «¿Aplicar esta regla solo a las versiones anteriores del objeto?» La hora no actual no aparecerá en la lista desplegable. La regla predeterminada debe aplicarse a todas las versiones del objeto.

11. Especifica las instrucciones de ubicación para la regla predeterminada.

- La regla predeterminada debe conservar los objetos indefinidamente. Aparece una advertencia cuando activas una nueva política si la regla predeterminada no conserva los objetos indefinidamente. Debes confirmar que este es el comportamiento que esperas.
- La regla predeterminada debería crear copias replicadas.



No utilices una regla que cree copias con código de borrado como regla predeterminada de una política. Las reglas de código de borrado deben incluir el filtro avanzado **Tamaño del objeto (MB) superior a 200 KB** para evitar que los objetos más pequeños se codifiquen con código de borrado.

- Si estás utilizando (o tienes previsto activar) la configuración global de S3 Object Lock, la regla predeterminada debe ser compatible:
 - Debe crear al menos dos copias replicadas de objetos 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 Cloud Storage Pool.
 - Al menos una línea de las instrucciones de colocación debe comenzar en el día 0, usando la hora de ingesta como referencia.
 - Al menos una de las instrucciones de colocación debe ser "para siempre".

12. Consulta el diagrama de retención para confirmar las instrucciones de colocación.

13. Selecciona **Continuar**.

Aparece el paso 3 (Select ingest behavior).

14. Selecciona la opción de ingestión que quieres usar y selecciona **Crear**.

Gestiona las políticas de ILM

Conoce las políticas ILM en StorageGRID

Una política de gestión del ciclo de vida de la información (ILM) es un conjunto ordenado de reglas de ILM que determina cómo el sistema StorageGRID gestiona los datos de objetos a lo largo del tiempo.



Una política de ILM configurada incorrectamente puede provocar una pérdida de datos irre recuperable. Antes de activar una política de ILM, revisa detenidamente la política de ILM y sus reglas de ILM, y luego simula la política de ILM. Confirma siempre que la política de ILM funcionará como se espera.

Política predeterminada de ILM

Al instalar StorageGRID y añadir sitios, se crea automáticamente una política de ILM predeterminada, como sigue:

- Si tu grid contiene un único sitio, la política predeterminada incluye una regla predeterminada que replica dos copias de cada objeto en ese sitio.
- Si tu grid contiene más de un sitio, la regla predeterminada replica una copia de cada objeto en cada sitio.

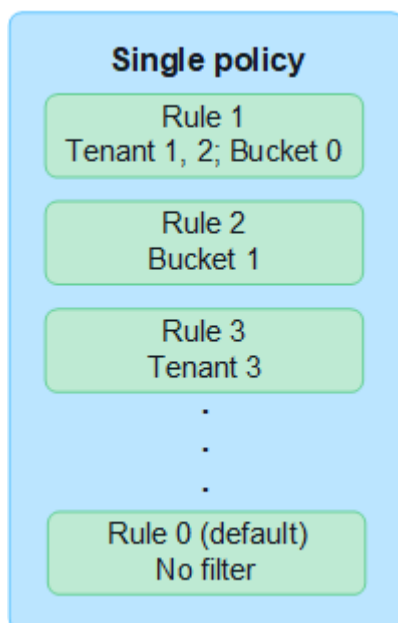
Si la política predeterminada no cumple con los requisitos de almacenamiento, puedes crear tus propias reglas y políticas. Consulta "[Crear una regla de ILM](#)" y "[Crear una política de ILM](#)".

¿Una o varias políticas de ILM activas?

Puedes tener una o varias políticas de ILM activas a la vez.

Una política

Si tu grid va a utilizar un esquema sencillo de protección de datos con pocas reglas específicas para cada tenant y cada bucket, utiliza una única política de ILM activa. Las reglas de ILM pueden incluir filtros para gestionar diferentes buckets o tenants.



Cuando solo tienes una política y cambian los requisitos de un inquilino, debes crear una nueva política de ILM o clonar la política existente para aplicar los cambios, simular y luego activar la nueva política de ILM. Los cambios en la política de ILM podrían provocar movimientos de objetos que podrían durar varios días y causar latencia en el sistema.

Varias políticas

Para ofrecer diferentes opciones de calidad de servicio a los inquilinos, puedes tener más de una política activa a la vez. Cada política puede gestionar inquilinos, buckets de S3 y objetos específicos. Cuando aplicas o modificas una política para un conjunto específico de inquilinos u objetos, las políticas aplicadas a otros inquilinos y objetos no se ven afectadas.

Etiquetas de políticas de ILM

Si deseas permitir que los clientes cambien fácilmente entre varias políticas de protección de datos para cada bucket, utiliza varias políticas de ILM con *etiquetas de política de ILM*. Asignas cada política de ILM a una etiqueta, luego los clientes etiquetan un bucket para aplicar la política a ese bucket. Solo puedes configurar etiquetas de política de ILM en buckets de S3.

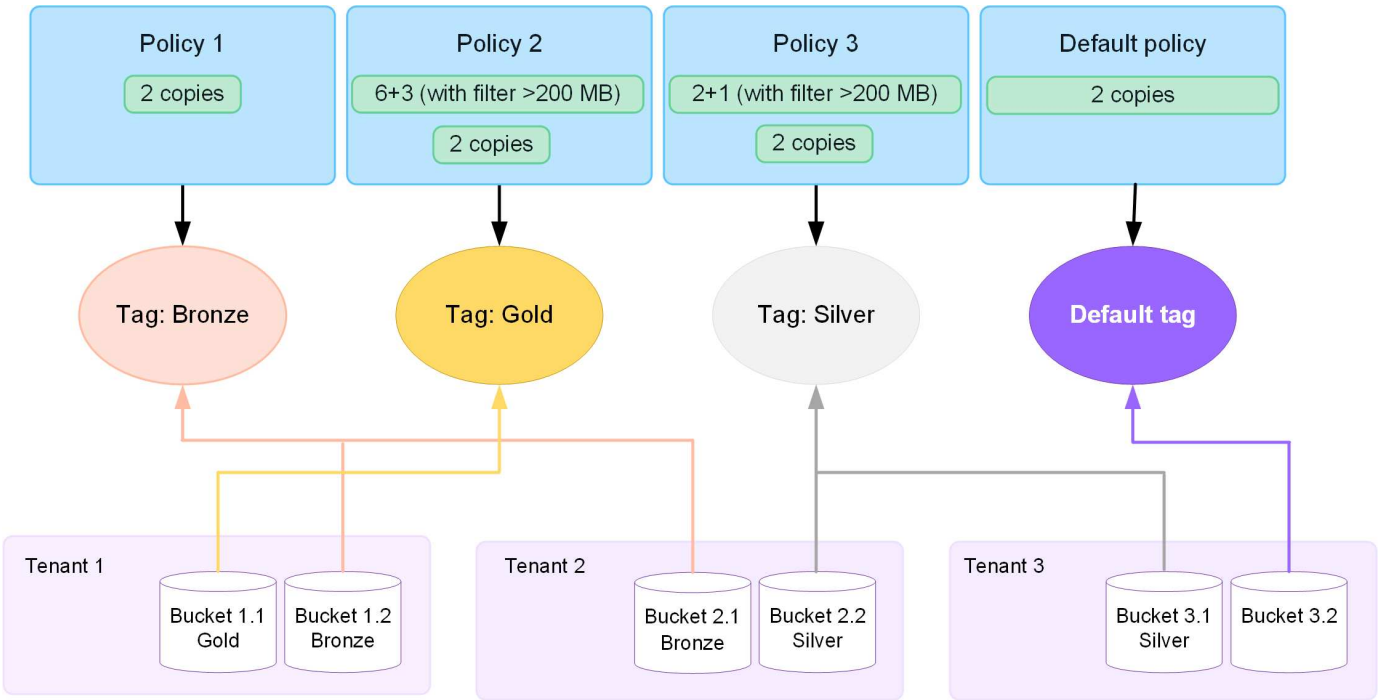
Por ejemplo, podrías tener tres etiquetas llamadas Gold, Silver y Bronze. Puedes asignar una política de ILM a cada etiqueta, según cuánto tiempo y dónde esa política almacene los objetos. Los tenants pueden elegir qué política usar etiquetando sus buckets. Un bucket etiquetado como Gold se gestiona mediante la política Gold y recibe el nivel Gold de protección de datos y rendimiento.



Puedes "crear un máximo de 10 etiquetas de política" para tu grid.

Etiqueta de política ILM predeterminada

Al instalar StorageGRID, se crea automáticamente una etiqueta de política ILM predeterminada. Cada grid debe tener una política activa asignada a la etiqueta Default. La política predeterminada se aplica a cualquier bucket de S3 sin etiqueta.



¿Cómo evalúa una política de ILM los objetos?

Una política de ILM activa controla la ubicación, la duración y la protección de datos de los objetos.

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

1. Si los filtros de la primera regla de la política coinciden con un objeto, el objeto se incorpora según el comportamiento de incorporación de esa regla y se almacena según las instrucciones de ubicación de esa regla.
2. Si los filtros de la primera regla no coinciden con el objeto, el objeto se evalúa con cada una de las reglas siguientes 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 de la política. La regla predeterminada es la última regla de una política. La regla predeterminada debe aplicarse a todos los tenants, todos los buckets de S3 y todas las versiones de los objetos, y no puede usar ningún filtro avanzado.

Ejemplo de política de ILM

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

- **Regla 1: Copias replicadas para Tenant A**

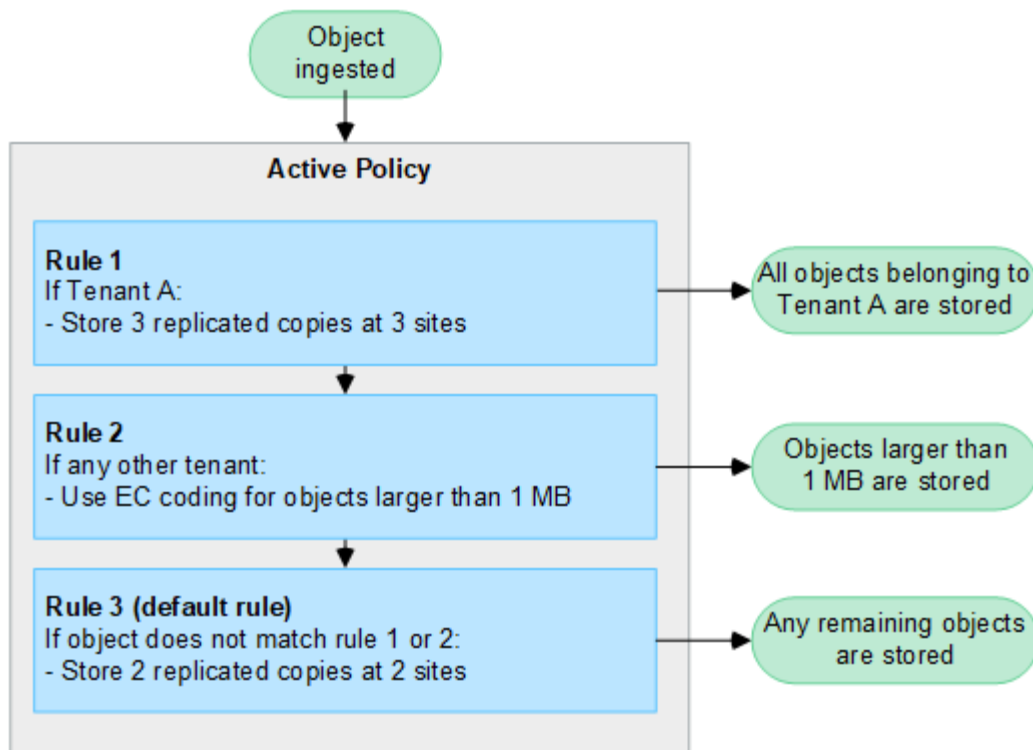
- Selecciona todos los objetos que pertenezcan a Tenant A.
- Almacena estos objetos como tres copias replicadas en tres ubicaciones.
- Los objetos que pertenecen a otros inquilinos no se ajustan a la Regla 1, así que se evalúan según la Regla 2.

- **Regla 2: código de borrado para objetos de más de 1 MB**

- Selecciona todos los objetos de otros tenants, pero solo si superan 1 MB. Estos objetos de mayor tamaño se almacenan utilizando erasure coding 6+3 en tres sitios.
- No coincide con los objetos de 1 MB o menos, así que estos objetos se evalúan según la Regla 3.

- **Regla 3: 2 copias 2 centros de datos (por defecto)**

- Es la última y predeterminada regla de la política. No utiliza filtros.
- Crea dos copias replicadas de todos los objetos que no se ajusten a la Regla 1 ni a la Regla 2 (objetos que no pertenezcan a Tenant A y que tengan un tamaño igual o inferior a 1 MB).



¿Qué son las políticas activas e inactivas?

Cada sistema StorageGRID debe tener al menos una política de ILM activa. Si quieres tener más de una política de ILM activa, creas etiquetas de política de ILM y asignas una política a cada etiqueta. Luego, los inquilinos aplican etiquetas a los buckets de S3. La política predeterminada se aplica a todos los objetos en los buckets que no tienen una etiqueta de política asignada.

Cuando creas una política de ILM por primera vez, seleccionas una o varias reglas de ILM y las ordenas en un orden específico. Después de simular la política para confirmar su comportamiento, la activas.

Al activar una política de ILM, StorageGRID utiliza dicha política para gestionar todos los objetos, tanto los ya existentes como los recién incorporados. Es posible que los objetos existentes se trasladen a nuevas ubicaciones cuando se apliquen las reglas de ILM de la nueva política.

Si activas más de una política de ILM a la vez y los inquilinos aplican etiquetas de política a los buckets de S3, los objetos de cada bucket se gestionan según la política asignada a la etiqueta.

Un sistema StorageGRID realiza un seguimiento del historial de las políticas que se han activado o desactivado.

Aspectos a tener en cuenta a la hora de crear una política de ILM

- Utiliza únicamente la política proporcionada por el sistema, Baseline 2 copies policy, en los sistemas de prueba. Para StorageGRID 11.6 y versiones anteriores, la regla Make 2 Copies en esta política utiliza el grupo de almacenamiento All Storage Nodes, que contiene todos los sitios. Si tu sistema StorageGRID tiene más de un sitio, dos copias de un objeto podrían colocarse en el mismo sitio.



El grupo de almacenamiento All Storage Nodes se crea automáticamente durante la instalación de StorageGRID 11.6 y versiones anteriores. Si actualizas a una versión posterior de StorageGRID, el grupo All Storage Nodes seguirá existiendo. Si instalas StorageGRID 11.7 o una versión posterior como nueva instalación, no se crea el grupo All Storage Nodes.

- Al diseñar una nueva política, ten en cuenta todos los diferentes tipos de objetos que podrían incorporarse a tu grid. Asegúrate de que la política incluya reglas para identificar y ubicar estos objetos según sea necesario.
- Mantén la política de ILM lo más sencilla posible. De este modo se evitan situaciones potencialmente peligrosas en las que los datos de los objetos no estén protegidos como se pretende cuando se realicen cambios en el sistema StorageGRID con el paso del tiempo.
- Asegúrate de que las reglas de la política estén en el orden correcto. Cuando se activa la política, los objetos nuevos y existentes se evalúan según las reglas en el orden en que aparecen, empezando por la primera. Por ejemplo, si la primera regla de una política coincide con un objeto, ese objeto no será evaluado por ninguna otra regla.
- La última regla de cada política de ILM es la regla predeterminada de ILM, que no puede utilizar ningún filtro. Si un objeto no ha sido coincidido por otra regla, la regla predeterminada controla dónde se coloca ese objeto y durante cuánto tiempo se retiene.
- Antes de activar una nueva política, revisa cualquier cambio que la política haga en la ubicación de los objetos existentes. Cambiar la ubicación de un objeto existente podría provocar problemas temporales con los recursos cuando se evalúen y apliquen las nuevas ubicaciones.

Crea políticas ILM en StorageGRID

Crea una o varias políticas de ILM para cumplir con tus requisitos de calidad de servicio.

Contar con una política de ILM activa te permite aplicar las mismas reglas de ILM a todos los tenants y buckets.

Disponer de varias políticas de ILM activas te permite aplicar las reglas de ILM adecuadas a tenants y buckets específicos para cumplir diversos requisitos de calidad de servicio.

Crear una política de ILM

Acerca de esta tarea

Antes de crear tu propia política, verifica que la ["política de ILM predeterminada"](#) no cumpla con tus requisitos de almacenamiento.



Utiliza únicamente las políticas proporcionadas por el sistema, 2 copies Policy (para grids de un solo sitio) o 1 Copy per Site (para grids de varios sitios), en sistemas de prueba. Para StorageGRID 11.6 y versiones anteriores, la regla predeterminada en esta política utiliza el grupo de almacenamiento All Storage Nodes, que contiene todos los sitios. Si tu sistema StorageGRID tiene más de un sitio, dos copias de un objeto podrían colocarse en el mismo sitio.



Si el ["Se ha activado la configuración global de S3 Object Lock"](#), debes asegurarte de que la política de ILM cumpla con los requisitos de los buckets que tienen habilitado S3 Object Lock. En esta sección, sigue las instrucciones que mencionan tener S3 Object Lock habilitado.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["permisos de acceso necesarios"](#).
- Tienes ["reglas de ILM creadas"](#) según si S3 Object Lock está activado.

S3 Object Lock no está activado

- Tienes ["creó las normas de ILM"](#) que quieres añadir a la política. Según sea necesario, puedes guardar una política, crear reglas adicionales y luego editar la política para añadir las nuevas reglas.
- Tienes ["creaste una regla ILM predeterminada"](#) que no contiene ningún filtro.

S3 Object Lock activado

- El ["La configuración global de S3 Object Lock ya está activada"](#) para el sistema StorageGRID.
- Tienes ["creaste las reglas de ILM conformes y no conformes"](#) que quieres añadir a la política. Según sea necesario, puedes guardar una política, crear reglas adicionales y luego editar la política para añadir las nuevas reglas.
- Tienes ["creaste una regla ILM predeterminada"](#) para la política que cumple con los requisitos.

- Opcionalmente, has visto el vídeo:

[Resumen de las políticas de ILM](#)

Véase también ["Usa políticas de ILM"](#).

Pasos

1. Selecciona **ILM > Policies**.

Si la configuración global de S3 Object Lock está activada, la página de políticas de ILM indica qué reglas de ILM cumplen.

2. Decide cómo quieres crear la política de ILM.

Crear nueva política

- a. Selecciona **Crear política**.

Clonar una política existente

- a. Marca la casilla de la política con la que quieras empezar y, a continuación, selecciona **Clonar**.

Editar política existente

- a. Si una política está inactiva, puedes editarla. Marca la casilla de la política inactiva con la que quieras empezar y luego selecciona **Editar**.

3. En el campo **Nombre de la política**, introduce un nombre único para la política.
4. Opcionalmente, en el campo **Motivo del cambio**, introduce el motivo por el que estás creando una nueva política.
5. Para añadir reglas a la política, selecciona **Seleccionar reglas**. Selecciona el nombre de una regla para ver su configuración.

Si vas a clonar una política:

- Se han seleccionado las reglas que utiliza la política que estás clonando.
- Si la política que estás clonando utilizaba alguna regla sin filtros que no fuera la regla predeterminada, se te pedirá que elimines todas esas reglas excepto una.
- Si la regla predeterminada utilizaba un filtro, se te pedirá que selecciones una nueva regla predeterminada.
- Si la regla predeterminada no era la última regla, puedes mover la regla al final de la nueva política.

S3 Object Lock no está activado

- a. Selecciona una regla predeterminada para la política. Para crear una nueva regla predeterminada, selecciona **ILM rules page**.

La regla por defecto se aplica a cualquier objeto que no coincida con otra regla de la política. La regla por defecto no puede usar ningún filtro y siempre se evalúa al final.



No utilices la regla Make 2 Copies como regla predeterminada para una política. La regla Make 2 Copies utiliza un único grupo de almacenamiento, All Storage Nodes, que contiene todos los sitios. Si tu sistema StorageGRID tiene más de un sitio, dos copias de un objeto podrían almacenarse en el mismo sitio.

S3 Object Lock activado

- a. Selecciona una regla predeterminada para la política. Para crear una nueva regla predeterminada, selecciona **ILM rules page**.

La lista de reglas contiene solo las reglas que cumplen los requisitos y no utilizan ningún filtro.



No utilices la regla «Make 2 Copies» como regla predeterminada para una política. La regla «Make 2 Copies» utiliza un único grupo de almacenamiento, «All Storage Nodes», que contiene todos los sitios. Si utilizas esta regla, varias copias de un objeto podrían colocarse en el mismo sitio.

- b. Si necesitas una regla «predeterminada» diferente para los objetos en los buckets de S3 que no cumplen los requisitos, selecciona **Incluir una regla sin filtros para los buckets de S3 que no cumplen los requisitos** y selecciona una regla para estos buckets que no utilice ningún filtro.

Por ejemplo, es posible que quieras utilizar un Cloud Storage Pool para almacenar objetos en buckets en los que no esté habilitado S3 Object Lock.



Solo puedes seleccionar una regla que no cumpla los requisitos y que no utilice un filtro.

Véase también ["Ejemplo 7: política de ILM compatible con S3 Object Lock"](#).

6. Cuando hayas terminado de seleccionar la regla predeterminada, selecciona **Continuar**.
7. En el paso «Otras reglas», selecciona cualquier otra regla que desees añadir a la política. Estas reglas utilizan al menos un filtro (cuenta de inquilino, nombre del bucket, filtro avanzado o el tiempo de referencia no actual). Luego selecciona **Seleccionar**.

La ventana «Crear una política» muestra ahora las reglas que has seleccionado. La regla predeterminada aparece al final, con el resto de reglas por encima de ella.

Si S3 Object Lock está activado y además has seleccionado una regla «predeterminada» que no cumple los requisitos, dicha regla se añade como la penúltima regla de la política.



Aparecerá una advertencia si alguna regla no conserva los objetos de forma permanente. Al activar esta política, debes confirmar que quieres que StorageGRID elimine los objetos cuando caduquen las instrucciones de ubicación de la regla predeterminada (a menos que un ciclo de vida de bucket mantenga los objetos durante un periodo de tiempo más largo).

8. Arrastra las filas correspondientes a las reglas no predeterminadas para determinar el orden en el que se evaluarán dichas reglas.

No puedes mover la regla predeterminada. Si S3 Object Lock está habilitado, tampoco puedes mover la regla "predeterminada" que no cumpla los requisitos, si se seleccionó alguna.



Debes comprobar que las reglas de ILM estén en el orden correcto. Cuando se activa la política, los objetos nuevos y existentes se evalúan según las reglas en el orden indicado, empezando por la parte superior.

9. Según sea necesario, selecciona **Select rules** para añadir o eliminar reglas.
10. Cuando hayas terminado, selecciona **Guardar**.
11. Repite estos pasos para crear políticas de ILM adicionales.
12. [Simula una política de ILM](#). Siempre debes simular una política antes de activarla para asegurarte de que funciona como se espera.

Simular una política

Simula una política en objetos de prueba antes de activarla y aplicarla a tus datos de producción.

Antes de empezar

- Conoces el bucket de S3 y la clave de objeto de cada objeto que quieres probar.

Pasos

1. Utiliza un cliente S3 o la ["Consola de S3"](#) para cargar los objetos necesarios para probar cada regla.
2. En la página de políticas de ILM, marca la casilla correspondiente a la política y luego selecciona **Simular**.
3. En el campo **Objeto**, introduce el S3 `bucket/object-key` para un objeto de prueba. Por ejemplo, `bucket-01/filename.png`.
4. Si está activada la función de versiones de S3, puedes introducir, si lo deseas, un ID de versión para el objeto en el campo **Version ID**.
5. Selecciona **Simular**.
6. En la sección de resultados de la simulación, confirma que cada objeto se haya asignado a la regla correcta.
7. Para determinar qué grupo de almacenamiento o qué perfil de código de borrado está activo, selecciona el nombre de la regla correspondiente para acceder a la página de detalles de la regla.



Revisa cualquier cambio en la ubicación de los objetos replicados y con código de borrado existentes. Cambiar la ubicación de un objeto existente podría provocar problemas temporales con los recursos mientras se evalúan y se implementan las nuevas ubicaciones.

Resultados

Cualquier modificación en las reglas de la política se reflejará en los resultados de la simulación y mostrará la nueva coincidencia y la coincidencia anterior. La ventana Simular policy conserva los objetos que probaste hasta que selecciones **Clear all** o el icono de eliminar  para cada objeto en la lista de resultados de la simulación.

Información relacionada

["Ejemplos de simulaciones de políticas de ILM"](#)

Activar una política

Al activar una única política nueva de ILM, tanto los objetos existentes como los recién incorporados se gestionan según dicha política. Al activar varias políticas, las etiquetas de política de ILM asignadas a los buckets determinan los objetos que se van a gestionar.

Antes de activar una nueva política:

1. Simula la directiva para confirmar que se comporta como esperas.
2. Revisa cualquier cambio en la ubicación de los objetos replicados y con código de borrado existentes. Cambiar la ubicación de un objeto existente podría provocar problemas temporales con los recursos mientras se evalúan y se implementan las nuevas ubicaciones.



Los errores en una política de ILM pueden provocar una pérdida de datos irreparable.

Acerca de esta tarea

Al activar una política de 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 recibir la nueva política. En algunos casos, el sistema espera antes de aplicar una nueva política activa para asegurarse de que los objetos de la red no se eliminen accidentalmente. En concreto:

- Si realizas cambios en las políticas que **aumenten la redundancia o la durabilidad de los datos**, dichos cambios se aplican de forma inmediata. Por ejemplo, si activas una nueva política que incluye una regla de tres copias en lugar de una de dos, dicha política se aplicará de inmediato, ya que aumenta la redundancia de los datos.
- Si realizas cambios en las políticas que **pudieran reducir la redundancia o la durabilidad de los datos**, dichos cambios no se aplicarán hasta que todos los nodos de la red estén disponibles. Por ejemplo, si activas una nueva política que utiliza una regla de dos copias en lugar de una de tres, la nueva política aparecerá en la pestaña Active policy pero no entrará en vigor hasta que todos los nodos estén en línea y disponibles.

Pasos

Sigue los pasos para activar una o varias políticas:

Activa una política

Sigue estos pasos si solo vas a tener una política activa. Si ya tienes una o más políticas activas y vas a activar políticas adicionales, sigue los pasos para activar varias políticas.

1. Cuando estés listo para activar una política, selecciona **ILM > Políticas**.

También puedes activar una única política desde la página **ILM > Policy tags**.

2. En la pestaña «Políticas», marca la casilla correspondiente a la política que quieras activar y luego selecciona **Activar**.
3. Sigue el paso correspondiente:
 - Si aparece un mensaje de advertencia pidiéndote que confirmes que quieres activar la política, selecciona **OK**.
 - Si aparece un mensaje de advertencia con información sobre la política:
 - i. Revisa los detalles para asegurarte de que la política gestione los datos como esperas.
 - ii. Si la regla predeterminada almacena los objetos durante un número limitado de días, revisa el diagrama de retención y luego escribe ese número de días en el cuadro de texto.
 - iii. Si la regla predeterminada almacena los objetos indefinidamente, pero hay una o varias reglas más con un plazo de conservación limitado, escribe **sí** en el cuadro de texto.
 - iv. Selecciona **Activar política**.

Activar varias políticas

Para activar varias políticas, debes crear etiquetas de política y asignar una política a cada etiqueta. Puedes crear un máximo de 10 etiquetas de política para tu grid.



Cuando se utilizan varias etiquetas de política, si los inquilinos reasignan con frecuencia etiquetas de política a los buckets, el rendimiento del grid podría verse afectado. Si tienes inquilinos no confiables, considera usar solo la etiqueta de política Default.

1. Selecciona **ILM > Etiquetas de política**.
2. Selecciona **Crear**.
3. En el cuadro de diálogo «Crear etiqueta de política», escribe un nombre para la etiqueta y, opcionalmente, una descripción para la etiqueta.



Los nombres y las descripciones de las etiquetas son visibles para los inquilinos. Elige valores que ayuden a los inquilinos a tomar una decisión informada cuando seleccionen las etiquetas de política que van a asignar a sus buckets. Por ejemplo, si la política asignada va a eliminar objetos después de un periodo de tiempo, podrías comunicar eso en la descripción. No incluyas información confidencial en estos campos.

4. Selecciona **Crear etiqueta**.
5. En la tabla de etiquetas de políticas de ILM, utiliza el menú desplegable para seleccionar una política que quieras asignar a la etiqueta.
6. Si aparecen advertencias en la columna «Limitaciones de la política», selecciona **Ver detalles de la política** para revisar la política.

7. Asegúrate de que cada política gestione los datos como esperas.
8. Selecciona **Activar políticas asignadas**. O selecciona **Borrar cambios** para eliminar la asignación de políticas.
9. En el cuadro de diálogo «Activar políticas con nuevas etiquetas», revisa las descripciones de cómo cada etiqueta, política y regla gestionará los objetos. Haz los cambios que necesites para asegurarte de que las políticas gestionen los objetos como esperas.
10. Cuando estés seguro de que quieres activar las políticas, escribe **sí** en el cuadro de texto y luego selecciona **Activar políticas**.

Información relacionada

["Ejemplo 6: cambio de una política de ILM"](#)

Ejemplos de simulaciones de políticas ILM en StorageGRID

Los ejemplos de simulaciones de políticas de ILM ofrecen pautas para estructurar y modificar simulaciones para tu entorno.

Ejemplo 1: verifica las reglas al simular una política de ILM

Este ejemplo describe cómo verificar las reglas al simular una política.

En este ejemplo, la **política ILM de ejemplo** se está simulando con los objetos importados en dos buckets. La política incluye tres reglas, como sigue:

- La primera regla, **Dos copias, dos años para bucket-a**, solo se aplica a los objetos en bucket-a.
- La segunda regla, **Objetos EC > 1 MB**, se aplica a todos los buckets pero filtra los objetos que superan 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 Noncurrent.

Después de simular la política, confirma que cada objeto fue asignado a la regla correcta.

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
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 se encuentra en bucket-b, por lo que no coincidía con la primera regla. En cambio, coincidía correctamente con la segunda regla, que filtra los objetos de más de 1 MB.
- bucket-b/test object less than 1 MB.pdf no coincidía con los filtros de las dos primeras reglas, así que se colocará según la regla predeterminada, que no incluye ningún filtro.

Ejemplo 2: reordena las reglas al simular una política de ILM

Este ejemplo muestra cómo puedes reordenar las reglas para cambiar los resultados al simular una política.

En este ejemplo, se simula la política **Demo**. Esta política, cuyo objetivo es localizar objetos que tengan metadatos de usuario series=x-men, incluye tres reglas, como sigue:

- La primera regla, **PNGs**, filtra los nombres de claves que terminan en .png.
- La segunda regla, **X-men**, se aplica únicamente a los objetos del inquilino A y filtra los metadatos de usuario para series=x-men.
- La última regla, **Dos copias en dos centros de datos**, es la regla predeterminada, que coincide con cualquier objeto que no coincida con las dos primeras reglas.

Pasos

1. Una vez añadidas las reglas y guardada la política, selecciona **Simular**.
2. En el campo **Objeto**, introduce el bucket/object-key de S3 para un objeto de prueba y selecciona **Simular**.

Aparecen los resultados de la simulación, mostrando que el objeto Havok.png fue coincidido por 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 **X-men**.

3. Para resolver el problema, cambia el orden de las reglas.
 - a. Selecciona **Finalizar** para cerrar la ventana Simular política de ILM.
 - b. Selecciona **Editar** para editar la política.
 - c. Arrastra la regla **X-men** hasta la parte superior de la lista.
 - d. Selecciona **Guardar**.
4. Selecciona **Simular**.

Los objetos que se habían comprobado anteriormente se vuelven a evaluar según la política actualizada y se muestran los nuevos resultados de la simulación. En el ejemplo, la columna «Regla coincidente» muestra que el objeto Havok.png ahora cumple la regla de metadatos «X-men», como se esperaba. La

columna «Coincidencia anterior» muestra que la regla «PNGs» coincidía 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 de 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 está pensada para encontrar objetos que tengan `series=x-men` metadatos de usuario. Sin embargo, se produjeron resultados inesperados al simular esta política con el objeto `Beast.jpg`. En lugar de coincidir con la regla de metadatos X-men, el objeto coincidió con la regla predeterminada, `Two copies two data centers`.

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 se ajusta a la regla prevista en la política, debes revisar cada regla en la política y corregir cualquier error.

Pasos

1. Selecciona **Finalizar** para cerrar el cuadro de diálogo Simulate policy. En la página de detalles de la política, selecciona **Retention diagram**. Luego selecciona **Expandir todo** o **Ver detalles** para cada regla según lo necesites.
2. Revisa la cuenta de inquilino de la regla, el periodo de referencia y los criterios de filtrado.

Por ejemplo, supón que los metadatos para la regla X-men se ingresaron como "x-men01" en vez de "x-men".
3. Para solucionar el error, corrige la regla de la siguiente manera:
 - Si la regla forma parte de la política, puedes clonarla o eliminar la regla de la política y luego editarla.
 - Si la regla forma parte de la política activa, debes clonarla. No puedes editar ni eliminar una regla de la política activa.
4. Vuelve a realizar la simulación.

En este ejemplo, la regla «X-men» corregida ahora coincide con el `Beast.jpg` objeto según los `series=x-men` metadatos de 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

Administra las etiquetas de políticas ILM en StorageGRID

Puedes consultar los detalles de una etiqueta de política de ILM, editar una etiqueta o eliminar una etiqueta.

Antes de empezar

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

Ver detalles de la etiqueta de política de ILM

Para ver los detalles de una etiqueta:

1. Selecciona **ILM > Etiquetas de política**.
2. Selecciona el nombre de la política en la tabla. Aparece la página de detalles de la etiqueta.
3. En la página de detalles, consulta el historial anterior de las políticas asignadas.
4. Ver una política seleccionándola.

Editar etiqueta de política de ILM



Los nombres y las descripciones de las etiquetas son visibles para los inquilinos. Elige valores que ayuden a los inquilinos a tomar una decisión informada cuando seleccionen las etiquetas de política que van a asignar a sus buckets. Por ejemplo, si la política asignada va a eliminar objetos después de un periodo de tiempo, podrías comunicar eso en la descripción. No incluyas información confidencial en estos campos.

Para editar la descripción de una etiqueta ya existente:

1. Selecciona **ILM > Etiquetas de política**.
2. Marca la casilla de selección correspondiente a la etiqueta y luego selecciona **Editar**.

También puedes seleccionar el nombre de la etiqueta. Aparece la página de detalles de la etiqueta y puedes seleccionar **Editar** en esa página.

3. Modifica la descripción de la etiqueta según sea necesario
4. Selecciona **Guardar**.

Eliminar la etiqueta de la política de ILM

Al eliminar una etiqueta de política, cualquier bucket al que se le haya asignado esa etiqueta tendrá aplicada

la política predeterminada.

Para eliminar una etiqueta:

1. Selecciona **ILM > Etiquetas de política**.
2. Marca la casilla de selección correspondiente a la etiqueta y luego selecciona **Eliminar**. Aparece un cuadro de diálogo de confirmación.

También puedes seleccionar el nombre de la etiqueta. Aparece la página de detalles de la etiqueta y puedes seleccionar **Eliminar** en esa página.

3. Selecciona **Sí** para eliminar la etiqueta.

Información relacionada

["Conoce cómo crear etiquetas de políticas de ILM"](#)

Verifica una política ILM con búsqueda de metadatos de objetos en StorageGRID

Una vez que hayas activado una política de ILM, introduce objetos de prueba representativos en el sistema StorageGRID y luego realiza una búsqueda de metadatos de los objetos para confirmar que las copias se están creando como se espera y se están ubicando en los lugares correctos.

Antes de empezar

Tienes un identificador de objeto, que puede ser uno de:

- **UUID:** El identificador único universal del objeto.
- **CBID:** El identificador único del objeto dentro de StorageGRID. Puedes obtener el CBID de un objeto a partir del registro de auditoría. Introduce el CBID en mayúsculas.
- **Depósito S3 y clave de objeto:** Cuando se importa un objeto a través de la interfaz de S3, la aplicación cliente utiliza una combinación de depósito y clave de objeto para almacenar e identificar el objeto. Si el depósito S3 está versionado y deseas buscar una versión específica de un objeto S3 utilizando el depósito y la clave de objeto, dispones del **ID de versión**.

Pasos

1. Ingresa el objeto.
2. Selecciona **ILM > Búsqueda de metadatos de objetos**.
3. Escribe el identificador del objeto en el campo **Identificador**. Puedes introducir un UUID, un CBID o una clave de bucket/objeto de S3.
4. Si lo deseas, introduce un identificador de versión para el objeto (solo S3).
5. Selecciona **Buscar**.

Aparecen los resultados de la búsqueda de metadatos del objeto. Esta página muestra los siguientes tipos de información:

- Metadatos del sistema, como el ID del objeto (UUID), el tipo de resultado (objeto, marcador de eliminación, S3 bucket) y el tamaño lógico del objeto. Consulta la captura de pantalla de ejemplo que aparece a continuación para obtener más detalles.
- Cualquier par clave-valor de metadatos de usuario personalizados asociados al objeto.

- Para los objetos de S3, cualquier par clave-valor de etiquetas asociado con el objeto.
 - En el caso de las copias replicadas de objetos, la ubicación de almacenamiento actual de cada copia.
 - En el caso de las copias de objetos con código de borrado, la ubicación actual de almacenamiento de cada fragmento.
 - Para las copias de objetos en un Cloud Storage Pool, la ubicación del objeto, incluyendo el nombre del bucket externo y el identificador único del objeto.
 - En el caso de los objetos segmentados y los objetos compuestos, una lista de los segmentos del objeto que incluye los identificadores de los segmentos y los tamaños de los datos. Para los objetos con más de 100 segmentos, solo se muestran los primeros 100 segmentos.
 - Todos los metadatos de los objetos en el formato de almacenamiento interno sin procesar. Estos metadatos sin procesar incluyen metadatos internos del sistema cuya persistencia no está garantizada de una versión a otra.
6. Confirma que el objeto esté almacenado en la ubicación o ubicaciones correctas y que sea el tipo de copia correcto.

Si la opción de auditoría está activada, también puedes supervisar el registro de auditoría para ver el mensaje "ORLM Object Rules Met". El mensaje de auditoría ORLM puede darte más información sobre el estado del proceso de evaluación de ILM, pero no puede darte información sobre la corrección de la ubicación de los datos del objeto ni sobre la integridad de la política de ILM. Debes evaluarlo tú mismo. Para más detalles, consulta ["Revisar los registros de auditoría"](#).

El siguiente ejemplo muestra los resultados de la consulta de metadatos de un objeto de prueba de S3 almacenado en dos copias replicadas.



La siguiente captura de pantalla es un ejemplo. Tus resultados variarán dependiendo de tu 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": {
      "PAHS": "2",

```

Información relacionada

["Usa la API de REST de S3"](#)

Trabaja con políticas ILM y reglas ILM en StorageGRID

A medida que cambian tus requisitos de almacenamiento, puede que necesites aplicar políticas adicionales o modificar las reglas de ILM asociadas a una política. Puedes consultar las métricas de ILM para determinar el rendimiento del sistema.

Antes de empezar

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

Ver las políticas de ILM

Para consultar las políticas de ILM activas e inactivas y el historial de activación de políticas:

1. Selecciona **ILM > Políticas**.
2. Selecciona **Políticas** para ver una lista de las políticas activas e inactivas. La tabla muestra el nombre de cada política, las etiquetas a las que está asignada y si está activa o inactiva.
3. Selecciona **Historial de activación** para ver una lista de las fechas de inicio y fin de la activación de las políticas.
4. Selecciona el nombre de una política para ver los detalles de la política.



Si consultas los detalles de una política cuyo estado sea «Editado» o «Eliminado», aparecerá un mensaje en el que se explica que estás viendo la versión de la política que estuvo activa durante el periodo de tiempo especificado y que, desde entonces, ha sido editada o eliminada.

Editar una política de ILM

Solo puedes editar una política inactiva. Si quieres editar una política activa, desactívala o crea un clon y edita el clon.

Para editar una política:

1. Selecciona **ILM > Políticas**.
2. Marca la casilla de la política que quieras editar y luego selecciona **Editar**.
3. Modifica la política siguiendo las instrucciones en "[Crear políticas de ILM](#)".
4. Simula la política antes de volver a activarla.



Una política de ILM configurada incorrectamente puede provocar una pérdida de datos irreparable. Antes de activar una política de ILM, revisa detenidamente la política de ILM y sus reglas de ILM, y luego simula la política de ILM. Confirma siempre que la política de ILM funcionará como se espera.

Clonar una política de ILM

Para clonar una política de ILM:

1. Selecciona **ILM > Políticas**.
2. Marca la casilla de la política que quieres clonar y luego selecciona **Clonar**.
3. Crea una nueva política a partir de la que has clonado siguiendo las instrucciones en "[Crear políticas de ILM](#)".



Una política de ILM configurada incorrectamente puede provocar una pérdida de datos irreparable. Antes de activar una política de ILM, revisa detenidamente la política de ILM y sus reglas de ILM, y luego simula la política de ILM. Confirma siempre que la política de ILM funcionará como se espera.

Eliminar una política de ILM

Solo puedes eliminar una política de ILM si está inactiva. Para eliminar una política:

1. Selecciona **ILM > Políticas**.

2. Marca la casilla de la política inactiva que quieras eliminar.
3. Selecciona **Eliminar**.

Ver detalles de la regla ILM

Para consultar los detalles de una regla ILM, incluido el diagrama de retención y las instrucciones de ubicación de la regla:

1. Selecciona **ILM > Reglas**.
2. Selecciona el nombre de la regla cuyos detalles quieras consultar. 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

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

Replicated copy Erasure-coded (EC) copy

Además, puedes 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 de ILM

Puedes clonar una regla existente si quieres crear una nueva regla que use algunos de los ajustes de la regla existente. Si necesitas editar una regla que se usa en alguna política, clona la regla y haz los cambios en la copia. Después de hacer los cambios en la copia, puedes quitar la regla original de la política y reemplazarla por la versión modificada según sea necesario.



No puedes clonar una regla de ILM si se creó con StorageGRID versión 10.2 o anterior.

Pasos

1. Selecciona **ILM > Reglas**.
2. Marca la casilla de la regla que quieras clonar y luego selecciona **Clonar**. O bien, selecciona el nombre de

la regla y luego selecciona **Clonar** en la página de detalles de la regla.

3. Actualiza 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, debes introducir un nuevo nombre.

Editar una regla de ILM

Es posible que tengas que modificar una regla de ILM para cambiar un filtro o una instrucción de ubicación.

No puedes editar una regla si se utiliza en alguna política de ILM. En su lugar, puedes [clonar la regla](#) y realizar los cambios necesarios en la copia clonada.



Una política de ILM configurada incorrectamente puede provocar una pérdida de datos irrecuperable. Antes de activar una política de ILM, revisa detenidamente la política de ILM y sus reglas de ILM, y luego simula la política de ILM. Confirma siempre que la política de ILM funcionará como se espera.

Pasos

1. Selecciona **ILM > Reglas**.
2. Confirma que la regla que deseas editar no se use en ninguna política de ILM.
3. Si la regla que deseas editar no está en uso, marca la casilla correspondiente a dicha regla y selecciona **Acciones > Editar**. O bien, selecciona el nombre de la regla y luego selecciona **Editar** en la página de detalles de la regla.
4. Sigue los pasos del asistente para editar reglas de ILM. Si es necesario, sigue los pasos para "[crear una regla de ILM](#)" y "[uso de filtros avanzados en las reglas de ILM](#)".

Al editar una regla de ILM, no puedes cambiar su nombre.

Eliminar una regla de ILM

Para que la lista de reglas de ILM actuales sea más manejable, elimina aquellas reglas de ILM que probablemente no vayas a utilizar.

Pasos

Para eliminar una regla de ILM que se esté utilizando actualmente en una política activa:

1. Clona la política.
2. Elimina la regla ILM del clon de la política.
3. Guarda, simula y activa la nueva política para asegurarte de que los objetos estén protegidos tal y como se espera.
4. Ve a los pasos para eliminar una regla de ILM que se está usando en una política inactiva.

Para eliminar una regla de ILM que se está utilizando actualmente en una política inactiva:

1. Selecciona la política inactiva.
2. Elimina la regla ILM de la política o [eliminar la política](#).
3. Sigue los pasos para eliminar una regla de ILM que no se esté utilizando actualmente.

Para eliminar una regla de ILM que no se está utilizando actualmente:

1. Selecciona **ILM > Reglas**.
2. Confirma que la regla que deseas eliminar no se use en ninguna política.
3. Si la regla que deseas eliminar no está en uso, selecciónala y elige **Acciones > Eliminar**. Puedes seleccionar varias reglas y eliminarlas todas a la vez.
4. Selecciona **Sí** para confirmar que deseas eliminar la regla de ILM.

Ver métricas de ILM

Puedes consultar métricas de ILM, como el número de objetos en la cola y la tasa de evaluación. Puedes supervisar estas métricas para determinar el rendimiento del sistema. Una cola o una tasa de evaluación elevadas podrían indicar que el sistema no es capaz de seguir el ritmo de la tasa de consumo, que la carga de las aplicaciones cliente es excesiva o que existe alguna situación anómala.

Pasos

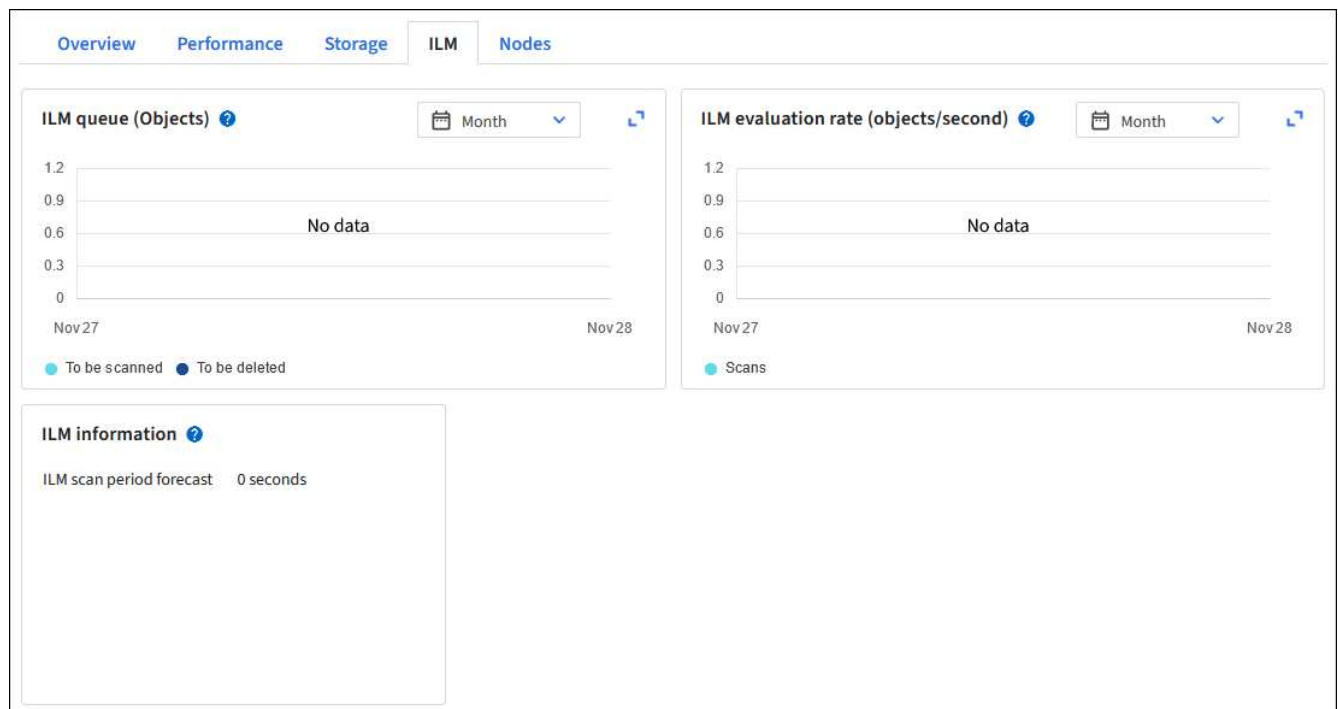
1. Selecciona **Dashboard > ILM**.



Dado que el panel de control se puede personalizar, es posible que la pestaña ILM no esté disponible.

2. Supervisa las métricas en la pestaña «ILM».

Puedes hacer clic en el signo de interrogación (?) para ver una descripción de los elementos de la pestaña ILM.



Usa S3 Object Lock

Cómo S3 Object Lock protege los objetos en StorageGRID

Como administrador de la grid, puedes habilitar S3 Object Lock para tu sistema StorageGRID e implementar una política de ILM compatible para ayudar a garantizar que los objetos en buckets específicos de S3 no se eliminen ni se sobrescriban durante un periodo de tiempo especificado.

¿Qué es S3 Object Lock?

La función S3 Object Lock de StorageGRID es una solución de protección de objetos equivalente a S3 Object Lock en Amazon Simple Storage Service (Amazon S3).

Cuando la configuración global de S3 Object Lock está habilitada para un sistema StorageGRID, una cuenta de inquilino de S3 puede crear buckets con o sin S3 Object Lock habilitado. Si un bucket tiene S3 Object Lock habilitado, el control de versiones de buckets es obligatorio y se habilita automáticamente.

Un bucket sin S3 Object Lock solo puede tener objetos sin una configuración de retención especificada. Ningún objeto ingerido tendrá configuración de retención.

Un bucket con S3 Object Lock puede tener objetos con y sin ajustes de retención especificados por las aplicaciones cliente de S3. Algunos objetos incorporados tendrán ajustes de retención.

Un bucket con S3 Object Lock y la retención predeterminada configurada puede contener objetos cargados con ajustes de retención especificados y nuevos objetos sin ajustes de retención. Los nuevos objetos usan la configuración predeterminada, porque la configuración de retención no se ha configurado a nivel de objeto.

Efectivamente, todos los objetos recién ingeridos tienen ajustes de retención cuando se configura la retención predeterminada. Los objetos existentes sin ajustes de retención de objetos no se ven afectados.

Modos de retención

La función Object Lock de StorageGRID S3 admite dos modos de retención para aplicar distintos niveles de protección a los objetos. Estos modos son equivalentes a los modos de retención de Amazon S3.

- En modo de cumplimiento:
 - El objeto no se puede eliminar hasta que se alcance su fecha de retención.
 - La fecha límite de retención del objeto se puede ampliar, pero no se puede reducir.
 - La fecha de retención del objeto no se puede eliminar hasta que se alcance dicha fecha.
- En modo de gobernanza:
 - Los usuarios con permisos especiales pueden utilizar un encabezado de omisión en las solicitudes para modificar determinados ajustes de retención.
 - Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su retain-until-date.
 - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

Configuración de retención para las versiones de los objetos

Si se crea un depósito con S3 Object Lock activado, los usuarios pueden usar la aplicación cliente de S3 para especificar de forma opcional los siguientes parámetros de retención para cada objeto que se añada al depósito:

- **Modo de retención:** cumplimiento normativo o gobernanza.
- **Fecha límite de conservación:** Si la fecha límite de conservación de una versión de un objeto es posterior a la fecha actual, el objeto se puede recuperar, pero no se puede eliminar.
- **Retención legal:** Al aplicar una retención legal a la versión de un objeto, dicho objeto queda bloqueado de inmediato. Por ejemplo, podrías necesitar aplicar una retención legal a un objeto relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de caducidad, sino que permanece vigente hasta que se elimine de forma explícita. Las retenciones legales son independientes de la retain-until-date.



Si un objeto está sujeto a una retención legal, nadie puede eliminar el objeto, independientemente de su modo de retención.

Para obtener detalles sobre la configuración de los objetos, consulta ["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#).

Configuración predeterminada de retención para los buckets

Si se crea un bucket con S3 Object Lock activado, los usuarios pueden, si lo desean, especificar los siguientes ajustes predeterminados para el bucket:

- **Modo de retención predeterminado:** cumplimiento o gobernanza.
- **Período de retención predeterminado:** cuánto tiempo deben conservarse las nuevas versiones de objetos añadidas a este bucket, a partir del día en que se añaden.

La configuración predeterminada del depósito solo se aplica a los objetos nuevos que no tienen su propia configuración de retención. Los objetos existentes en el depósito no se ven afectados cuando añades o cambias esta configuración predeterminada.

Consulta ["Crear un depósito de S3"](#) y ["Actualizar la retención predeterminada de S3 Object Lock"](#).

Comparación entre S3 Object Lock y Compliance tradicional

La función S3 Object Lock sustituye a la función Compliance que estaba disponible en versiones anteriores de StorageGRID. Porque la función S3 Object Lock cumple con los requisitos de Amazon S3, deja de utilizarse la función Compliance propia de StorageGRID, que ahora se denomina "legacy Compliance".



La configuración global de Compliance está obsoleta. Si activaste esta configuración usando una versión anterior de StorageGRID, la configuración de S3 Object Lock se activa automáticamente. Puedes seguir usando StorageGRID para gestionar la configuración de los buckets conformes existentes; sin embargo, no puedes crear nuevos buckets conformes. Para más detalles, consulta ["NetApp base de conocimientos: cómo gestionar los buckets Compliant heredados en StorageGRID 11.5"](#).

Si usaste la función heredada de Compliance en una versión anterior de StorageGRID, consulta la siguiente tabla para saber cómo se compara con la función S3 Object Lock en StorageGRID.

	Bloqueo de objetos de S3	Cumplimiento (legacy)
¿Cómo se activa la función a nivel global?	En el Grid Manager, selecciona Configuración > Sistema > S3 Object Lock .	Ya no es compatible.

	Bloqueo de objetos de S3	Cumplimiento (legacy)
¿Cómo se activa la función en un bucket?	Los usuarios deben habilitar S3 Object Lock al crear un nuevo bucket mediante el Tenant Manager, la Tenant Management API o la API de REST de S3.	Ya no es compatible.
¿Se admite el versionado de los buckets?	Sí. El control de versiones del bucket es obligatorio y se activa automáticamente cuando S3 Object Lock está habilitado para el bucket.	No.
¿Cómo se configura la retención de objetos?	Los usuarios pueden establecer una fecha de retención para cada versión de objeto, o pueden establecer un periodo de retención predeterminado para cada bucket.	Los usuarios deben establecer un periodo de retención para todo el bucket. El periodo de retención se aplica a todos los objetos del bucket.
¿Se puede cambiar el periodo de retención?	• En el modo de cumplimiento, la fecha límite de conservación de una versión de un objeto se puede aumentar, pero nunca disminuir. • En el modo de governance, los usuarios con permisos especiales pueden reducir o incluso eliminar la configuración de retención de un objeto.	El periodo de retención de un bucket puede aumentarse, pero nunca reducirse.
¿Dónde se controla la retención legal?	Los usuarios pueden aplicar o levantar una retención legal para cualquier versión de objeto en el bucket.	Se aplica una retención legal al bucket y afecta a todos los objetos en el bucket.
¿Cuándo se pueden eliminar los objetos?	• En el modo de cumplimiento, una versión de objeto puede eliminarse después de que se alcance 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 retain-until-date, siempre que el objeto no esté bajo legal hold.	Un objeto se puede eliminar una vez que haya vencido el periodo de retención, siempre que el bucket no esté bajo retención legal. Los objetos se pueden eliminar automáticamente o manualmente.

	Bloqueo de objetos de S3	Cumplimiento (legacy)
¿Se admite la configuración del ciclo de vida de los buckets?	Sí	No

Flujo de trabajo de S3 Object Lock en StorageGRID

Como administrador de la grid, debes coordinarte estrechamente con los usuarios de los tenants para garantizar que los objetos estén protegidos de forma que se cumplan sus requisitos de retención.



Aplicar la configuración de los inquilinos en toda la grid podría tardar 15 minutos o más, según la conectividad de red, el estado de los nodos y las operaciones de Cassandra.

Las siguientes listas para administradores de grid y usuarios de inquilinos contienen las tareas a grandes rasgos para usar la función S3 Object Lock.

Administrador de grid

- Activa la configuración global de S3 Object Lock para todo el sistema StorageGRID.
- Asegúrate de que las políticas de gestión del ciclo de vida de la información (ILM) sean *conformes*; es decir, que cumplan con "[Requisitos de los buckets con S3 Object Lock activado](#)".
- Si es necesario, permite que un inquilino utilice Compliance como modo de retención. De lo contrario, solo se permite el modo Governance.
- Si es necesario, establece un periodo máximo de retención para un tenant.

Usuario arrendatario

- Revisa las consideraciones para los buckets y objetos con S3 Object Lock.
- Si es necesario, ponte en contacto con el administrador de grid para activar la configuración global de S3 Object Lock y establecer los permisos.
- Crea buckets con S3 Object Lock activado.
- Opcionalmente, configura los ajustes de retención predeterminados para un bucket:
 - Modo de retención predeterminado: Governance o Compliance, si lo permite el administrador del grid.
 - Período de retención predeterminado: debe ser menor o igual al período máximo de retención establecido por el administrador de grid.
- Utiliza la aplicación cliente de S3 para añadir objetos y, si lo deseas, configurar la retención específica de cada objeto:
 - Modo de retención. Gobernanza o Cumplimiento, si lo permite el administrador de la grid.
 - Fecha de retención: debe ser menor o igual a lo permitido por el periodo máximo de retención establecido por el administrador de grid.

Requisitos de S3 Object Lock en StorageGRID

Debes revisar los requisitos para habilitar la configuración global de S3 Object Lock, los requisitos para crear reglas de ILM y políticas de ILM compatibles, y las restricciones que StorageGRID impone a los buckets y objetos que usan S3 Object Lock.

Requisitos para usar la configuración global de S3 Object Lock

- Debes activar la configuración global de S3 Object Lock usando el Grid Manager o la Grid Management API antes de que cualquier tenant de S3 pueda crear un bucket con S3 Object Lock activado.
- Al habilitar la configuración global de S3 Object Lock, todas las cuentas de inquilinos de S3 pueden crear buckets con S3 Object Lock habilitado.
- Una vez que hayas activado la configuración global de S3 Object Lock, no podrás desactivarla.
- No puedes habilitar S3 Object Lock a nivel global a menos que la regla predeterminada de todas las políticas de ILM activas sea *conforme* (es decir, la regla predeterminada debe cumplir con los requisitos de los buckets con S3 Object Lock habilitado).
- Cuando la configuración global de S3 Object Lock está activada, no puedes crear una nueva política de ILM ni activar una política de ILM existente a menos que la regla predeterminada de la política sea compatible. Después de que la configuración global de S3 Object Lock se haya activado, las páginas de reglas de ILM y políticas de ILM indican qué reglas de ILM son compatibles.

Requisitos para reglas de ILM compatibles

Si deseas habilitar la configuración global de S3 Object Lock, debes asegurarte de que la regla predeterminada de todas las políticas de ILM activas sea compatible. Una regla compatible satisface los requisitos tanto de los buckets con S3 Object Lock habilitado como de cualquier bucket existente que tenga habilitado el cumplimiento heredado:

- Debe crear al menos dos copias replicadas de objetos 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 Cloud Storage Pool.
- Al menos una línea de las instrucciones de colocación debe comenzar en el día 0, usando **Hora de ingesta** como hora de referencia.
- Al menos una de las instrucciones de colocación debe ser "para siempre".

Requisitos para las políticas de ILM

Cuando la configuración global de S3 Object Lock está activada, las políticas de ILM activas e inactivas pueden incluir tanto reglas que cumplen los requisitos como reglas que no los cumplen.

- La regla predeterminada en una política de ILM activa o inactiva debe ser compatible.
- Las reglas de incumplimiento solo se aplican a los objetos en los buckets que no tienen habilitado S3 Object Lock o que no tienen habilitada la función de cumplimiento heredada.
- Las reglas de cumplimiento pueden aplicarse a los objetos de cualquier bucket; no es necesario que el bucket tenga activado S3 Object Lock ni el cumplimiento heredado.

"Ejemplo de una política de ILM conforme para S3 Object Lock"

Requisitos para los buckets con S3 Object Lock activado

- Si la configuración global de S3 Object Lock está habilitada para el sistema StorageGRID, puedes usar el Tenant Manager, la API de gestión de inquilinos o la API de REST de S3 para crear buckets con S3 Object Lock habilitado.
- Si tienes pensado utilizar S3 Object Lock, debes habilitar S3 Object Lock al crear el bucket. No puedes habilitar S3 Object Lock en un bucket ya existente.

- Cuando se habilita S3 Object Lock para un bucket, StorageGRID habilita automáticamente el control de versiones para ese bucket. No puedes deshabilitar S3 Object Lock ni suspender el control de versiones para el bucket.
- Si lo deseas, puedes especificar un modo de retención y un periodo de retención predeterminados para cada bucket usando el Tenant Manager, la Tenant Management API o la API de REST de S3. La configuración de retención predeterminada del bucket solo se aplica a los nuevos objetos añadidos al bucket que no tengan su propia configuración de retención. Puedes anular esta configuración predeterminada especificando un modo de retención y una retain-until-date para cada versión del objeto cuando se suba.
- La configuración del ciclo de vida de los buckets es compatible con los buckets que tienen activada la función S3 Object Lock.
- CloudMirror replication no es compatible con los buckets con S3 Object Lock habilitado.

Requisitos para los objetos en buckets con S3 Object Lock activado

- Para proteger una versión de un objeto, puedes especificar ajustes de retención predeterminados para el bucket, o puedes especificar ajustes de retención para cada versión del objeto. Los ajustes de retención a nivel de objeto se pueden especificar usando la aplicación cliente de S3 o la API de REST de S3.
- Los ajustes de retención se aplican a las versiones individuales de los objetos. Una versión de un objeto puede tener tanto una configuración de «retención hasta una fecha» como una de «retención legal», una de ellas pero no la otra, o ninguna de las dos. Al especificar una configuración de «retención hasta una fecha» o de «retención legal» para un objeto, solo se protege la versión especificada en la solicitud. Puedes crear nuevas versiones del objeto, mientras que la versión anterior del objeto permanece bloqueada.

Ciclo de vida de los objetos en los buckets con S3 Object Lock activado

Cada objeto que se guarda en un bucket con S3 Object Lock activado pasa por estas etapas:

1. Ingesta de objetos

Cuando se añade una versión de un objeto a un bucket que tiene activado S3 Object Lock, la configuración de retención se aplica de la siguiente manera:

- Si especificas la configuración de retención para el objeto, se aplica la configuración a nivel de objeto. Se ignora cualquier configuración predeterminada del bucket.
- Si no se especifican ajustes de retención para el objeto, se aplican los ajustes predeterminados del bucket, si existen.
- Si no se especifican ajustes de retención para el objeto o el depósito, el objeto no está protegido por S3 Object Lock.

Si se aplican los parámetros de retención, quedan protegidos tanto el objeto como cualquier metadato definido por el usuario en S3.

2. Retención y eliminación de objetos

StorageGRID almacena varias copias de cada objeto protegido durante el periodo de retención especificado. El número exacto y el tipo de copias de objeto y las ubicaciones de almacenamiento se determinan por las reglas de cumplimiento en las políticas de ILM activas. Si un objeto protegido puede eliminarse antes de que se alcance su fecha de retención depende de su modo de retención.

- Si un objeto está sujeto a una retención legal, nadie puede eliminar el objeto, independientemente de su modo de retención.

Información relacionada

- ["Crear un depósito de S3"](#)
- ["Actualizar la retención predeterminada de S3 Object Lock"](#)
- ["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#)
- ["Ejemplo 7: política de ILM compatible con S3 Object Lock"](#)

Habilita el bloqueo de objetos S3 a nivel global en StorageGRID

Si una cuenta de inquilino de S3 debe cumplir con los requisitos normativos a la hora de guardar datos de objetos, debes habilitar S3 Object Lock para todo tu sistema StorageGRID. Al habilitar la configuración global de S3 Object Lock, cualquier usuario de inquilino de S3 podrá crear y gestionar buckets y objetos con S3 Object Lock.

Antes de empezar

- Tienes el ["Permiso de acceso raíz"](#).
- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Has revisado el flujo de trabajo de S3 Object Lock y entiendes las consideraciones.
- Has confirmado que la regla predeterminada de la política de ILM activa cumple con los requisitos. Consulta ["Crear una regla de ILM predeterminada"](#) para más detalles.

Acerca de esta tarea

El administrador de grid debe activar la configuración global de S3 Object Lock para permitir que los usuarios inquilinos creen nuevos buckets con S3 Object Lock activado. Una vez activada esta configuración, no se puede desactivar.

Revisa la configuración de cumplimiento de los inquilinos existentes después de habilitar la configuración global de S3 Object Lock. Cuando habilitas esta configuración, los ajustes de S3 Object Lock por inquilino dependen de la versión de StorageGRID vigente en el momento en que se creó el inquilino.



La configuración global de Compliance está obsoleta. Si activaste esta configuración usando una versión anterior de StorageGRID, la configuración de S3 Object Lock se activa automáticamente. Puedes seguir usando StorageGRID para gestionar la configuración de los buckets conformes existentes; sin embargo, no puedes crear nuevos buckets conformes. Para más detalles, consulta ["NetApp base de conocimientos: cómo gestionar los buckets Compliant heredados en StorageGRID 11.5"](#).

Pasos

1. Selecciona **Configuración > Sistema > S3 Object Lock**.

Aparece la página «Configuración de S3 Object Lock».

2. Selecciona **Habilitar bloqueo de objetos S3**.
3. Selecciona **Aplicar**.

Aparece un cuadro de diálogo de confirmación que te recuerda que no puedes desactivar S3 Object Lock después de que se haya activado.

4. Si estás seguro de que quieres activar de forma permanente S3 Object Lock para todo tu sistema, selecciona **OK**.

Cuando seleccionas **OK**:

- Si la regla predeterminada de la política de ILM activa cumple con los requisitos, S3 Object Lock queda habilitado para toda la grid y no se puede desactivar.
- Si la regla predeterminada no cumple los requisitos, aparece un error. Debes crear y activar una nueva política de ILM que incluya una regla que cumpla los requisitos como regla predeterminada. Selecciona **OK**. Luego, crea una nueva política, simúlala y actívala. Consulta ["Crear política de ILM"](#) para ver las instrucciones.

Resuelve errores de consistencia al actualizar la configuración de S3 Object Lock o legacy Compliance en StorageGRID

Si un centro de datos o varios nodos de almacenamiento de una misma ubicación dejan de estar disponibles, es posible que tengas que ayudar a los usuarios de S3 a aplicar cambios en la configuración de S3 Object Lock o en la configuración de cumplimiento heredada.

Los usuarios de un inquilino que tengan buckets con S3 Object Lock (o Compliance heredado) activado pueden cambiar ciertos ajustes. Por ejemplo, un usuario de un inquilino que use S3 Object Lock podría necesitar poner una versión de un objeto bajo retención legal.

Cuando un usuario de un inquilino actualiza la configuración de un bucket de S3 o la versión de un objeto, StorageGRID intenta actualizar inmediatamente los metadatos del bucket o del objeto en toda la grid. Si el sistema no puede actualizar los metadatos porque un data center o varios Storage Nodes 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 solucionar este error, sigue estos pasos:

1. Intenta que todos los nodos de almacenamiento o sitios vuelvan a estar disponibles lo antes posible.
2. Si no puedes poner a disposición un número suficiente de nodos de almacenamiento en cada sitio, ponte en contacto con el soporte técnico, que te ayudará a recuperar los nodos y a garantizar que los cambios se apliquen de forma coherente en toda la grid.
3. Una vez resuelto el problema subyacente, recuerda al usuario del tenant que vuelva a intentar aplicar los cambios de configuración.

Información relacionada

- ["Utiliza una cuenta de inquilino"](#)
- ["Usa la API de REST de S3"](#)
- ["Recuperar y mantener"](#)

Ejemplos de reglas y políticas de ILM

Reglas y políticas de ILM para la protección y retención básica de objetos en StorageGRID

Puedes usar las siguientes reglas y políticas de ejemplo como punto de partida al definir una política de ILM que se ajuste a tus requisitos de protección y retención de objetos.



Las siguientes reglas y políticas de ILM son solo ejemplos. Existen muchas formas de configurar reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará como esperas y protegerá el contenido contra la pérdida.

Regla 1 de ILM para el ejemplo 1: Copia los datos de los objetos en dos sitios

Esta regla de ILM de ejemplo copia los datos de los objetos a grupos de almacenamiento en dos sitios.

Definición de regla	Valor de ejemplo
Grupos de almacenamiento en un único sitio	Dos grupos de almacenamiento, cada uno con diferentes sitios, llamados Site 1 y Site 2.
Nombre de la regla	Dos copias dos sitios
Hora de referencia	Tiempo de ingesta
Ubicaciones	Desde el día 0 hasta siempre, mantén una copia replicada en el sitio 1 y otra copia replicada en el sitio 2.

La sección de análisis de reglas del diagrama de retención dice:

- La protección contra la pérdida de un sitio de StorageGRID se aplicará mientras esté vigente 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 código de borrado con coincidencia de bucket

Esta regla de ILM de ejemplo utiliza un perfil de código de borrado y un bucket de S3 para determinar dónde y durante cuánto tiempo se almacena el objeto.

Definición de regla	Valor de ejemplo
Grupo de almacenamiento con múltiples emplazamientos	Un grupo de almacenamiento que abarca tres sitios (sitios 1, 2 y 3) Utiliza el esquema de codificación de borrado 6+3
Nombre de la regla	Bucket S3 finance-records
Hora de referencia	Tiempo de ingesta
Ubicaciones	Para los objetos del bucket S3 llamado finance-records, crea una copia con código de borrado en el pool especificado por el perfil de erasure-coding. Conserva 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 para el ejemplo 1

En la práctica, la mayoría de las políticas de ILM son sencillas, aunque el sistema StorageGRID permite diseñar políticas de ILM sofisticadas y complejas.

Una política típica de ILM para una red con múltiples emplazamientos podría incluir reglas de ILM como las siguientes:

- Durante la importación, almacena todos los objetos pertenecientes al bucket de S3 llamado `finance-records` en un pool de almacenamiento que contenga tres sitios. Utiliza codificación de borrado 6+3.
- Si un objeto no cumple con la primera regla de ILM, usa la regla de ILM predeterminada de la política, Two Copies Two Data Centers, para almacenar una copia de ese objeto en Site 1 y otra copia en Site 2.

Proposed policy name

Object Storage Policy

Reason for change

example 1

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	S3 Bucket finance-records	Tenant is Finance Bucket name is finance-records
Default	Two Copies Two Data Centers	—

Información relacionada

- ["Usa políticas de ILM"](#)
- ["Crear políticas de ILM"](#)

Reglas y política de ILM para el filtrado de tamaño de objetos EC en StorageGRID

Puedes usar las siguientes reglas y políticas de ejemplo como punto de partida para definir una política de ILM que filtre según el tamaño de los objetos para cumplir los requisitos recomendados de EC.



Las siguientes reglas y políticas de ILM son solo ejemplos. Existen muchas formas de configurar reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará como esperas y protegerá el contenido contra la pérdida.

Regla 1 de ILM para el ejemplo 2: usa EC para objetos mayores de 1 MB

Esta regla de ILM de ejemplo aplica códigos de borrado a los objetos que son mayores de 1 MB.



El código de borrado es más adecuado para objetos de más de 1 MB. No uses el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos muy pequeños codificados por borrado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Solo objetos EC > 1 MB
Hora de referencia	Tiempo de ingesta
Filtro avanzado por tamaño del objeto	Tamaño del objeto superior a 1 MB

Definición de regla	Valor de ejemplo
Ubicaciones	Crea una copia con código de borrado 2+1 usando tres sitios

Filter group 1 Objects with all of following metadata will be evaluated by this rule:

Object size

greater than

1

MB

Regla de ILM 2 para el ejemplo 2: dos copias replicadas

Esta regla de ILM de ejemplo crea dos copias replicadas y no filtra por tamaño de objeto. Esta regla es la regla predeterminada de la política. Dado que la primera regla descarta todos los objetos de más de 1 MB, esta regla solo se aplica a los objetos de 1 MB o menos.

Definición de regla	Valor de ejemplo
Nombre de la regla	Dos copias replicadas
Hora de referencia	Tiempo de ingesta
Filtro avanzado por tamaño del objeto	Ninguno
Ubicaciones	Desde el día 0 hasta siempre, mantén una copia replicada en el sitio 1 y otra copia replicada en el sitio 2.

Política de ILM para el ejemplo 2: usar EC para objetos de más de 1 MB

Esta política de ILM de ejemplo incluye dos reglas de ILM:

- La primera regla aplica códigos de borrado a todos los objetos que son mayores de 1 MB.
- La segunda regla de ILM (predeterminada) crea dos copias replicadas. Dado que la regla 1 ha filtrado los objetos de más de 1 MB, la regla 2 solo se aplica a los objetos de 1 MB o menos.

Reglas ILM y política para proteger archivos de imagen en StorageGRID

Puedes utilizar las siguientes reglas y la política de ejemplo para garantizar que las imágenes de más de 1 MB se codifiquen con código de borrado y que se creen dos copias de las imágenes más pequeñas.



Las siguientes reglas y políticas de ILM son solo ejemplos. Existen muchas formas de configurar reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará como esperas y protegerá el contenido contra la pérdida.

Regla 1 de ILM para el ejemplo 3: usa EC para los archivos de imagen mayores de 1 MB

Este ejemplo de regla de ILM utiliza un filtrado avanzado para aplicar el código de borrado a todos los

archivos de imagen de más de 1 MB.



El código de borrado es más adecuado para objetos de más de 1 MB. No uses el código de borrado para objetos de menos de 200 KB para evitar la sobrecarga de gestionar fragmentos muy pequeños codificados por borrado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Archivos de imagen EC > 1 MB
Hora de referencia	Tiempo de ingesta
Filtro avanzado por tamaño del objeto	Tamaño del objeto superior a 1 MB
Filtros avanzados para Key	• Termina en .jpg • Termina en .png
Ubicaciones	Crea una copia con código de borrado 2+1 usando tres sitios

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼ greater than ▼ 1 ⬆️⬇️⬆️ MB ▼ ✕

and Key ▼ ends with ▼ .jpg ✕

or **Filter group 2** Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼ greater than ▼ 1 ⬆️⬇️⬆️ MB ▼ ✕

and Key ▼ ends with ▼ .png ✕

Dado que esta regla está configurada como la primera de la política, la instrucción de ubicación del código de borrado solo se aplica a los archivos .jpg y .png que superan 1 MB.

Regla 2 de ILM para el ejemplo 3: crea 2 copias replicadas de todos los archivos de imagen restantes

Esta regla de ILM de ejemplo utiliza un filtrado avanzado para especificar que se repliquen los archivos de imagen más pequeños. Porque la primera regla de la política ya ha seleccionado los archivos de imagen de más de 1 MB, esta regla se aplica a los archivos de imagen de 1 MB o menos.

Definición de regla	Valor de ejemplo
Nombre de la regla	2 copias para los archivos de imagen
Hora de referencia	Tiempo de ingesta

649

Definición de regla	Valor de ejemplo
Filtros avanzados para Key	• Termina en .jpg • Termina en .png
Ubicaciones	Crear 2 copias replicadas en dos grupos de almacenamiento

Política de ILM para el ejemplo 3: mejor protección para los archivos de imagen

Esta política de ILM de ejemplo incluye tres reglas:

- La primera regla codifica mediante códigos de borrado todos los archivos de imagen de más de 1 MB.
- La segunda regla crea dos copias de los archivos de imagen restantes (es decir, las imágenes de 1 MB o menos).
- La regla por defecto se aplica a todos los demás objetos (es decir, a cualquier archivo que no sea una imagen).

Rule order	Rule name	Filters
1	EC image files > 1 MB	Object size is greater than 1 MB
2	2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

Reglas y políticas ILM para versiones no actuales de objetos S3 en StorageGRID

Si tienes un bucket de S3 con el versionado activado, puedes gestionar las versiones de objetos no actuales incluyendo reglas en tu política de ILM que usen "Noncurrent time" como tiempo de referencia.



Si especificas un plazo de retención limitado para los objetos, estos se eliminarán de forma definitiva una vez transcurrido dicho plazo. Asegúrate de entender durante cuánto tiempo se conservarán los objetos.

Como muestra este ejemplo, puedes controlar la cantidad de almacenamiento que ocupan los objetos versionados usando diferentes instrucciones de ubicación para las versiones no actuales de los objetos.



Las siguientes reglas y políticas de ILM son solo ejemplos. Existen muchas formas de configurar reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará como esperas y protegerá el contenido contra la pérdida.



Para realizar una simulación de la política de ILM en una versión no actual de un objeto, debes conocer el UUID o el CBID de la versión del objeto. Para encontrar el UUID y el CBID, usa ["búsqueda de metadatos de objetos"](#) mientras el objeto siga siendo actual.

Información relacionada

["Cómo se eliminan los objetos"](#)

Regla 1 de ILM para el ejemplo 4: guardar tres copias durante 10 años

Esta regla de ILM de ejemplo almacena una copia de cada objeto en tres ubicaciones durante 10 años.

Esta regla se aplica a todos los objetos, tengan o no versión.

Definición de regla	Valor de ejemplo
Grupos de almacenamiento	Tres grupos de almacenamiento, cada uno compuesto por diferentes centros de datos, llamados Site 1, Site 2 y Site 3.
Nombre de la regla	Tres copias diez años
Hora de referencia	Tiempo de ingesta
Ubicaciones	El día 0, conserva tres copias replicadas durante 10 años (3,652 días), una en el sitio 1, una en el sitio 2 y una en el sitio 3. Al cabo de 10 años, elimina todas las copias del objeto.

Regla 2 de ILM para el ejemplo 4: guarda dos copias de las versiones no actuales durante 2 años

Esta regla de ILM de ejemplo almacena dos copias de las versiones no actuales de un objeto con versiones de S3 durante 2 años.

Dado que la regla 1 de ILM se aplica a todas las versiones del objeto, debes crear otra regla para filtrar cualquier versión que no sea la actual.

Para crear una regla que utilice «Tiempo no actual» como tiempo de referencia, selecciona **Sí** en la pregunta «¿Aplicar esta regla solo a versiones antiguas de objetos (en buckets de S3 con control de versiones activado)?» en el Paso 1 (Introducir detalles) del asistente para crear una regla de ILM. Cuando seleccionas **Sí**, *Tiempo no actual* se selecciona automáticamente como tiempo de referencia y no puedes seleccionar un tiempo 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 dichas copias se almacenarán durante dos años.

Definición de regla	Valor de ejemplo
Grupos de almacenamiento	Dos grupos de almacenamiento, cada uno en un centro de datos diferente, Sitio 1 y Sitio 2.
Nombre de la regla	Versiones no actuales: dos copias dos años
Hora de referencia	Tiempo no corriente Se selecciona automáticamente cuando eliges Sí en la pregunta, «¿Aplicar esta regla solo a las versiones anteriores de los objetos (en buckets de S3 con control de versiones activado)?» en el asistente para crear una regla de ILM.
Ubicaciones	En el día 0 con respecto al tiempo no actual (es decir, a partir del día en que la versión del objeto pasa a ser la versión no actual), conserva dos copias replicadas de las versiones no actuales del objeto durante 2 años (730 días), una en Site 1 y otra en Site 2. Al cabo de 2 años, elimina las versiones no actuales.

Política de ILM para el ejemplo 4: objetos con versiones de S3

Si deseas gestionar las versiones anteriores de un objeto de forma diferente a la versión actual, las reglas que utilicen "Noncurrent time" como momento de referencia deben aparecer en la política de ILM antes que las reglas que se aplican a la versión actual del objeto.

Una política de ILM para objetos versionados de S3 podría incluir reglas de ILM como las siguientes:

- Conserva las versiones antiguas (no actuales) de cada objeto durante 2 años, a partir del día en que la versión se volvió no actual.



Las reglas de «Tiempo no actual» deben aparecer en la política antes que las reglas que se aplican a la versión actual del objeto. De lo contrario, las versiones no actuales del objeto nunca se ajustarán a la regla de «Tiempo no actual».

- En el momento de la importación, crea tres copias replicadas y almacena una copia en cada uno de los tres sitios. Conserva las copias de la versión actual del objeto durante 10 años.

Cuando simulas la política de ejemplo, esperarías que los objetos de prueba se evaluarán de la siguiente manera:

- Cualquier versión de objeto no actual se ajustaría a la primera regla. Si una versión de objeto no actual tiene más de dos años, ILM la elimina de forma permanente (se eliminan de la grid todas las copias de la versión no actual).
- La versión actual del objeto se ajustaría a la segunda regla. Cuando la versión actual del objeto lleva almacenada 10 años, el proceso ILM añade un marcador de eliminación como la versión actual del objeto y convierte la versión anterior del objeto en "no actual". La próxima vez que se realice una evaluación de ILM, esta versión no actual se ajusta a la primera regla. Como resultado, se elimina la copia en el Sitio 3 y las dos copias en el Sitio 1 y el Sitio 2 se almacenan durante 2 años más.

Reglas y política de ILM para el comportamiento de ingesta estricto en StorageGRID

Puedes utilizar un filtro de ubicación y el comportamiento de ingesta Strict en una regla para evitar que se guarden objetos en una ubicación concreta del centro de datos.

En este ejemplo, un cliente con sede en París no desea almacenar algunos objetos fuera de la UE por motivos normativos. El resto de objetos, incluidos todos los de otras cuentas de cliente, pueden almacenarse tanto en el centro de datos de París como en el de EE. UU.



Las siguientes reglas y políticas de ILM son solo ejemplos. Existen muchas formas de configurar reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará como esperas y protegerá el contenido contra la pérdida.

Información relacionada

- ["Opciones de ingesta"](#)
- ["Crear regla de ILM: seleccionar comportamiento de ingesta"](#)

Regla 1 de ILM para el ejemplo 5: ingesta estricta para garantizar el centro de datos de París

Esta regla de ILM de ejemplo utiliza el comportamiento de ingesta estricto para garantizar que los objetos guardados por un cliente con sede en París en buckets de S3 con la región configurada como 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 Paris y que tienen la región del bucket S3 configurada como eu-west-3 (Paris).

Definición de regla	Valor de ejemplo
Cuenta de inquilino	Arrendatario de Paris
Filtro avanzado	La restricción de ubicación es eu-west-3
Grupos de almacenamiento	Sede 1 (Paris)
Nombre de la regla	Ingesta estricta para garantizar el centro de datos de París
Hora de referencia	Tiempo de ingesta
Ubicaciones	El día 0, mantén dos copias replicadas para siempre en Site 1 (Paris)
Comportamiento de ingesta	Estricta. Utiliza siempre las ubicaciones de esta regla durante la ingesta. 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

654

Regla 2 de ILM para el ejemplo 5: captura equilibrada para otros objetos

Esta regla de ILM de ejemplo utiliza el comportamiento de ingesta equilibrado para ofrecer una eficiencia óptima de ILM para cualquier objeto que no se ajuste a la primera regla. Se almacenarán dos copias de todos los objetos que se ajusten a esta regla: una en el centro de datos de EE. UU. y otra en el centro de datos de París. Si la regla no se puede cumplir de inmediato, 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>
Grupos de almacenamiento	Sede 1 (París) y Sede 2 (US)
Nombre de la regla	2 copias 2 centros de datos
Hora de referencia	Tiempo de ingesta
Ubicaciones	El día 0, mantén dos copias replicadas para siempre en dos centros de datos
Comportamiento de ingesta	Equilibrado. Los objetos que cumplen esta regla se colocan según las instrucciones de colocación de la misma, si es posible. De lo contrario, se crean copias provisionales en cualquier ubicación disponible.

Política de ILM para el ejemplo 5: combinación de comportamientos de ingesta

La política de ILM de ejemplo incluye dos reglas que presentan comportamientos de ingesta diferentes.

Una política de ILM que utilice dos comportamientos de ingesta distintos podría incluir reglas de ILM como las siguientes:

- Almacena los objetos que pertenezcan al tenant de París y cuya región del bucket de S3 esté configurada como eu-west-3 (París) únicamente en el centro de datos de París. Falla la ingesta si el centro de datos de París no está disponible.
- Almacena todos los demás objetos (incluidos aquellos que pertenecen al inquilino de París pero que tienen una región de bucket diferente) tanto en el centro de datos de EE. UU. como en el centro de datos de París. Realiza copias provisionales en cualquier ubicación disponible si no se puede cumplir la instrucción de ubicación.

Cuando simulas la política de ejemplo, esperas que los objetos de prueba se evalúen de la siguiente manera:

- Cualquier objeto que pertenezca al inquilino de París y cuya región del bucket S3 esté configurada como eu-west-3 se ajusta a la primera regla y se almacena en el centro de datos de París. Porque la primera regla usa Strict ingest, estos objetos nunca se almacenan en el centro de datos de EE. UU. Si los Storage Nodes del centro de datos de París no están disponibles, la ingesta falla.
- El resto de objetos se ajustan a la segunda regla, incluidos aquellos que pertenecen al inquilino de París y

que no tienen la región del bucket de S3 configurada como eu-west-3. Se guarda una copia de cada objeto en cada centro de datos. Sin embargo, porque la segunda regla usa Balanced ingest, si un centro de datos no está disponible, se guardan dos copias provisionales en cualquier ubicación disponible.

Cómo cambiar una política ILM afecta el rendimiento de StorageGRID

Si necesitas cambiar la protección de tus datos o añades nuevos sitios, puedes crear y activar una nueva política de ILM.

Antes de modificar una política, debes comprender cómo los cambios en las ubicaciones de ILM pueden afectar temporalmente el rendimiento general de un sistema StorageGRID.

En este ejemplo, se ha añadido un nuevo sitio de StorageGRID como parte de una ampliación, y es necesario 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. Existen muchas formas de configurar reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará como esperas y protegerá el contenido contra la pérdida.

Cómo afecta al rendimiento el cambio de una política de ILM

Al activar una nueva política de ILM, el rendimiento de tu sistema StorageGRID podría verse afectado temporalmente, sobre todo si las instrucciones de ubicación de la nueva política requieren que muchos objetos existentes se trasladen a nuevas ubicaciones.

Al activar una nueva política de ILM, StorageGRID la utiliza para gestionar todos los objetos, tanto los ya existentes como los recién incorporados. Antes de activar una nueva política de ILM, revisa cualquier cambio en la ubicación de los objetos replicados y con código de borrado ya existentes. Cambiar la ubicación de un objeto existente podría provocar problemas temporales de recursos mientras se evalúan y se implementan las nuevas ubicaciones.

Para garantizar que una nueva política de ILM no afecte la ubicación de los objetos replicados y con código de borrado ya existentes, puedes **"crear una regla de ILM con un filtro de hora de ingesta"**. Por ejemplo, **Ingest time is on or after <date and time>**, así que la nueva regla solo se aplica a los objetos incorporados en o después de la fecha y hora especificadas.

Los tipos de cambios en las políticas de ILM que pueden afectar temporalmente el rendimiento de StorageGRID incluyen los siguientes:

- Aplicar un perfil de código de borrado diferente a los objetos de código de borrado existentes.



StorageGRID considera que cada perfil de código de borrado es único y no reutiliza los fragmentos de código de borrado cuando se utiliza un nuevo perfil.

- Modificar el tipo de copias requeridas para los objetos existentes; por ejemplo, convertir un gran porcentaje de objetos replicados a objetos con código de borrado.
- Trasladar copias de objetos existentes a una ubicación completamente diferente; por ejemplo, trasladar un gran número de objetos hacia o desde un Cloud Storage Pool o hacia o desde una sede remota.

Política de ILM activa para el ejemplo 6: protección de datos en dos emplazamientos

En este ejemplo, la política de ILM activa se diseñó inicialmente para un sistema StorageGRID de dos sitios y

utiliza dos reglas de 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 de ILM, los objetos pertenecientes a Tenant A están protegidos mediante código de borrado 2+1 en un único sitio, mientras que los objetos pertenecientes a todos los demás tenants están protegidos en dos sitios usando replicación de 2 copias.

Regla 1: código de borrado en un solo sitio para el inquilino A

Definición de regla	Valor de ejemplo
Nombre de la regla	Codificación de borrado en un solo sitio para el inquilino A
Cuenta de inquilino	Inquilino A
Pool de almacenamiento	Sitio 1
Ubicaciones	Codificación de borrado 2+1 en Site 1 desde el día 0 para siempre

Regla 2: replicación en dos sitios para otros inquilinos

Definición de regla	Valor de ejemplo
Nombre de la regla	Replicación en dos sitios para otros tenants
Cuenta de inquilino	Ignorar
Grupos de almacenamiento	Sitio 1 y Sitio 2
Ubicaciones	Dos copias replicadas desde el día 0 hasta siempre: una copia en Site 1 y una copia en Site 2.

Política de ILM para el ejemplo 6: protección de datos en tres sedes

En este ejemplo, la política de ILM se está sustituyendo por una nueva política para un sistema StorageGRID de tres sitios.

Tras realizar una ampliación para añadir 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 incluye los tres sitios (que no es lo mismo que el grupo de almacenamiento predeterminado All Storage Nodes). Luego, el administrador creó dos nuevas reglas de ILM y una nueva política de ILM, que está diseñada para proteger los datos en los tres sitios.

Cuando se active esta nueva política de ILM, los objetos pertenecientes a Tenant A estarán protegidos mediante código de borrado 2+1 en tres sitios, mientras que los objetos pertenecientes a otros tenants (y los objetos más pequeños pertenecientes a Tenant A) estarán protegidos en tres sitios usando replicación de 3 copias.

Regla 1: código de borrado en tres ubicaciones para Tenant A

Definición de regla	Valor de ejemplo
Nombre de la regla	Codificación de borrado en tres sitios para el tenant A
Cuenta de inquilino	Inquilino A
Pool de almacenamiento	Las tres sedes (incluye la sede 1, la sede 2 y la sede 3)
Ubicaciones	Codificación de borrado 2+1 en los 3 sitios desde el día 0 para siempre

Regla 2: replicación en tres sitios para otros inquilinos

Definición de regla	Valor de ejemplo
Nombre de la regla	Replicación en tres sitios para otros inquilinos
Cuenta de inquilino	Ignorar
Grupos de almacenamiento	Sitio 1, Sitio 2 y Sitio 3
Ubicaciones	Tres copias replicadas desde el día 0 hasta el infinito: una copia en Site 1, una copia en Site 2 y una copia en Site 3.

Activar la política de ILM para el ejemplo 6

Al activar una nueva política de ILM, es posible que los objetos existentes se trasladen a nuevas ubicaciones o que se creen nuevas copias de los objetos existentes, según las instrucciones de ubicación que figuren en las reglas nuevas o actualizadas.



Los errores en una política de ILM pueden provocar una pérdida irrecuperable de datos. Revisa detenidamente y simula la política antes de activarla para confirmar que funcionará como esperas.



Al activar una nueva política de ILM, StorageGRID la utiliza para gestionar todos los objetos, tanto los ya existentes como los recién incorporados. Antes de activar una nueva política de ILM, revisa cualquier cambio en la ubicación de los objetos replicados y con código de borrado ya existentes. Cambiar la ubicación de un objeto existente podría provocar problemas temporales de recursos mientras se evalúan y se implementan las nuevas ubicaciones.

¿Qué pasa cuando cambian las instrucciones de codificación de borrado?

En la política de ILM actualmente activa para este ejemplo, los objetos pertenecientes a Tenant A están protegidos mediante código de borrado 2+1 en el sitio 1. En la nueva política de ILM, los objetos pertenecientes a Tenant A estarán protegidos mediante código de borrado 2+1 en los sitios 1, 2 y 3.

Cuando se activa la nueva política de ILM, se llevan a cabo las siguientes operaciones de ILM:

- Los nuevos objetos incorporados por Tenant A se dividen en dos fragmentos de datos y se añade un fragmento de paridad. Luego, cada uno de los tres fragmentos se almacena en un sitio diferente.
- Los objetos existentes que pertenecen a Tenant A se reevalúan durante el proceso de análisis de ILM en curso. Porque las instrucciones de ubicación de ILM usan un nuevo perfil de código de borrado, se crean fragmentos con código de borrado completamente nuevos y se distribuyen en los tres sitios.



Los fragmentos 2+1 existentes en el sitio 1 no se reutilizan. StorageGRID considera que cada perfil de código de borrado es único y no reutiliza los fragmentos de código de borrado cuando se utiliza un nuevo perfil.

¿Qué ocurre cuando cambian las instrucciones de replicación?

En la política de ILM actualmente activa para este ejemplo, los objetos que pertenecen a otros inquilinos se protegen mediante dos copias replicadas en los grupos de almacenamiento de los sitios 1 y 2. En la nueva política de ILM, los objetos que pertenecen a otros inquilinos se protegerán mediante tres copias replicadas en los grupos de almacenamiento de los sitios 1, 2 y 3.

Cuando se activa la nueva política de ILM, se llevan a cabo las siguientes operaciones de ILM:

- Cuando cualquier inquilino que no sea Tenant A incorpora un nuevo objeto, StorageGRID crea tres copias y guarda una copia en cada sitio.
- Los objetos existentes que pertenecen a estos otros inquilinos se reevalúan durante el proceso de análisis de ILM en curso. Porque las copias existentes del objeto en Site 1 y Site 2 siguen cumpliendo los requisitos de replicación de la nueva regla de ILM, StorageGRID solo necesita crear una nueva copia del objeto para Site 3.

Impacto en el rendimiento de la activación de esta política

Cuando se active la política de ILM de este ejemplo, el rendimiento general de este sistema StorageGRID se verá afectado temporalmente. Se necesitarán niveles de recursos de grid superiores a los habituales para crear nuevos fragmentos con código de borrado para los objetos existentes de Tenant A y nuevas copias replicadas en Site 3 para los objetos existentes de otros tenants.

Como consecuencia del cambio en la política de ILM, las solicitudes de lectura y escritura de los clientes podrían experimentar temporalmente latencias superiores a las normales. Las latencias volverán a los niveles normales después de que las instrucciones de ubicación se implementen por completo en toda la grid.

Para evitar problemas con los recursos al activar una nueva política de ILM, puedes usar el filtro avanzado

Ingest time en cualquier regla que pueda cambiar la ubicación de un gran número de objetos existentes. Establece Ingest time en un valor mayor o igual a la hora aproximada en la que la nueva política entrará en vigor para asegurarte de que los objetos existentes no se trasladen innecesariamente.



Ponte en contacto con el soporte técnico si necesitas reducir o aumentar la velocidad a la que se procesan los objetos tras un cambio en la política de ILM.

Política ILM compatible para S3 Object Lock en StorageGRID

Puedes utilizar el depósito de S3, las reglas de ILM y la política de ILM de este ejemplo como punto de partida a la hora de definir una política de ILM que cumpla los requisitos de protección y retención de los objetos en depósitos con S3 Object Lock habilitado.



Si has utilizado la función de Compliance heredada en versiones anteriores de StorageGRID, también puedes usar este ejemplo para gestionar cualquier bucket existente que tenga activada la función de Compliance heredada.



Las siguientes reglas y políticas de ILM son solo ejemplos. Existen muchas formas de configurar reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará como esperas y protegerá el contenido contra la pérdida.

Información relacionada

- ["Gestiona objetos con S3 Object Lock"](#)
- ["Crear una política de ILM"](#)

Bucket y objetos para el ejemplo de S3 Object Lock

En este ejemplo, una cuenta de inquilino de S3 llamada Bank of ABC ha usado el Tenant Manager para crear un bucket con S3 Object Lock activado para guardar registros bancarios críticos.

Definición de bucket	Valor de ejemplo
Nombre de la cuenta del inquilino	Banco ABC
Nombre del bucket	registros bancarios
Región de bucket	us-east-1 (predeterminado)

Cada objeto y cada versión de objeto que se añada al bucket bank-records usará los siguientes valores para retain-until-date y legal hold.

Configuración de cada objeto	Valor de ejemplo
retain-until-date	«2030-12-30T23:59:59Z» (30 de diciembre de 2030) Cada versión de objeto tiene su propio retain-until-date valor. Este valor se puede aumentar, pero no disminuir.

Configuración de cada objeto	Valor de ejemplo
legal hold	"OFF" (No está en vigor) Se puede aplicar o levantar una retención legal sobre cualquier versión de un objeto en cualquier momento durante el periodo de retención. Si un objeto está sujeto a una retención legal, no se puede eliminar aunque se haya alcanzado el <code>retain-until-date</code>.

Regla 1 de ILM para S3 Object Lock: perfil de código de borrado con coincidencia de buckets

Esta regla de ILM de ejemplo se aplica únicamente a la cuenta de cliente de S3 denominada Bank of ABC. Coincide con cualquier objeto en el bucket `bank-records` y luego utiliza el código de borrado para almacenar el objeto en los Storage Nodes de tres sitios de centros de datos usando un perfil de código de borrado 6+3. Esta regla cumple los requisitos de los buckets con S3 Object Lock habilitado: se mantiene una copia en los Storage Nodes desde el día 0 para siempre, usando la hora de ingesta como referencia.

Definición de regla	Valor de ejemplo
Nombre de la regla	Regla de cumplimiento: Objetos EC en el bucket <code>bank-records</code> - Bank of ABC
Cuenta de inquilino	Banco ABC
Nombre del bucket	<code>bank-records</code>
Filtro avanzado	Tamaño del objeto (MB) superior a 1 Nota: Este filtro garantiza que no se utilice el código de borrado para los objetos de 1 MB o menos.

Definición de regla	Valor de ejemplo
Hora de referencia	Tiempo de ingesta
Ubicaciones	Desde el día 0 almacena para siempre
Perfil de código de borrado	• Crea una copia con código de borrado en los nodos de almacenamiento en tres centros de datos • Utiliza un esquema de código de borrado 6+3

Regla n.º 2 de ILM para el ejemplo de S3 Object Lock: regla no conforme

Esta regla ILM de ejemplo almacena inicialmente dos copias replicadas del objeto en Storage Nodes. Después de un año, almacena una copia en un Cloud Storage Pool para siempre. Como esta regla usa un Cloud Storage Pool, no cumple y no se aplicará a los objetos en los buckets con S3 Object Lock habilitado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Regla incumplida: usar Cloud Storage Pool
Cuentas de inquilinos	No especificado
Nombre del bucket	No se especifica, pero solo se aplicará a los buckets que no tengan activado S3 Object Lock (o la función heredada de Compliance).
Filtro avanzado	No especificado

Definición de regla	Valor de ejemplo
Hora de referencia	Tiempo de ingesta
Ubicaciones	• El día 0, mantén dos copias replicadas en los nodos de almacenamiento en Data Center 1 y Data Center 2 durante 365 días • Después de 1 año, conserva una copia replicada en un Cloud Storage Pool para siempre

Regla 3 de ILM para S3 Object Lock: regla predeterminada

Esta regla de ILM de ejemplo copia los datos de los objetos a grupos de almacenamiento en dos centros de datos. Esta regla conforme está diseñada para ser la regla predeterminada en la política de ILM. No incluye ningún filtro, no utiliza el tiempo de referencia Noncurrent y cumple los requisitos de los buckets con S3 Object Lock habilitado: se conservan dos copias de los objetos en los Storage Nodes desde el día 0 hasta siempre, utilizando Ingest como tiempo de referencia.

Definición de regla	Valor de ejemplo
Nombre de la regla	Regla de cumplimiento predeterminada: dos copias en dos centros de datos
Cuenta de inquilino	No especificado
Nombre del bucket	No especificado
Filtro avanzado	No especificado

Definición de regla	Valor de ejemplo
Hora de referencia	Tiempo de ingesta
Ubicaciones	Desde el día 0 y de forma permanente, mantén dos copias replicadas: una en los nodos de almacenamiento en Data Center 1 y otra en los nodos de almacenamiento en Data Center 2.

Ejemplo de política de ILM conforme a los requisitos para S3 Object Lock

Para crear una política de ILM que proteja de forma eficaz todos los objetos de tu sistema, incluidos los que se encuentran en buckets con S3 Object Lock activado, debes seleccionar reglas de ILM que cumplan los requisitos de almacenamiento de todos los objetos. Luego, tienes que simular y activar la política.

Agrega reglas a la política

En este ejemplo, la política de ILM incluye tres reglas de ILM, en el siguiente orden:

1. Una regla conforme que utiliza código de borrado para proteger objetos de más de 1 MB en un bucket específico con S3 Object Lock activado. Los objetos se almacenan en Storage Nodes desde el día 0 hasta siempre.
2. Una regla no conforme que crea dos copias replicadas de un objeto en Storage Nodes durante un año y luego mueve una copia del objeto a un Cloud Storage Pool para siempre. Esta regla no se aplica a los buckets con S3 Object Lock habilitado porque utiliza un Cloud Storage Pool.
3. La regla de cumplimiento predeterminada que crea dos copias replicadas de objetos en los Storage Nodes desde el día 0 y para siempre.

Simular la política

Una vez que hayas añadido reglas a tu política, hayas elegido una regla de cumplimiento predeterminada y hayas organizado el resto de reglas, debes simular la política probando objetos del bucket en el que se ha habilitado S3 Object Lock y de otros buckets. Por ejemplo, al simular la política de ejemplo, esperarías que los objetos de prueba se evaluarán de la siguiente manera:

- La primera regla solo coincidirá con los objetos de prueba que sean mayores de 1 MB en el bucket bank-records para el inquilino Bank of ABC.
- La segunda regla coincidirá con todos los objetos en todos los buckets no conformes de todas las demás cuentas de inquilino.
- La regla predeterminada coincidirá con estos objetos:
 - Objetos de 1 MB o menos en el bucket bank-records para el tenant Bank of ABC.
 - Objetos en cualquier otro depósito que tenga S3 Object Lock activado para todas las demás cuentas de inquilino.

Activa la política

Cuando estés completamente seguro de que la nueva política protege los datos de los objetos como esperabas, puedes activarla.

Cómo interactúan el ciclo de vida de los buckets S3 y la política ILM en StorageGRID

En función de la configuración del ciclo de vida, los objetos siguen los parámetros de retención del ciclo de vida del bucket de S3 o de una política de ILM.

Ejemplo de cómo el ciclo de vida de un bucket tiene prioridad sobre la política de ILM

Política de ILM

- Regla basada en una referencia temporal no actual: el día 0, conserva X copias durante 20 días
- Regla basada en la referencia de la hora de ingesta (por defecto): el día 0, conserva X copias durante 50 días

Ciclo de vida del bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},  
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Resultado

- Se ha importado un objeto denominado "docs/text". Coincide con el filtro de ciclo de vida del bucket que tiene el prefijo "docs/".
 - Después de 100 días se crea un marcador de eliminación y "docs/text" pasa a ser no actual.
 - Después de 5 días, es decir, un total de 105 días desde la incorporación, "docs/text" se elimina.
 - Después de 95 días, un total de 200 días desde la ingestión y 100 días desde que se creó el marcador de eliminación, se elimina el marcador de eliminación caducado.
- Se ha importado un objeto denominado "video/movie". No coincide con el filtro y utiliza la política de retención de ILM.
 - Después de 50 días, se crea un marcador de eliminación y "video/movie" pasa a estar no actual.
 - Después de 20 días, es decir, un total de 70 días desde la ingesta, "video/movie" se elimina.
 - Después de 30 días, es decir, un total de 100 días desde la ingesta y 50 días desde que se creó el marcador de eliminación, el marcador de eliminación caducado se elimina.

Ejemplo de ciclo de vida de un bucket que, de forma implícita, se mantiene indefinidamente

Política de ILM

- Regla basada en una referencia temporal no actual: el día 0, conserva X copias durante 20 días
- Regla basada en la referencia de la hora de ingesta (por defecto): el día 0, conserva X copias durante 50 días

Ciclo de vida del bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":  
true}
```

Resultado

- Se ha importado un objeto denominado "docs/text". Coincide con el filtro de ciclo de vida del bucket que tiene el prefijo "docs/".

La acción `Expiration` solo se aplica a los marcadores de eliminación caducados, lo que implica conservar todo lo demás para siempre (empezando por "docs/").

Los marcadores de eliminación que empiezan por "docs/" se eliminan cuando caducan.

- Se ha importado un objeto denominado "video/movie". No coincide con el filtro y utiliza la política de retención de ILM.
 - Después de 50 días, se crea un marcador de eliminación y "video/movie" pasa a estar no actual.
 - Después de 20 días, es decir, un total de 70 días desde la ingesta, "video/movie" se elimina.
 - Después de 30 días, es decir, un total de 100 días desde la ingesta y 50 días desde que se creó el marcador de eliminación, el marcador de eliminación caducado se elimina.

Ejemplo de cómo utilizar el ciclo de vida de los buckets para duplicar el ILM y eliminar los marcadores de eliminación caducados

Política de ILM

- Regla basada en una referencia temporal no actual: el día 0, conserva X copias durante 20 días
- Regla basada en la referencia de la hora de importación (por defecto): el día 0, conserva X copias para siempre

Ciclo de vida del bucket

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},  
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Resultado

- La política de ILM se duplica en el ciclo de vida del bucket.
 - La regla «para siempre» de la política ILM está diseñada para eliminar objetos manualmente y limpiar las versiones obsoletas al cabo de 20 días. Por consiguiente, la regla basada en la fecha de ingesta conservará para siempre los marcadores de eliminación caducados.
 - El ciclo de vida del bucket reproduce el comportamiento de la política de ILM mientras añade "ExpiredObjectDeleteMarker": true, que elimina los marcadores de eliminación una vez que han caducado
- Se ingiere un objeto. La ausencia de filtro significa que el ciclo de vida del bucket se aplica a todos los objetos y anula la configuración de retención de ILM.
 - Cuando un inquilino envía una solicitud de eliminación de un objeto, se crea un marcador de eliminación y el objeto pasa a estar no 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.

Refuerzo del sistema para StorageGRID

Conoce el endurecimiento del sistema para StorageGRID

El refuerzo de la seguridad del sistema es el proceso de eliminar la mayor cantidad posible de riesgos de seguridad de un sistema StorageGRID.

Al instalar y configurar StorageGRID, sigue estas directrices para cumplir con los objetivos de seguridad establecidos en materia de confidencialidad, integridad y disponibilidad.

Ya deberías estar aplicando las mejores prácticas estándar del sector para el refuerzo de la seguridad del sistema. Por ejemplo, debes utilizar contraseñas seguras para StorageGRID, emplear HTTPS en lugar de HTTP y habilitar la autenticación basada en certificados siempre que sea posible. Estas mejores prácticas deben incluir medidas de seguridad física y ambiental que limiten el acceso físico, además de proteger el centro de datos físico y la infraestructura de apoyo. También debes consultar las normas y recomendaciones reglamentarias aplicables a tu negocio y zona geográfica.

StorageGRID sigue el ["NetApp Política de gestión de vulnerabilidades"](#). Las vulnerabilidades notificadas se verifican y se abordan según el proceso de respuesta a incidentes de seguridad del producto.

A la hora de reforzar la seguridad de un sistema StorageGRID, ten en cuenta lo siguiente:

- ¿Cuál de las tres redes de StorageGRID has implementado? Todos los sistemas StorageGRID deben

usar la red Grid, pero también podrías estar usando la red Admin, la red Client o ambas. Cada red tiene diferentes consideraciones de seguridad.

- **El tipo de plataformas** que utilices para los nodos individuales de tu sistema StorageGRID. Los nodos de StorageGRID pueden implementarse en máquinas virtuales de 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 prácticas recomendadas de refuerzo.
- **El nivel de confianza de las cuentas de inquilino.** Si eres un proveedor de servicios con cuentas de inquilino no fiables, tendrás otras preocupaciones en materia de seguridad que si solo usas cuentas de inquilino internas y fiables.
- **Qué requisitos y normas de seguridad** sigue tu organización. Es posible que tengas que cumplir con requisitos normativos o corporativos específicos.

Directrices de refuerzo para las actualizaciones de software de StorageGRID

Debes mantener actualizados tu sistema StorageGRID y los servicios relacionados para protegerte frente a ataques.

Actualizaciones del software StorageGRID

Siempre que sea posible, deberías actualizar el software de StorageGRID a la versión principal más reciente o a la versión principal anterior. Mantener StorageGRID actualizado ayuda a reducir el tiempo durante el que las vulnerabilidades conocidas están activas y reduce la superficie de ataque total. Además, las versiones más recientes de StorageGRID suelen incluir funciones de refuerzo de la seguridad que no están incluidas en versiones anteriores.

Consulta el "[Herramienta NetApp Interoperability Matrix Tool](#)" (IMT) para determinar qué versión del software StorageGRID debes usar. Cuando se requiere una corrección urgente, NetApp prioriza crear actualizaciones para las versiones más recientes. Algunos parches podrían no ser compatibles con versiones anteriores.

- Para descargar las últimas versiones y correcciones urgentes de StorageGRID, visita "[Descargas de NetApp: StorageGRID](#)".
- Para actualizar el software de StorageGRID, consulta la "[instrucciones de actualización](#)".
- Para aplicar una corrección urgente, consulta el "[Procedimiento de corrección urgente de StorageGRID](#)".

Mejoras en los servicios externos

Los servicios externos pueden presentar vulnerabilidades que afecten indirectamente a StorageGRID. Asegúrate de que los servicios de los que depende StorageGRID se mantengan actualizados. Estos servicios incluyen LDAP, KMS (o KMIP server), DNS y NTP.

Para consultar la lista de versiones compatibles, consulta el "[Herramienta NetApp Interoperability Matrix Tool](#)".

Actualizaciones de los hipervisores

Si tus nodos de StorageGRID se ejecutan en VMware u otro hipervisor, debes asegurarte de que el software y el firmware del hipervisor estén actualizados.

Para consultar la lista de versiones compatibles, consulta el "[Herramienta NetApp Interoperability Matrix Tool](#)".

Actualizaciones de los nodos de Linux

Si los nodos de StorageGRID utilizan plataformas de host Linux, debes asegurarte de que se apliquen las actualizaciones de seguridad y del kernel al sistema operativo del host. Además, debes aplicar las actualizaciones de firmware al hardware vulnerable cuando estas actualizaciones estén disponibles.

Para consultar la lista de versiones compatibles, consulta el ["Herramienta NetApp Interoperability Matrix Tool"](#).

Directrices de refuerzo de la seguridad para redes StorageGRID

El sistema StorageGRID admite hasta tres interfaces de red por nodo de la red, lo que te permite configurar la red de cada nodo de forma individual para que se adapte a tus requisitos de seguridad y acceso.

Para obtener información detallada sobre las redes StorageGRID, consulta la ["Tipos de redes StorageGRID"](#).

Directrices para la red Grid

Debes configurar una Grid Network para todo el tráfico interno de StorageGRID. Todos los nodos de la grid están en la Grid Network y deben poder comunicarse con todos los demás nodos.

Al configurar la Grid Network, sigue estas directrices:

- Asegúrate de que la red esté protegida frente a clientes no fiables, como los que están en internet abierta.
- Siempre que sea posible, utiliza la Grid Network exclusivamente para el tráfico interno. Tanto la Admin Network como la Client Network tienen restricciones adicionales de firewall que bloquean el tráfico externo hacia los servicios internos. Usar la Grid Network para el tráfico externo de los clientes está permitido, pero este uso ofrece menos capas de protección.
- Si la implementación de StorageGRID abarca varios centros de datos, usa una red privada virtual (VPN) o una solución equivalente en la red Grid para brindar protección adicional al tráfico interno.
- Algunos procedimientos de mantenimiento requieren acceso SSH (Secure Shell) en el puerto 22 entre el nodo de administración principal y todos los demás nodos de la grid. Usa un firewall externo para restringir el acceso SSH a clientes de confianza.

Directrices para la red de administración

La red de administración se utiliza normalmente 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 impone este uso internamente.

Si utilizas la red de administración, sigue estas instrucciones:

- Bloquea todos los puertos de tráfico interno en la red de administración. Consulta el ["lista de puertos internos"](#).
- Si hay clientes no fiables que puedan acceder a la red de administración, bloquea el acceso a StorageGRID en dicha red mediante un cortafuegos externo.

Directrices para la red de clientes

La red de clientes se utiliza normalmente para los inquilinos y para comunicarse con servicios externos, como el servicio de replicación CloudMirror o con otro servicio de la plataforma. Sin embargo, StorageGRID no impone este uso internamente.

Si utilizas la Client Network, sigue estas instrucciones:

- Bloquea todos los puertos de tráfico interno en la red del cliente. Consulta ["lista de puertos internos"](#).
- Acepta el tráfico entrante de los clientes únicamente en los puntos finales configurados explícitamente. Consulta la información sobre ["gestión de los controles del cortafuegos"](#).

Directrices de refuerzo de la seguridad para los nodos de StorageGRID

Los nodos de StorageGRID pueden implementarse en máquinas virtuales de 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 prácticas recomendadas de refuerzo de la seguridad.

Controlar el acceso IPMI remoto al BMC

Puedes activar o desactivar el acceso IPMI remoto para todos los dispositivos que incluyan un BMC. La interfaz IPMI remota permite el acceso de bajo nivel al hardware de tus dispositivos StorageGRID a cualquier persona que tenga una cuenta y una contraseña de BMC. Si no necesitas acceso IPMI remoto al BMC, desactiva esta opción.

- Para controlar el acceso IPMI remoto al BMC en Grid Manager, ve a **Configuración > Seguridad > Ajustes de seguridad > Dispositivos**:
 - Desmarca la casilla **Habilitar acceso IPMI remoto** para desactivar el acceso IPMI al BMC.
 - Marca la casilla **Habilitar acceso IPMI remoto** para habilitar el acceso IPMI al BMC.

Para obtener información adicional sobre el refuerzo de BMC, consulta la ["Refuerza los controladores de gestión de placas base"](#) ficha informativa sobre ciberseguridad de la ["Agencia de Seguridad Nacional \(NSA\)"](#) y la ["Agencia de Ciberseguridad y Seguridad de las Infraestructuras \(CISA\)"](#).

Configuración del cortafuegos

Como parte del proceso de refuerzo de la seguridad del sistema, debes revisar las configuraciones de los cortafuegos externos y modificarlas para que solo se acepte el tráfico procedente de las direcciones IP y en los puertos desde los que sea estrictamente necesario.

StorageGRID incluye un cortafuegos interno en cada nodo que mejora la seguridad de tu grid, ya que te permite controlar el acceso a la red al nodo. Debes ["gestionar los controles del firewall interno"](#) para evitar el acceso a la red en todos los puertos excepto en los necesarios para tu implementación específica de grid. Los cambios de configuración que realices en la página de control del cortafuegos se aplican a cada nodo.

En concreto, puedes gestionar las siguientes áreas:

- **Direcciones privilegiadas:** Puedes permitir que determinadas direcciones IP o subredes accedan a los puertos que están bloqueados mediante la configuración de la pestaña Gestionar acceso externo.
- **Gestiona el acceso externo:** Puedes cerrar los puertos que están abiertos por defecto o volver a abrir los puertos que cerraste antes.
- **Red de clientes no fiables:** Puedes especificar si un nodo considera fiable el tráfico entrante procedente de la red de clientes, así como los puertos adicionales que deseas mantener abiertos cuando se configura una red de clientes no fiables.

Aunque este cortafuegos interno ofrece una capa adicional de protección frente a algunas amenazas

habituales, no elimina la necesidad de un cortafuegos externo.

Para consultar una lista de todos los puertos internos y externos que utiliza StorageGRID, visita ["Puertos internos de StorageGRID"](#) y ["Puertos utilizados para las comunicaciones externas"](#).

Desactivar los servicios que no se utilicen

En todos los nodos de StorageGRID, debes desactivar o bloquear el acceso a los servicios que no uses. Por ejemplo, si no planeas usar DHCP, usa Grid Manager para cerrar el puerto 68. Selecciona **Configuration > Firewall control > Manage external access**. Luego cambia el interruptor de estado del puerto 68 de **Open** a **Closed**.

Virtualización, contenedores y hardware compartido

En todos los nodos de StorageGRID, evita ejecutar StorageGRID en el mismo hardware físico que software no confiable. No asumas que las protecciones del hipervisor impedirán que el malware acceda a los datos protegidos por StorageGRID si tanto StorageGRID como el malware están en el mismo hardware físico. Por ejemplo, los ataques Meltdown y Spectre aprovechan vulnerabilidades críticas en procesadores modernos y permiten que los programas roben datos de la memoria en el mismo ordenador.

Proteger los nodos durante la instalación

No permitas que usuarios no de confianza accedan a los nodos de StorageGRID a través de la red mientras se están instalando. Los nodos no están totalmente protegidos hasta que se hayan unido a la grid.

Limita el acceso físico al hardware

Debes limitar el acceso físico a los nodos de los dispositivos de hardware de StorageGRID, así como a los hosts de máquinas virtuales de VMware y a los hosts de Linux donde se ejecuta StorageGRID, solo a los administradores autorizados. Algunos ejemplos de controles de acceso físico incluyen cerraduras, guardias, barreras físicas y videovigilancia.

Los nodos de dispositivos de hardware están diseñados para que solo los instalen y los utilicen administradores autorizados. No dejes que administradores no autorizados accedan a los nodos de dispositivos de hardware.

Directrices para los nodos de administración

Los nodos de administración proporcionan servicios de gestión, como la configuración del sistema, la supervisión y el registro de eventos. Cuando inicias sesión en Grid Manager o en Tenant Manager, te conectas a un nodo de administración.

Sigue estas instrucciones para proteger los nodos de administración en tu sistema StorageGRID:

- Protege todos los nodos de administración frente a clientes no fiables, como los que se encuentran en la red pública de Internet. Asegúrate de que ningún cliente no fiable 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. Concede a cada grupo de usuarios los permisos mínimos necesarios para su función y utiliza el modo de acceso de solo lectura para evitar que los usuarios modifiquen la configuración.
- Cuando utilices los puntos de conexión del equilibrador de carga de StorageGRID, usa nodos de puerta de enlace en lugar de nodos de administración para el tráfico de clientes no fiables.
- Si tienes inquilinos no de confianza, no les permitas tener acceso directo al Tenant Manager ni a la Tenant

Management API. En su lugar, haz que los inquilinos no de confianza utilicen un portal de inquilinos o un sistema externo de gestión de inquilinos que interactúe con la Tenant Management API.

- Si lo deseas, utiliza un proxy de administración para tener más control sobre la comunicación de AutoSupport desde los nodos de administración hacia NetApp Support. Consulta los pasos para ["creando un proxy de administrador"](#).
- Si lo deseas, utiliza los puertos restringidos 8443 y 9443 para separar las comunicaciones entre Grid Manager y Tenant Manager. Bloquea el puerto compartido 443 y limita las solicitudes de los inquilinos al puerto 9443 para mayor protección.
- Opcionalmente, usa nodos de administración independientes para los administradores del grid y los usuarios de los tenants.

Para obtener más información, consulta las instrucciones de ["administrar StorageGRID"](#).

Directrices para los nodos de almacenamiento

Los nodos de almacenamiento gestionan y almacenan datos de objetos y metadatos. Sigue estas directrices para proteger los nodos de almacenamiento de tu sistema StorageGRID.

- No permitas que clientes no fiables se conecten directamente a los nodos de almacenamiento. Usa un endpoint de equilibrador de carga servido por un Gateway Node o un equilibrador de carga de terceros.
- No habilites los servicios de salida para los inquilinos no fiables. Por ejemplo, al crear la cuenta de un inquilino no fiable, no permitas que este utilice su propia fuente de identidad ni que utilice los servicios de la plataforma. Consulta los pasos en ["crear una cuenta de inquilino"](#).
- Utiliza un equilibrador de carga de terceros para el tráfico de clientes no fiables. El equilibrio de carga de terceros ofrece más control y capas adicionales de protección contra ataques.
- Si lo deseas, usa un proxy de almacenamiento para tener más control sobre los Cloud Storage Pools y la comunicación de los servicios de la plataforma desde los nodos de almacenamiento hacia servicios externos. Consulta los pasos para ["creación de un proxy de almacenamiento"](#).
- Si lo deseas, conéctate a servicios externos usando la Client Network. Luego, selecciona **Configuration > Security > Firewall control > Untrusted Client Networks** e indica que la Client Network en el Storage Node no es de confianza. El Storage Node ya no acepta ningún tráfico entrante en la Client Network, pero sigue permitiendo las solicitudes salientes para Platform Services.

Directrices para los nodos de gateway

Los nodos de puerta de enlace proporcionan una interfaz opcional de equilibrio de carga que las aplicaciones cliente pueden utilizar para conectarse a StorageGRID. Sigue estas directrices para proteger cualquier nodo de puerta de enlace de tu sistema StorageGRID:

- Configura y usa los endpoints del balanceador de carga. Consulta ["Aspectos a tener en cuenta para el equilibrio de carga"](#).
- Utiliza 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 fiables. El equilibrio de carga de terceros ofrece más control y capas adicionales de protección contra ataques. Si usas un equilibrador de carga de terceros, el tráfico de red también puede configurarse opcionalmente para pasar por un endpoint interno del equilibrador de carga o enviarse directamente a los nodos de almacenamiento.
- Si utilizas puntos finales de equilibrador de carga, puedes optar por que los clientes se conecten a través de la Client Network. Luego, selecciona **Configuration > Security > Firewall control > Untrusted Client Networks** e indica que la Client Network en el Gateway Node no es de confianza. El Gateway Node solo acepta tráfico entrante en los puertos configurados explícitamente como puntos finales de equilibrador de carga.

Directrices para los nodos de dispositivos de hardware

Los dispositivos de hardware de StorageGRID están diseñados específicamente para su uso en un sistema StorageGRID. Algunos dispositivos pueden usarse como Storage Nodes. Otros dispositivos pueden usarse como Admin Nodes o Gateway Nodes. Puedes combinar nodos de dispositivo con nodos basados en software o implementar grids totalmente diseñados solo con dispositivos.

Sigue estas directrices para proteger cualquier nodo de dispositivo de hardware de tu sistema StorageGRID:

- Si el dispositivo utiliza SANtricity System Manager para la administración de los controladores de almacenamiento, evita que los clientes no de confianza accedan a SANtricity System Manager a través de la red.
- Si el dispositivo cuenta con un controlador de gestión de placa base (BMC), ten en cuenta que el puerto de gestión del BMC permite el acceso de bajo nivel al hardware. Conecta el puerto de gestión del BMC solo a una red de gestión interna segura y de confianza.

Puedes establecer una VLAN para aislar las conexiones de red del BMC y restringir el acceso a Internet del BMC a redes de confianza. Para obtener más información sobre cómo aplicar la separación por VLAN, consulta la hoja informativa de ciberseguridad de ["Refuerza los controladores de gestión de placas base"](#) y de ["Agencia de Seguridad Nacional \(NSA\)"](#) y ["Agencia de Ciberseguridad y Seguridad de las Infraestructuras \(CISA\)"](#).

Si no se dispone de una red de gestión interna segura y fiable, deja el puerto de gestión de BMC sin conectar o bloqueado. Es posible que el soporte técnico solicite acceso temporal durante un caso de soporte.

- Si el dispositivo admite la gestión remota del hardware del controlador a través de Ethernet mediante el estándar Intelligent Platform Management Interface (IPMI), bloquea el tráfico no fiable en el puerto 623.



Puedes habilitar o deshabilitar el acceso IPMI remoto para todos los appliances que contengan un BMC. La interfaz IPMI remota permite el acceso a nivel de hardware de bajo nivel a tus appliances StorageGRID a cualquier persona que tenga una cuenta y contraseña de BMC. Si no necesitas acceso IPMI remoto al BMC, deshabilita esta opción mediante uno de los siguientes métodos: + en Grid Manager, ve a **Configuration > Security > Security settings > Appliances** y desmarca la casilla de verificación **Enable remote IPMI access**. + en la API de gestión de Grid, usa el endpoint privado: `PUT /private/bmc`.

+ También puedes [desactivar el acceso remoto a IPMI](#).

- Para los modelos de dispositivos que incluyan unidades SED, FDE o FIPS NL-SAS y que gestionas con SANtricity System Manager, ["Habilitar y configurar SANtricity Drive Security"](#).
- Para los modelos de dispositivos que incluyen unidades SSD SED o FIPS NVMe y que gestionas usando el StorageGRID Appliance Installer y Grid Manager, ["Habilita y configura el cifrado de unidades de StorageGRID"](#).
- En el caso de los dispositivos que no cuenten con unidades SED, FDE o FIPS, usa un servidor de gestión de claves (KMS) para ["Habilita y configura el cifrado de los nodos de software de StorageGRID"](#).

Información relacionada

["Conoce la seguridad de las unidades en SANtricity System Manager"](#)

Directrices de endurecimiento para TLS y SSH en StorageGRID

Debes controlar el acceso SSH, reemplazar los certificados TLS predeterminados y seleccionar la política de seguridad adecuada para las conexiones TLS y SSH.

Directrices de refuerzo de la seguridad de los certificados

Debes sustituir los certificados predeterminados creados durante la instalación por tus propios certificados personalizados.

Para muchas organizaciones, el certificado digital autofirmado para el acceso web a StorageGRID no cumple con sus políticas de seguridad de la información. En los sistemas de producción, deberías instalar un certificado digital firmado por una CA para usarlo en la autenticación de StorageGRID.

En concreto, deberías utilizar certificados de servidor personalizados en lugar de estos certificados predeterminados:

- **Certificado de interfaz de gestión:** Se utiliza para proteger el acceso al Grid Manager, al Tenant Manager, a la Grid Management API y a la Tenant Management API.
- **Certificado de la API de S3:** Se utiliza para proteger el acceso a los nodos de almacenamiento y a los nodos de puerta de enlace, que las aplicaciones cliente de S3 utilizan para cargar y descargar datos de objetos.

Consulta ["Gestiona certificados de seguridad"](#) para obtener detalles e instrucciones.



StorageGRID gestiona por separado los certificados utilizados para los puntos finales del equilibrador de carga. Para configurar los certificados del equilibrador de carga, consulta ["Configura los puntos de conexión del equilibrador de carga"](#).

Si utilizas certificados de servidor personalizados, sigue estas directrices:

- Los certificados deben tener un `subjectAltName` que coincida con las entradas DNS de StorageGRID. Para más detalles, consulta la sección 4.2.1.6, "Subject Alternative Name", en ["RFC 5280: Perfil de certificados PKIX y CRL"](#).
- Siempre que sea posible, evita el uso de certificados comodín. Una excepción a esta directriz es el certificado para un endpoint de estilo S3 virtual hosted, que requiere el uso de un comodín si no se conocen de antemano los nombres de los buckets.
- Cuando tengas que utilizar comodines en los certificados, debes tomar medidas adicionales para reducir los riesgos. Utiliza un patrón de comodín como `*.s3.example.com`, y no utilices el sufijo `s3.example.com` para otras aplicaciones. Este patrón también funciona con el acceso S3 de tipo ruta, como `dc1-s1.s3.example.com/mybucket`.
- Establece plazos de caducidad cortos para los certificados (por ejemplo, 2 meses) y utiliza la Grid Management API para automatizar la rotación de certificados. Esto es especialmente importante para los certificados comodín.

Además, los clientes deben aplicar una verificación rigurosa del nombre de host al comunicarse con StorageGRID.

Directrices de refuerzo para la política de TLS y SSH

Puedes seleccionar una política de seguridad para determinar qué protocolos y algoritmos de cifrado se utilizan para establecer conexiones TLS seguras con aplicaciones cliente y conexiones SSH seguras con los

servicios internos de StorageGRID.

La política de seguridad controla cómo TLS y SSH cifran los datos en tránsito. Como práctica recomendada, debes desactivar las opciones de cifrado que no sean necesarias para la compatibilidad de las aplicaciones. Utiliza la política predeterminada Modern, a menos que tu sistema necesite cumplir con Common Criteria, FIPS 140-2, o que necesites usar otros cifrados.

Consulta ["Administra la política de TLS y SSH"](#) para obtener más detalles e instrucciones.

Gestiona el acceso externo mediante SSH

Para mejorar la seguridad del sistema, el acceso SSH externo está bloqueado de forma predeterminada. Activa el acceso SSH únicamente cuando necesites realizar tareas que requieran acceso SSH entrante, como la resolución de problemas. Consulta ["Gestiona el acceso externo mediante SSH"](#) para obtener más detalles e instrucciones.

Directrices de refuerzo para logs, contraseñas y mensajes de auditoría en StorageGRID

Además de seguir las directrices de refuerzo de la seguridad para las redes y los nodos de StorageGRID, debes seguir las directrices de refuerzo de la seguridad para otras áreas del sistema StorageGRID.

Contraseña de instalación temporal

Para proteger el sistema StorageGRID durante la instalación, establece una contraseña en la página de contraseña temporal del instalador, disponible en la interfaz de usuario de instalación de StorageGRID o en la API de instalación. Una vez establecida, esta contraseña se aplica a todos los métodos de instalación de StorageGRID, incluyendo la interfaz de usuario, la API de instalación y `configure-storagegrid.py` script.

Para más información, consulta:

- ["Instalar StorageGRID en nodos basados en software"](#)
- ["Instalar el dispositivo StorageGRID"](#)

Registros y mensajes de auditoría

Protege siempre de forma segura los registros de StorageGRID y la salida de mensajes de auditoría. Los registros de StorageGRID y los mensajes de auditoría proporcionan información muy valiosa desde el punto de vista del soporte y la disponibilidad del sistema. Además, la información y los detalles que contienen los registros de StorageGRID y la salida de mensajes de auditoría suelen ser de naturaleza sensible.

Configura StorageGRID para enviar eventos de seguridad a un servidor syslog externo. Si utilizas la exportación syslog, selecciona TLS y RELP/TLS como protocolos de transporte.

Consulta la ["Referencia de los archivos de registro"](#) para más información sobre los registros de StorageGRID. Consulta ["Mensajes de auditoría"](#) para más información sobre los mensajes de auditoría de StorageGRID.

NetApp AutoSupport

La función AutoSupport de StorageGRID te permite supervisar de forma proactiva el estado de tu sistema y enviar automáticamente paquetes al sitio de soporte de NetApp, al equipo de soporte interno de tu organización o a un socio de soporte. De forma predeterminada, el envío de paquetes AutoSupport a NetApp

está habilitado cuando se configura StorageGRID por primera vez.

La función AutoSupport se puede desactivar. Sin embargo, NetApp recomienda activarla porque AutoSupport ayuda a acelerar la identificación y resolución de problemas si surge algún inconveniente en tu sistema StorageGRID.

AutoSupport admite HTTPS, HTTP y SMTP como protocolos de transporte. Debido al carácter sensible de los paquetes de AutoSupport, NetApp recomienda encarecidamente usar HTTPS como protocolo de transporte predeterminado para enviar paquetes de AutoSupport a NetApp.

Compartición de recursos entre orígenes (CORS)

Puedes configurar el intercambio de recursos entre orígenes (CORS) para un bucket de S3 si quieres que ese bucket y los objetos en ese bucket sean accesibles para aplicaciones web en otros dominios. En general, no actives CORS a menos que sea necesario. Si CORS es necesario, restríngelo a orígenes de confianza.

Consulta los pasos para ["configuración de CORS para buckets y objetos"](#).

Dispositivos de seguridad externos

Una solución de refuerzo de seguridad completa debe tener en cuenta los mecanismos de seguridad externos a StorageGRID. El uso de dispositivos de infraestructura adicionales para filtrar y limitar el acceso a StorageGRID es una forma eficaz de establecer y mantener un nivel de seguridad riguroso. Entre estos dispositivos de seguridad externos se incluyen cortafuegos, sistemas de prevención de intrusiones (IPS) y otros dispositivos de seguridad.

Se recomienda utilizar un equilibrador de carga de terceros para el tráfico de clientes no fiables. El equilibrio de carga de terceros ofrece más control y capas adicionales de protección contra ataques.

Mitigación de ransomware

Ayuda a proteger los datos de tus objetos frente a los ataques de ransomware siguiendo las recomendaciones en ["Defensa contra ransomware con StorageGRID"](#).

StorageGRID con FabricPool

Flujo de trabajo de configuración para usar StorageGRID con FabricPool

Si utilizas el software NetApp ONTAP, puedes usar NetApp FabricPool para trasladar los datos inactivos a un sistema de almacenamiento de objetos NetApp StorageGRID.

Sigue estas instrucciones para:

- Descubre los aspectos que hay que tener en cuenta y las mejores prácticas para configurar StorageGRID para una carga de trabajo de FabricPool.
- Descubre cómo configurar un sistema de almacenamiento de objetos StorageGRID para utilizarlo con FabricPool.
- Descubre cómo proporcionar los valores necesarios a ONTAP al conectar StorageGRID como un nivel de nube FabricPool.

Guía de inicio rápido para configurar StorageGRID para FabricPool

1

Planifica tu configuración

- Decide qué política de organización por niveles de volúmenes de FabricPool vas a utilizar para organizar por niveles los datos inactivos de ONTAP en StorageGRID.
- Planifica e instala un sistema StorageGRID que se adapte a tus necesidades de capacidad de almacenamiento y rendimiento.
- Familiarízate con el software del sistema StorageGRID, incluyendo el ["Grid Manager"](#) y el ["Administrador de inquilinos"](#).
- Consulta las mejores prácticas de FabricPool para ["Grupos HA"](#), ["balanceo de carga"](#), ["ILM"](#) y ["más"](#).
- Consulta estos recursos adicionales, que ofrecen información detallada sobre el uso y la configuración de ONTAP y FabricPool:

["TR-4598: FabricPool prácticas recomendadas en ONTAP"](#)

["Documentación de ONTAP para FabricPool"](#)

2

Realiza las tareas previas necesarias

Obtén el ["Información necesaria para integrar StorageGRID como nivel de nube"](#), que incluye:

- Direcciones IP
- Nombres de dominio
- Certificado SSL

Si lo deseas, configura ["federación de identidades"](#) y ["inicio de sesión único"](#).

3

Configura los ajustes de StorageGRID

Utiliza StorageGRID para obtener los valores que ONTAP necesita para conectarse a la grid.

Usar la ["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

Configura ONTAP y DNS

Usa ONTAP para ["añadir un nivel de nube"](#) que use los valores de StorageGRID. Después, ["configurar las entradas DNS"](#) para asociar direcciones IP a cualquier nombre de dominio que planees usar.

5

Supervisar y gestionar

Cuando tu sistema esté en funcionamiento, realiza tareas continuas en ONTAP y StorageGRID para gestionar y supervisar la organización en niveles 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 en la nube. Usar agregados habilitados para FabricPool te ayuda a reducir los costes de almacenamiento sin comprometer el rendimiento, la eficiencia ni la protección.

FabricPool asocia un nivel en la 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 organización por niveles manteniendo los datos activos (calientes) en almacenamiento de alto rendimiento (el nivel local) y trasladando los datos inactivos (fríos) al almacén de objetos externo (el nivel en la nube).

No es necesario realizar ningún cambio arquitectónico y puedes seguir gestionando tus datos y tu entorno de aplicaciones desde el sistema de almacenamiento central ONTAP.

¿Qué es StorageGRID?

NetApp StorageGRID es una arquitectura de almacenamiento que gestiona los datos como objetos, a diferencia de otras arquitecturas de almacenamiento como el almacenamiento de archivos o de bloques. Los objetos se guardan dentro de un único contenedor (como un bucket) y no se anidan como archivos dentro de un directorio dentro de otros directorios. Aunque el almacenamiento de objetos generalmente ofrece un rendimiento inferior al del almacenamiento de archivos o de bloques, es significativamente más escalable. Los buckets de StorageGRID pueden albergar petabytes de datos y miles de millones de objetos.

¿Por qué usar StorageGRID como cloud tier de FabricPool?

FabricPool puede organizar en niveles los datos de ONTAP en varios proveedores de almacenamiento de objetos, incluido StorageGRID. A diferencia de las nubes públicas que pueden establecer un número máximo de operaciones de entrada/salida por segundo (IOPS) admitidas a nivel de bucket o contenedor, el rendimiento de StorageGRID escala con el número de nodos del sistema. Usar StorageGRID como nivel de nube de FabricPool te permite mantener tus datos inactivos en tu propia nube privada para obtener el máximo rendimiento y un control total sobre tus datos.

Además, no se requiere una licencia de FabricPool cuando usas StorageGRID como nivel de cloud.

Información necesaria para adjuntar StorageGRID como un nivel de nube FabricPool

Antes de poder vincular StorageGRID como un nivel de nube para FabricPool, debes realizar pasos de configuración en StorageGRID y obtener ciertos valores para usarlos en ONTAP.

¿Qué valores necesito?

La siguiente tabla muestra los valores que debes configurar en StorageGRID y cómo los utilizan ONTAP y el servidor DNS.

Valor	Dónde se configura el valor	Dónde se utiliza el valor
Direcciones IP virtuales (VIP)	StorageGRID > Grupo de alta disponibilidad	Entrada DNS

Valor	Dónde se configura el valor	Dónde se utiliza el valor
Puerto	StorageGRID > Punto de conexión del equilibrador de carga	ONTAP System Manager > Añadir cloud tier
Certificado SSL	StorageGRID > Punto de conexión del equilibrador de carga	ONTAP System Manager > Añadir cloud tier
Nombre del servidor (FQDN)	StorageGRID > Punto de conexión del equilibrador de carga	Entrada DNS
ID de la clave de acceso y clave secreta de acceso	StorageGRID > Usuario y bucket	ONTAP System Manager > Añadir cloud tier
Nombre del bucket/contenedor	StorageGRID > Usuario y bucket	ONTAP System Manager > Añadir cloud tier

¿Cómo obtengo estos valores?

En función de tus necesidades, puedes hacer cualquiera de las siguientes cosas para obtener la información que necesitas:

- Usa el ["Asistente de configuración de FabricPool"](#). El asistente de configuración de FabricPool te ayuda a configurar rápidamente los valores necesarios en StorageGRID y genera un archivo que puedes usar para configurar ONTAP System Manager. El asistente te guía por los pasos necesarios y te ayuda a asegurarte de que tu configuración cumple con las prácticas recomendadas de StorageGRID y FabricPool.
- Configura cada elemento manualmente. A continuación, introduce los valores en ONTAP System Manager o en la CLI de ONTAP. Sigue estos pasos:
 - a. ["Configura un grupo de alta disponibilidad \(HA\) para FabricPool"](#).
 - b. ["Crear un punto de conexión del equilibrador de carga para FabricPool"](#).
 - c. ["Crear una cuenta de inquilino para FabricPool"](#).
 - d. Inicia sesión en la cuenta del tenant y ["Crea el bucket y las claves de acceso para el usuario raíz"](#).
 - e. Crea una regla de ILM para los datos de FabricPool y añádela a tus políticas de ILM activas. Consulta ["Configura ILM para los datos de FabricPool"](#).
 - f. Si lo prefieres, ["crea una política de clasificación de tráfico para FabricPool"](#).

Utiliza el asistente de configuración de FabricPool

Conoce el asistente de configuración de StorageGRID FabricPool

Puedes usar 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, puedes ingresar los datos necesarios en ONTAP System Manager.

Cuándo usar el asistente de configuración de FabricPool

El asistente de configuración de FabricPool te guía por cada paso para configurar StorageGRID para usarlo con FabricPool y configura automáticamente ciertas entidades por ti, como las políticas de ILM y de clasificación del tráfico. Como parte de completar el asistente, descargas un archivo que puedes usar para ingresar valores en ONTAP System Manager. Usa el asistente para configurar tu sistema más rápido y para asegurarte de que tu configuración cumple con las prácticas recomendadas de StorageGRID y FabricPool.

Si tienes permiso de acceso a raíz, puedes completar el asistente de configuración de FabricPool cuando empieces a usar StorageGRID Grid Manager, o puedes acceder y completar el asistente en cualquier momento posterior. Dependiendo de tus necesidades, también puedes configurar manualmente algunos o todos los elementos necesarios y luego usar el asistente para reunir en un solo archivo los valores que ONTAP necesita.



Utiliza el asistente de configuración de FabricPool a menos que sepas que tienes requisitos especiales o que tu implementación requiera una personalización significativa.

Antes de utilizar el asistente

Comprueba que has completado estos pasos previos.

Revisa las mejores prácticas

- Tienes un conocimiento general de la ["Información necesaria para integrar StorageGRID como nivel de nube"](#).
- Has consultado las prácticas recomendadas de FabricPool para:
 - ["Grupos de alta disponibilidad \(HA\)"](#)
 - ["Balanceo de carga"](#)
 - ["Normas y política de ILM"](#)

Obtener direcciones IP y configurar interfaces VLAN

Si vas a configurar un grupo de alta disponibilidad (HA), sabes a qué nodos se conectará ONTAP y qué red StorageGRID se usará. También sabes qué valores ingresar para el CIDR de la subred, la dirección IP de la puerta de enlace y las direcciones IP virtuales (VIP).

Si planeas usar una LAN virtual para segregar el tráfico de FabricPool, ya configuraste la interfaz VLAN. Consulta ["Configurar interfaces VLAN"](#).

Configura la federación de identidades y el inicio de sesión único (SSO)

Si tienes previsto usar la federación de identidades o el inicio de sesión único (SSO) para tu sistema StorageGRID, ya habrás habilitado estas funciones. También sabes qué grupo federado debe tener acceso a raíz para la cuenta de inquilino que ONTAP va a usar. Consulta ["Usa la federación de identidades"](#) y ["Configura el inicio de sesión único"](#).

Obtener y configurar nombres de dominio

- Ya sabes qué nombre de dominio completo (FQDN) debes usar para StorageGRID. Las entradas del servidor DNS asignarán este FQDN a las direcciones IP virtuales (VIP) del grupo HA que crees usando el asistente. Consulta ["Configura el servidor DNS"](#).
- Si tienes pensado utilizar solicitudes de S3 con el estilo de alojamiento virtual, tienes ["Nombres de dominio"](#)

de los endpoints S3 configurados". ONTAP utiliza por defecto URL con estructura de ruta, pero se recomienda utilizar solicitudes con el estilo de alojamiento virtual.

Revisa los requisitos del equilibrador de carga y del certificado de seguridad

Si tienes previsto usar el equilibrador de carga de StorageGRID, ya revisaste la información general "[consideraciones para el equilibrio de carga](#)". Tienes los certificados que vas a subir o los valores que necesitas para generar un certificado.

Si tienes previsto usar un endpoint de un equilibrador de carga externo (de terceros), tienes el nombre de dominio completo (FQDN), el puerto y el certificado para ese equilibrador de carga.

Confirma la configuración del grupo de almacenamiento ILM

Si inicialmente instalaste StorageGRID 11.6 o una versión anterior, ya habrás configurado el grupo de almacenamiento que vas a utilizar. En general, debes crear un grupo de almacenamiento para cada sitio de StorageGRID que vayas a utilizar para almacenar datos de ONTAP.



Este requisito previo no se aplica si inicialmente instalaste StorageGRID 11.7 o 11.8. Cuando instalas inicialmente cualquiera de estas versiones, los grupos de almacenamiento se crean automáticamente para cada sitio.

Relación entre ONTAP y el nivel de nube de StorageGRID

El asistente de FabricPool te guía a lo largo del proceso de creación de un único nivel de nube de StorageGRID que incluye un inquilino de StorageGRID, un conjunto de claves de acceso y un bucket de StorageGRID. Puedes asociar este nivel de nube de StorageGRID a uno o varios niveles locales de ONTAP.

La práctica recomendada general consiste en asociar un único nivel en la nube a varios niveles locales dentro de un clúster. Sin embargo, en función de tus necesidades, podrías querer usar más de un bucket o incluso más de un tenant de StorageGRID para los niveles locales de un solo clúster. Usar diferentes buckets y tenants te 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 gestionar.

NetApp no recomienda vincular un único nivel en la nube a niveles locales de varios clústeres.



Para conocer las mejores prácticas para usar StorageGRID con NetApp MetroCluster™ y FabricPool Mirror, consulta "[TR-4598: FabricPool prácticas recomendadas en ONTAP](#)".

Opcional: utiliza un bucket diferente para cada nivel local

Para utilizar más de un bucket para los niveles locales en un clúster ONTAP, añade más de un nivel de nube de StorageGRID en ONTAP. Cada nivel de nube comparte el mismo grupo de alta disponibilidad (HA), el mismo punto final del equilibrador de carga, el mismo inquilino y las mismas claves de acceso, pero utiliza un contenedor diferente (bucket de StorageGRID). Sigue estos pasos generales:

1. Desde StorageGRID Grid Manager, completa el asistente de configuración de FabricPool para el primer nivel de la nube.
2. Desde ONTAP System Manager, añade un nivel de nube y utiliza el archivo que descargaste de StorageGRID para proporcionar los valores requeridos.
3. Desde StorageGRID Tenant Manager, inicia sesión en el inquilino que fue creado por el asistente y crea un segundo bucket.

4. Vuelve a completar el asistente de FabricPool. Selecciona el grupo HA existente, el endpoint del balanceador de carga y el tenant. Luego, selecciona el nuevo bucket que creaste manualmente. Crea una nueva regla de ILM para el nuevo bucket y activa una política de ILM que incluya esa regla.
5. Desde ONTAP, añade un segundo nivel en la nube pero indica el nombre del nuevo bucket.

Opcional: utiliza un inquilino y un bucket diferentes para cada nivel local

Para utilizar más de un inquilino y diferentes conjuntos de claves de acceso para los niveles locales en un clúster ONTAP, añade más de un nivel de nube de StorageGRID en ONTAP. Cada nivel de nube comparte el mismo grupo de alta disponibilidad (HA) y el mismo punto final del equilibrador de carga, pero utiliza un inquilino, claves de acceso y contenedor (bucket de StorageGRID) diferentes. Sigue estos pasos generales:

1. Desde StorageGRID Grid Manager, completa el asistente de configuración de FabricPool para el primer nivel de la nube.
2. Desde ONTAP System Manager, añade un nivel de nube y utiliza el archivo que descargaste de StorageGRID para proporcionar los valores requeridos.
3. Vuelve a completar el asistente de FabricPool. Selecciona el grupo HA existente y el endpoint del balanceador de carga. Crea un nuevo tenant y bucket. Crea una nueva regla de ILM para el nuevo bucket y activa una política de ILM que incluya esa regla.
4. Desde ONTAP, añade un segundo nivel de nube, pero introduce la nueva clave de acceso, la clave secreta y el nombre del bucket.

Accede y completa el asistente de configuración de StorageGRID FabricPool

Puedes usar 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

- Has revisado la ["consideraciones y requisitos"](#) para usar el asistente de configuración de FabricPool.



Si quieres configurar StorageGRID para utilizarlo con cualquier otra aplicación cliente S3, ve a ["Usa el asistente de configuración de S3"](#).

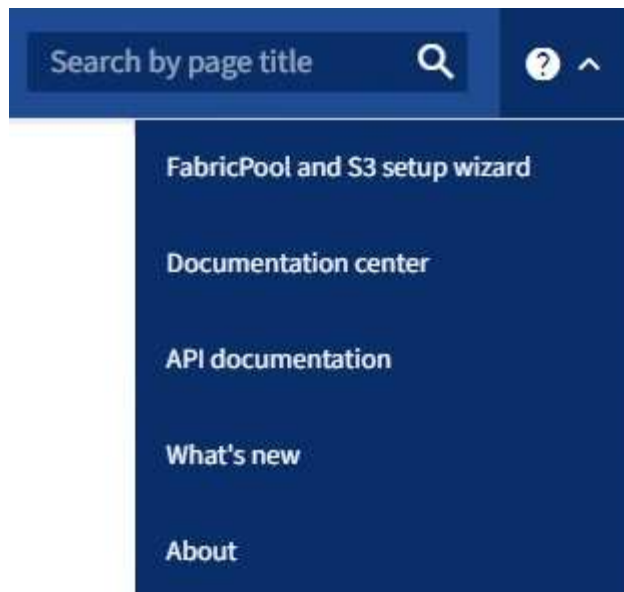
- Tienes el ["Permiso de acceso raíz"](#).

Accede al asistente

Puedes completar el asistente de configuración de FabricPool cuando empieces a usar StorageGRID Grid Manager, o puedes acceder y completar el asistente en cualquier momento después.

Pasos

1. Inicia sesión en Grid Manager usando una ["navegador web compatible"](#) cuenta.
2. Si aparece en el panel de control el banner **FabricPool and S3 setup wizard**, selecciona el enlace que aparece en el banner. Si el banner ya no aparece, selecciona el icono de ayuda de la barra de encabezado en el Grid Manager y selecciona **FabricPool and S3 setup wizard**.



3. En la sección FabricPool de la página del asistente de configuración de FabricPool y S3, selecciona **Configurar ahora**.

Paso 1 de 9: Configurar el grupo de alta disponibilidad aparece.

Paso 1 de 9: Configura el grupo de alta disponibilidad

Un grupo de alta disponibilidad (HA) es un conjunto de nodos que contienen, cada uno de ellos, el servicio StorageGRID Load Balancer. Un grupo HA puede contener Gateway Nodes, Admin Nodes o ambos.

Puedes usar un grupo de alta disponibilidad (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 altamente disponible al servicio Load Balancer. Si la interfaz activa en el grupo de alta disponibilidad falla, una interfaz de respaldo puede gestionar la carga de trabajo con poco impacto en las operaciones de FabricPool.

Para obtener más información sobre esta tarea, consulta ["Gestiona grupos de alta disponibilidad"](#) y ["Prácticas recomendadas para grupos de alta disponibilidad"](#).

Pasos

1. Si tienes pensado utilizar un equilibrador de carga externo, no es necesario que crees un grupo de alta disponibilidad. Selecciona **Omitir este paso** y ve a [Paso 2 de 9: Configura el endpoint del balanceador de carga](#).
2. Para utilizar el equilibrador de carga de StorageGRID, crea un nuevo grupo de alta disponibilidad o utiliza uno ya existente.

Crear grupo de alta disponibilidad

- Para crear un nuevo grupo de alta disponibilidad, selecciona **Crear grupo de alta disponibilidad**.
- En el paso **Introducir datos**, rellena los siguientes campos.

Campo	Descripción
Nombre del grupo HA	Un nombre para mostrar único para este grupo de alta disponibilidad.
Descripción (opcional)	La descripción de este grupo de HA.

- En el paso **Add interfaces**, selecciona las interfaces de nodo que quieres usar en este grupo de alta disponibilidad.

Utiliza los encabezados de las columnas para ordenar las filas o introduce un término de búsqueda para encontrar interfaces más rápido.

Puedes seleccionar uno o varios nodos, pero solo puedes seleccionar una interfaz por cada nodo.

- Para el paso **Priorizar interfaces**, determina la interfaz principal y cualquier interfaz de respaldo para este grupo de alta disponibilidad.

Arrastra las filas para cambiar los valores de la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa salvo que se produzca un fallo.

Si el grupo de alta disponibilidad (HA) incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se transfieren a la primera interfaz de respaldo según el orden de prioridad. Si esa interfaz falla, las direcciones VIP se transfieren a la siguiente interfaz de respaldo, y así sucesivamente. Cuando se resuelven los fallos, las direcciones VIP vuelven a la interfaz disponible con mayor prioridad.

- En el paso **Introducir direcciones IP**, completa los siguientes campos.

Campo	Descripción
CIDR de la 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 activado. 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, introduce la dirección IP de la pasarela local VIP de StorageGRID. La dirección IP de la pasarela local debe estar dentro de la subred VIP.

Campo	Descripción
Dirección IP virtual	Introduce al menos una y no más de diez direcciones VIP para la interfaz activa del grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP y todas estarán activas al mismo tiempo en la interfaz activa. Al menos una dirección debe ser IPv4. Opcionalmente, puedes especificar direcciones IPv4 e IPv6 adicionales.

f. Selecciona **Crear grupo de alta disponibilidad** y luego selecciona **Finalizar** para volver al asistente de configuración de FabricPool.

g. Selecciona **Continuar** para pasar al paso del equilibrador de carga.

Usa el grupo de alta disponibilidad existente

a. Para utilizar un grupo de alta disponibilidad ya existente, selecciona el nombre del grupo de alta disponibilidad en la lista desplegable **Select an HA group**.

b. Selecciona **Continuar** para pasar al paso del equilibrador de carga.

Paso 2 de 9: Configura el endpoint del balanceador de carga

StorageGRID utiliza un equilibrador de carga para gestionar la carga de trabajo de las aplicaciones cliente, como FabricPool. El equilibrio de carga maximiza la velocidad y la capacidad de conexión entre varios nodos de almacenamiento.

Puedes utilizar el servicio StorageGRID Load Balancer, que está disponible en todos los nodos Gateway y Admin, o puedes conectarte a un equilibrador de carga externo (de terceros). Se recomienda usar el load balancer de StorageGRID.

Para obtener más información sobre esta tarea, consulta la guía general "[consideraciones para el equilibrio de carga](#)" y la guía "[buenas prácticas para el equilibrio de carga en FabricPool](#)".

Pasos

1. Selecciona o crea un punto final del equilibrador de carga de StorageGRID o utiliza un equilibrador de carga externo.

Crear punto final

- Selecciona **Crear endpoint**.
- En el paso **Introducir los datos del punto final**, rellena los siguientes campos.

Campo	Descripción
Nombre	Un nombre descriptivo para el endpoint.
Puerto	El puerto de StorageGRID que deseas utilizar para el equilibrio de carga. Este campo tiene por defecto el valor 10433 para el primer punto final que crees, pero puedes introducir cualquier puerto externo que no esté en uso. Si introduces 80 o 443, el punto final solo se configura en los nodos de Gateway, porque estos puertos están reservados en los nodos de Admin. Nota: No se permiten los puertos utilizados por otros servicios de la grid. Consulta el "Referencia de puertos de red".
Tipo de cliente	Debe ser S3 .
Protocolo de red	Selecciona HTTPS. Nota: La comunicación con StorageGRID sin cifrado TLS es compatible, pero no se recomienda.

- En el paso **Seleccionar modo de enlace**, especifica el modo de enlace. El modo de enlace controla cómo se accede al endpoint utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final usando la dirección IP de cualquier Gateway Node o Admin Node, la dirección IP virtual (VIP) de cualquier grupo HA en cualquier red, o el FQDN correspondiente. Utiliza la configuración Global (por defecto) a menos que necesites restringir la accesibilidad de este endpoint.
Direcciones IP virtuales de los grupos de alta disponibilidad	Los clientes deben utilizar una dirección IP virtual (o el nombre de dominio completo correspondiente) de un grupo de alta disponibilidad para acceder a este endpoint. Todos los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que selecciones para los puntos finales no se solapen.
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o los FQDN correspondientes) de las interfaces de los nodos seleccionados para acceder a este endpoint.

Modo	Descripción
Tipo de nodo	En función del tipo de nodo que selecciones, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier Admin Node o la dirección IP (o el FQDN correspondiente) de cualquier Gateway Node para acceder a este endpoint.

d. Para el paso **Acceso del inquilino**, selecciona una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (por defecto)	Todas las cuentas de inquilinos pueden usar este endpoint para acceder a sus buckets. Permitir a todos los inquilinos suele ser casi siempre la opción adecuada para el endpoint del balanceador de carga usado para FabricPool. Debes seleccionar esta opción si estás utilizando el asistente de configuración de FabricPool para un nuevo sistema StorageGRID y aún no has creado ninguna cuenta de inquilino.
Permitir inquilinos seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este endpoint para acceder a sus buckets.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este endpoint para acceder a sus buckets. El resto de inquilinos sí pueden utilizar este endpoint.

e. En el paso **Adjuntar certificado**, selecciona una de las siguientes opciones:

Campo	Descripción
Subir certificado (recomendado)	Utiliza esta opción para cargar un certificado de servidor firmado por una CA, la clave privada del certificado y, opcionalmente, el paquete de CA.
Generar certificado	Utiliza esta opción para generar un certificado autofirmado. Consulta "Configura los puntos de conexión del equilibrador de carga" para ver los detalles de qué debes introducir.
Usa el certificado S3 de StorageGRID	Esta opción solo está disponible si ya has subido o generado una versión personalizada del certificado global de StorageGRID. Consulta "Configura los certificados de la API de S3" para obtener más información.

f. Selecciona **Finalizar** para volver al asistente de configuración de FabricPool.

g. Selecciona **Continuar** para pasar al paso del inquilino y el bucket.



Los cambios en el certificado de un endpoint pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Utiliza el punto de conexión del equilibrador de carga existente

- Selecciona el nombre de un punto final existente en la lista desplegable **Selecciona un punto final del equilibrador de carga**.
- Selecciona **Continuar** para pasar al paso del inquilino y el bucket.

Utilizar un equilibrador de carga externo

- Rellena los siguientes campos para el equilibrador de carga externo.

Campo	Descripción
FQDN	El nombre de dominio completo (FQDN) del equilibrador de carga externo.
Puerto	El número de puerto que utilizará FabricPool para conectarse al equilibrador de carga externo.
Certificado	Copia el certificado del servidor del equilibrador de carga externo y pégalo en este campo.

- Selecciona **Continuar** para pasar al paso del inquilino y el bucket.

Paso 3 de 9: inquilino y bucket

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, buckets, objetos y un conjunto específico de capacidades. Debes crear un inquilino de StorageGRID antes de poder crear el bucket que usará FabricPool.

Un bucket es un contenedor que se utiliza para almacenar los objetos y los metadatos de un inquilino. Aunque algunos inquilinos pueden tener muchos buckets, el asistente solo te permite crear o seleccionar un inquilino y un bucket a la vez. Puedes usar el Tenant Manager más adelante para añadir cualquier bucket adicional que necesites.

Puedes crear un nuevo inquilino y un depósito para uso de FabricPool, o puedes seleccionar un inquilino y un depósito existentes. Si creas 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 información sobre esta tarea, consulta ["Crear una cuenta de inquilino para FabricPool"](#) y ["Crea un depósito de S3 y obtén una clave de acceso"](#).

Pasos

Crea un nuevo inquilino y un depósito, o selecciona un inquilino existente.

Nuevo inquilino y bucket

1. Para crear un nuevo tenant y bucket, introduce un **Tenant name**. Por ejemplo, `FabricPool tenant`.
2. Define el acceso a raíz para la cuenta de inquilino, en función de si tu sistema StorageGRID utiliza "federación de identidades", "inicio de sesión único (SSO)" o ambos.

Opción	Haz esto
Si la federación de identidades no está habilitada	Indica la contraseña que se usará al iniciar sesión en el tenant como usuario raíz local.
Si la federación de identidades está activada	a. Selecciona un grupo federado ya existente para disponer de permiso de acceso a raíz para el inquilino. b. Si lo deseas, indica la contraseña que se usará al iniciar sesión en el tenant como usuario raíz local.
Si están habilitados tanto la federación de identidades como el inicio de sesión único (SSO)	Selecciona un grupo federado existente para tener permiso de acceso a raíz para el inquilino. Ningún usuario local puede iniciar sesión.

3. En «**Nombre del bucket**», introduce el nombre del bucket que FabricPool usará para almacenar los datos de ONTAP. Por ejemplo, `fabricpool-bucket`.



No puedes cambiar el nombre del bucket después de crearlo.

4. Selecciona la **región** para este depósito.

Utiliza la región predeterminada (`us-east-1`) a menos que tengas previsto utilizar ILM en el futuro para filtrar objetos en función de la región del bucket.

5. Selecciona **Crear y continuar** para crear el inquilino y el bucket y pasar al paso de descarga de datos

Selecciona el tenant y el bucket

La cuenta de inquilino existente debe tener al menos un bucket en el que no esté habilitado el versionado. No puedes seleccionar una cuenta de inquilino existente si no hay ningún bucket para ese inquilino.

1. Selecciona el inquilino existente en la lista desplegable **Nombre del inquilino**.
2. Selecciona el bucket existente de la lista desplegable **Nombre del bucket**.

FabricPool no admite el control de versiones de objetos, por lo que no se muestran los buckets que tienen activado el control de versiones.



No selecciones un bucket que tenga activada la función S3 Object Lock para utilizarlo con FabricPool.

3. Selecciona **Continuar** para pasar al paso de descarga de datos.

Paso 4 de 9: Descargar la configuración de ONTAP

Durante este paso, descargas un archivo que puedes usar para ingresar valores en ONTAP System Manager.

Pasos

1. Si lo deseas, selecciona el icono de copiar () para copiar tanto el ID de la clave de acceso como la clave de acceso secreta al portapapeles.

Estos valores se incluyen en el archivo descargado, pero quizá te interese guardarlos por separado.

2. Selecciona **Descargar configuración de ONTAP** para descargar un archivo de texto que contiene los valores que has introducido hasta ahora.

El archivo `ONTAP_FabricPool_settings_bucketname.txt` incluye la información que necesitas para configurar StorageGRID como el sistema de almacenamiento de objetos para un nivel de nube de FabricPool, incluyendo:

- Datos de conexión del equilibrador de carga, incluyendo el nombre del servidor (FQDN), el puerto y el certificado
- Nombre del bucket
- ID de la clave de acceso y clave secreta de acceso para el usuario raíz de la cuenta del inquilino

3. Guarda las claves copiadas y el archivo descargado en un lugar seguro.



No cierres esta página hasta que hayas copiado ambas claves de acceso, descargado la configuración de ONTAP o ambas cosas. Las claves no estarán disponibles después de que cierres esta página. Asegúrate de guardar esta información en un lugar seguro porque puede usarse para obtener datos de tu sistema StorageGRID.

4. Marca la casilla de verificación para confirmar que has descargado o copiado el ID de la clave de acceso y la clave de acceso secreta.
5. Selecciona **Continuar** para pasar al paso del grupo de almacenamiento ILM.

Paso 5 de 9: selecciona un grupo de almacenamiento

Un grupo de almacenamiento es un conjunto de nodos de almacenamiento. Cuando seleccionas un grupo de almacenamiento, determinas qué nodos usará StorageGRID para almacenar los datos transferidos por niveles desde ONTAP.

Para obtener más información sobre este paso, consulta ["Crear un grupo de almacenamiento"](#).

Pasos

1. En la lista desplegable **Sitio**, selecciona el sitio de StorageGRID que quieres usar para los datos jerarquizados desde ONTAP.
2. En la lista desplegable **Storage pool**, selecciona el storage pool para ese sitio.

El grupo de almacenamiento de un sitio incluye todos los nodos de almacenamiento de ese sitio.

3. Selecciona **Continuar** para pasar al paso de la regla de ILM.

Paso 6 de 9: revisa la regla de ILM para FabricPool

Las reglas de gestión del ciclo de vida de la información (ILM) controlan la ubicación, la duración y el comportamiento de ingesta de todos los objetos en tu sistema StorageGRID.

El asistente de configuración de FabricPool crea automáticamente la regla ILM recomendada para el uso de FabricPool. Esta regla solo se aplica al bucket que especificaste. Utiliza codificación de borrado 2+1 en un único sitio para almacenar los datos que se transfieren desde ONTAP.

Para obtener más información sobre este paso, consulta ["Crear regla de ILM"](#) y ["Prácticas recomendadas para usar ILM con datos de FabricPool"](#).

Pasos

1. Revisa los detalles de la regla.

Campo	Descripción
Nombre de la regla	Se genera automáticamente y no se puede modificar
Descripción	Se genera automáticamente y no se puede modificar
Filtro	El nombre del bucket Esta regla solo se aplica a los objetos guardados en el depósito que hayas especificado.
Hora de referencia	Tiempo de ingesta La instrucción de ubicación se inicia cuando los objetos se guardan por primera vez en el bucket.
Instrucción de colocación	Utiliza el código de borrado 2+1

2. Ordena 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 - forever**. **Día 0** significa que la regla se aplica cuando los datos se transfieren desde ONTAP. **Forever** significa que StorageGRID ILM no eliminará los datos que se hayan transferido desde ONTAP.
 - El **grupo de almacenamiento** de la regla es el grupo de almacenamiento que has seleccionado. **EC 2+1** significa que los datos se almacenarán utilizando el código 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 dentro de un mismo sitio.
3. Selecciona **Crear y continuar** para crear esta regla y pasar al paso de la política de ILM.

Paso 7 de 9: revisar y activar la política de ILM

Después de que el asistente de configuración de FabricPool crea la regla de ILM para uso de FabricPool, crea una política de ILM. Debes simular y revisar cuidadosamente esta política antes de activarla.

Para obtener más información sobre este paso, consulta ["Crear política de ILM"](#) y ["Prácticas recomendadas para usar ILM con datos de FabricPool"](#).



Cuando activas una nueva política de ILM, StorageGRID usa esa política para gestionar la ubicación, la duración y la protección de los datos de todos los objetos en la grid, incluidos los objetos existentes y los objetos recién incorporados. En algunos casos, activar una nueva política puede hacer que los objetos existentes se muevan a nuevas ubicaciones.



Para evitar la pérdida de datos, no utilices una regla de ILM que caduque o elimine datos del nivel de nube FabricPool. Establece el periodo de retención en **para siempre** para garantizar que los objetos de FabricPool no sean eliminados por StorageGRID ILM.

Pasos

1. Si lo deseas, actualiza el **nombre de la política** generado por el sistema. De forma predeterminada, el sistema añade "+ FabricPool" al nombre de tu política, ya sea activa o inactiva, pero puedes indicar el nombre que prefieras.
2. Revisa la lista de reglas en la política inactiva.
 - Si tu grid no tiene una política de ILM inactiva, el asistente crea una política inactiva clonando tu política activa y añadiendo la nueva regla al principio.
 - Si tu grid ya tiene una política de ILM inactiva y esa política usa las mismas reglas y el mismo orden que la política de ILM activa, el asistente añade la nueva regla al principio de la política inactiva.
 - Si tu política inactiva contiene reglas diferentes o un orden distinto al de la política activa, el asistente crea una nueva política inactiva clonando tu política activa y añadiendo la nueva regla al principio.
3. Revisa el orden de las reglas en la nueva política inactiva.

Porque la regla FabricPool es la primera, cualquier objeto en el bucket FabricPool se coloca antes de que se evalúen las demás reglas de la política. Los objetos en cualquier otro bucket se colocan según las reglas posteriores de la política.

4. Consulta el diagrama de retención para saber cómo se conservarán los distintos objetos.
 - a. Selecciona **Expandir todo** para ver un diagrama de retención de cada regla de la política inactiva.
 - b. Selecciona **Período de tiempo** y **Grupo de almacenamiento** para consultar el diagrama de retención. Asegúrate de que todas las reglas que se aplican al bucket o al tenant de FabricPool retengan los objetos **para siempre**.
5. Cuando hayas revisado la política inactiva, selecciona **Activar y continuar** para activar la política y pasar al paso de clasificación del tráfico.



Los errores en una política de ILM pueden provocar una pérdida irreparable de datos. Revisa la política detenidamente antes de activarla.

Paso 8 de 9: crear una política de clasificación del tráfico

Como opción, el asistente de configuración de FabricPool puede crear una política de clasificación de tráfico que puedes utilizar para supervisar la carga de trabajo de FabricPool. La política creada por el sistema utiliza una regla de coincidencia para identificar todo el tráfico de red relacionado con el bucket que creaste. Esta política solo supervisa el tráfico; no limita el tráfico de FabricPool ni de ningún otro cliente.

Para obtener más información sobre este paso, consulta ["Crear una política de clasificación del tráfico para FabricPool"](#).

Pasos

1. Revisa la política.

2. Si quieres crear esta política de clasificación del tráfico, selecciona **Crear y continuar**.

En cuanto FabricPool comience a transferir datos a StorageGRID, puedes ir a la página de Políticas de clasificación de tráfico para ver las métricas de tráfico de red de esta política. Más adelante, también puedes añadir reglas para limitar otras cargas de trabajo y asegurarte de que la carga de trabajo de FabricPool tenga la mayor parte del ancho de banda.

3. De lo contrario, selecciona **Omitir este paso**.

Paso 9 de 9: revisar resumen

El resumen ofrece información detallada sobre los elementos que has configurado, incluyendo el nombre del load balancer, tenant y bucket, la política de clasificación del tráfico y la política de ILM activa,

Pasos

1. Revisa el resumen.
2. Selecciona **Finalizar**.

Próximos pasos

Después de completar el asistente de FabricPool, realiza estos pasos adicionales.

Pasos

1. Accede a ["Configura ONTAP System Manager"](#) para introducir los valores guardados y completar la parte de ONTAP de la conexión. Debes añadir StorageGRID como nivel de nube, vincular el nivel de nube a un nivel local para crear un FabricPool y configurar las políticas de jerarquización de volúmenes.
2. Accede a ["Configura el servidor DNS"](#) y asegúrate de que el DNS incluya un registro que asocie el nombre del servidor StorageGRID (nombre de dominio completo) a cada dirección IP de StorageGRID que vayas a utilizar.
3. Ve 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.

Configura StorageGRID manualmente

Crea un grupo de alta disponibilidad (HA) para FabricPool en StorageGRID

Al configurar StorageGRID para usarlo con FabricPool, opcionalmente puedes crear uno o varios grupos de alta disponibilidad (HA). Un grupo de HA es un conjunto de nodos que contienen, cada uno, el servicio de equilibrador de carga de StorageGRID. Un grupo de HA puede contener nodos de gateway, nodos de administración o ambos.

Puedes usar un grupo de HA para ayudar a mantener disponibles las conexiones de datos de FabricPool. Un grupo de HA utiliza direcciones IP virtuales (VIP) para proporcionar un acceso de alta disponibilidad al servicio de equilibrador de carga. Si la interfaz activa del grupo de HA falla, una interfaz de respaldo puede gestionar la carga de trabajo con un impacto mínimo en las operaciones de FabricPool.

Para obtener más información sobre esta tarea, consulta ["Gestiona grupos de alta disponibilidad"](#). Para utilizar el asistente de configuración de FabricPool y completar esta tarea, accede a ["Accede y completa el asistente de configuración de FabricPool"](#).

Antes de empezar

- Has revisado la ["buenas prácticas para los grupos de alta disponibilidad"](#).
- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).
- Si tienes previsto usar una VLAN, ya creaste la interfaz de VLAN. Consulta ["Configurar interfaces VLAN"](#).

Pasos

1. Selecciona **Configuración > Red > Grupos de alta disponibilidad**.
2. Selecciona **Crear**.
3. En el paso **Introducir datos**, rellena los siguientes campos.

Campo	Descripción
Nombre del grupo HA	Un nombre para mostrar único para este grupo de alta disponibilidad.
Descripción (opcional)	La descripción de este grupo de HA.

4. En el paso **Add interfaces**, selecciona las interfaces de nodo que quieres usar en este grupo de alta disponibilidad.

Utiliza los encabezados de las columnas para ordenar las filas o introduce un término de búsqueda para encontrar interfaces más rápido.

Puedes seleccionar uno o varios nodos, pero solo puedes seleccionar una interfaz por cada nodo.

5. Para el paso **Priorizar interfaces**, determina la interfaz principal y cualquier interfaz de respaldo para este grupo de alta disponibilidad.

Arrastra las filas para cambiar los valores de la columna **Orden de prioridad**.

La primera interfaz de la lista es la interfaz principal. La interfaz principal es la interfaz activa salvo que se produzca un fallo.

Si el grupo de alta disponibilidad (HA) incluye más de una interfaz y la interfaz activa falla, las direcciones IP virtuales (VIP) se transfieren a la primera interfaz de respaldo según el orden de prioridad. Si esa interfaz falla, las direcciones VIP se transfieren a la siguiente interfaz de respaldo, y así sucesivamente. Cuando se resuelven los fallos, las direcciones VIP vuelven a la interfaz disponible con mayor prioridad.

6. En el paso **Introducir direcciones IP**, completa los siguientes campos.

Campo	Descripción
CIDR de la 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 activado. 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, introduce la dirección IP de la pasarela local VIP de StorageGRID. La dirección IP de la pasarela local debe estar dentro de la subred VIP.
Dirección IP virtual	Introduce al menos una y no más de diez direcciones VIP para la interfaz activa del grupo de alta disponibilidad. Todas las direcciones VIP deben estar dentro de la subred VIP. Al menos una dirección debe ser IPv4. Opcionalmente, puedes especificar direcciones IPv4 e IPv6 adicionales.

7. Selecciona **Crear grupo de alta disponibilidad** y luego selecciona **Finalizar**.

Creas un punto final de equilibrio de carga para FabricPool en StorageGRID

StorageGRID utiliza un equilibrador de carga para gestionar la carga de trabajo de las aplicaciones cliente, como FabricPool. El equilibrio de carga maximiza la velocidad y la capacidad de conexión entre varios nodos de almacenamiento.

Al configurar StorageGRID para su uso con FabricPool, debes configurar un punto final del equilibrador de carga y cargar o generar un certificado del 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 y completar esta tarea, ve a ["Accede y completa el asistente de configuración de FabricPool"](#).

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).
- Has revisado la ["consideraciones para el equilibrio de carga"](#) general, así como la ["buenas prácticas para el equilibrio de carga en FabricPool"](#).

Pasos

1. Selecciona **Configuración > Red > Puntos finales del equilibrador de carga**.
2. Selecciona **Crear**.
3. En el paso **Introducir los datos del punto final**, rellena los siguientes campos.

Campo	Descripción
Nombre	Un nombre descriptivo para el endpoint.

Campo	Descripción
Puerto	El puerto de StorageGRID que deseas utilizar para el equilibrio de carga. Este campo tiene por defecto el valor 10433 para el primer endpoint que crees, pero puedes introducir cualquier puerto externo que no esté en uso. Si introduces 80 o 443, el endpoint solo se configura en los Gateway Nodes. Estos puertos están reservados en los Admin Nodes. Nota: No se permiten los puertos utilizados por otros servicios de la grid. Consulta el "Referencia de puertos de red". Deberás facilitar este número a ONTAP cuando conectes StorageGRID como un nivel de nube FabricPool.
Tipo de cliente	Selecciona S3 .
Protocolo de red	Selecciona HTTPS. Nota: La comunicación con StorageGRID sin cifrado TLS es compatible, pero no se recomienda.

4. En el paso **Seleccionar modo de enlace**, especifica el modo de enlace. El modo de enlace controla cómo se accede al endpoint utilizando cualquier dirección IP o utilizando direcciones IP e interfaces de red específicas.

Modo	Descripción
Global (predeterminado)	Los clientes pueden acceder al punto final usando la dirección IP de cualquier Gateway Node o Admin Node, la dirección IP virtual (VIP) de cualquier grupo HA en cualquier red, o el FQDN correspondiente. Utiliza la configuración Global (por defecto) a menos que necesites restringir la accesibilidad de este endpoint.
Direcciones IP virtuales de los grupos de alta disponibilidad	Los clientes deben utilizar una dirección IP virtual (o el nombre de dominio completo correspondiente) de un grupo de alta disponibilidad para acceder a este endpoint. Todos los puntos finales con este modo de enlace pueden utilizar el mismo número de puerto, siempre y cuando los grupos de alta disponibilidad que selecciones para los puntos finales no se solapen.
Interfaces de nodo	Los clientes deben utilizar las direcciones IP (o los FQDN correspondientes) de las interfaces de los nodos seleccionados para acceder a este endpoint.
Tipo de nodo	En función del tipo de nodo que selecciones, los clientes deben usar la dirección IP (o el FQDN correspondiente) de cualquier Admin Node o la dirección IP (o el FQDN correspondiente) de cualquier Gateway Node para acceder a este endpoint.

5. Para el paso **Acceso del inquilino**, selecciona una de las siguientes opciones:

Campo	Descripción
Permitir a todos los inquilinos (por defecto)	Todas las cuentas de inquilinos pueden usar este endpoint para acceder a sus buckets. Permitir a todos los inquilinos suele ser casi siempre la opción adecuada para el endpoint del balanceador de carga usado para FabricPool. Debes seleccionar esta opción si aún no has creado ninguna cuenta de inquilino.
Permitir inquilinos seleccionados	Solo las cuentas de inquilino seleccionadas pueden usar este endpoint para acceder a sus buckets.
Bloquear inquilinos seleccionados	Las cuentas de inquilino seleccionadas no pueden utilizar este endpoint para acceder a sus buckets. El resto de inquilinos sí pueden utilizar este endpoint.

6. En el paso **Adjuntar certificado**, selecciona una de las siguientes opciones:

Campo	Descripción
Subir certificado (recomendado)	Utiliza esta opción para cargar un certificado de servidor firmado por una CA, la clave privada del certificado y, opcionalmente, el paquete de CA.
Generar certificado	Utiliza esta opción para generar un certificado autofirmado. Consulta "Configura los puntos de conexión del equilibrador de carga" para ver los detalles de qué debes introducir.
Usa el certificado S3 de StorageGRID	Esta opción solo está disponible si ya has subido o generado una versión personalizada del certificado global de StorageGRID. Consulta "Configura los certificados de la API de S3" para obtener más información.

7. Selecciona **Crear**.



Los cambios en el certificado de un endpoint pueden tardar hasta 15 minutos en aplicarse a todos los nodos.

Crea una cuenta de arrendatario para FabricPool en StorageGRID

Debes crear una cuenta de inquilino en Grid Manager para el uso de FabricPool.

Las cuentas de inquilino permiten a las aplicaciones de los clientes almacenar y recuperar objetos en StorageGRID. Cada cuenta de inquilino tiene su propio ID de cuenta, grupos y usuarios autorizados, buckets y objetos.

Para obtener más información sobre esta tarea, consulta ["Crear cuenta de inquilino"](#). Para utilizar el asistente de configuración de FabricPool y completar esta tarea, accede a ["Accede y completa el asistente de configuración de FabricPool"](#).

Antes de empezar

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

Pasos

1. Selecciona **Tenants**.
2. Selecciona **Crear**.
3. En los pasos «Introducir datos», introduce la siguiente información.

Campo	Descripción
Nombre	Un nombre para la cuenta de inquilino. Los nombres de los inquilinos no tienen que ser únicos. Cuando se crea la cuenta de inquilino, recibe un identificador de cuenta numérico único.
Descripción (opcional)	Una descripción que ayude a identificar al inquilino.
Tipo de cliente	Debe ser S3 para FabricPool.
Cuota de almacenamiento (opcional)	Deja este campo en blanco para FabricPool.

4. Para el paso: «Seleccionar permisos»

- a. No selecciones **Permitir servicios de plataforma**.

Los inquilinos de FabricPool normalmente no necesitan usar servicios de la plataforma, como la replicación de CloudMirror.

- b. Si lo deseas, selecciona **Usar fuente de identidad propia**.

- c. No marques la opción **Allow S3 Select**.

FabricPool los inquilinos no suelen necesitar usar S3 Select.

- d. Si lo deseas, selecciona **Usar conexión de federación de grid** para permitir que el inquilino use un ["conexión de federación de grid"](#) para la clonación de cuentas y la replicación entre grids. Luego, selecciona la conexión de federación de grid que quieras usar.

5. En el paso «Definir acceso a raíz», especifica qué usuario tendrá el permiso de acceso a raíz inicial para la cuenta de inquilino, en función de si tu sistema StorageGRID utiliza ["federación de identidades"](#), ["inicio de sesión único \(SSO\)"](#) o ambos.

Opción	Haz esto
Si la federación de identidades no está habilitada	Indica la contraseña que se usará al iniciar sesión en el tenant como usuario raíz local.

Opción	Haz esto
Si la federación de identidades está activada	a. Selecciona un grupo federado ya existente para disponer de permiso de acceso a raíz para el inquilino. b. Si lo deseas, indica la contraseña que se usará al iniciar sesión en el tenant como usuario raíz local.
Si están habilitados tanto la federación de identidades como el inicio de sesión único (SSO)	Selecciona un grupo federado existente para tener permiso de acceso a raíz para el inquilino. Ningún usuario local puede iniciar sesión.

6. Selecciona **Create tenant**.

Crea un bucket S3 y obtén claves de acceso para FabricPool en StorageGRID

Antes de usar StorageGRID con una carga de trabajo de FabricPool, debes crear un bucket S3 para tus datos de FabricPool. También necesitas obtener una clave de acceso y una clave secreta de acceso para la cuenta de tenant que vas a usar para FabricPool.

Para obtener más información sobre esta tarea, consulta ["Crear un bucket de S3"](#) y ["Crea tus propias claves de acceso a S3"](#). Para utilizar el asistente de configuración de FabricPool para completar esta tarea, ve a ["Accede y completa el asistente de configuración de FabricPool"](#).

Antes de empezar

- Has creado una cuenta de inquilino para usar con FabricPool.
- Tienes acceso a raíz a la cuenta del inquilino.

Pasos

1. Inicia sesión en Tenant Manager.

Puedes hacer cualquiera de las siguientes cosas:

- En la página «Cuentas de inquilinos» del Grid Manager, selecciona el enlace **Sign in** correspondiente al inquilino e introduce tus credenciales.
- Introduce la URL de la cuenta de inquilino en un navegador web e introduce tus credenciales.

2. Crea un bucket de S3 para los datos de FabricPool.

Debes crear un bucket único para cada clúster ONTAP que tengas previsto utilizar.

- Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.
- Selecciona **Create bucket**.
- Introduce el nombre del bucket de StorageGRID que deseas utilizar con FabricPool. Por ejemplo, `fabricpool-bucket`.



No puedes cambiar el nombre del bucket después de crearlo.

- Selecciona la región para este bucket.

De forma predeterminada, todos los buckets se crean en la `us-east-1` región. Si la región

predeterminada se ha configurado en una región distinta de `us-east-1`, esta otra región aparecerá seleccionada inicialmente en el menú desplegable.

- e. Selecciona **Continuar**.
- f. Selecciona **Create bucket**.



No selecciones **Habilitar control de versiones de objetos** para el depósito FabricPool. Del mismo modo, no modifiques un depósito FabricPool para que utilice **Disponible** o una consistencia no predeterminada. La consistencia recomendada para los depósitos FabricPool es **Lectura tras nueva escritura**, que es la consistencia predeterminada para un depósito nuevo.

3. Crea una clave de acceso y una clave secreta de acceso.

- a. Selecciona **STORAGE (S3) > Mis claves de acceso**.
- b. Selecciona **Crear clave**.
- c. Selecciona **Crear clave de acceso**.
- d. Copia el ID de la clave de acceso y la clave de acceso secreta en un lugar seguro, o selecciona **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.

Deberás introducir estos valores en ONTAP cuando configures StorageGRID como un nivel de nube FabricPool.



Si en el futuro generas una nueva clave de acceso y una nueva clave secreta de acceso en StorageGRID, introduce las nuevas claves en ONTAP antes de eliminar los valores antiguos de StorageGRID. De lo contrario, ONTAP podría perder temporalmente el acceso a StorageGRID.

Configura ILM de StorageGRID para datos de FabricPool

Puedes utilizar esta sencilla política de ejemplo como punto de partida para tus propias reglas y políticas de ILM.

En este ejemplo se da por supuesto que estás diseñando las reglas de ILM y una política de ILM para un sistema StorageGRID que cuenta con cuatro nodos de almacenamiento en un único centro de datos en Denver, Colorado. Los datos de FabricPool en este ejemplo usan un bucket llamado `fabricpool-bucket`.



Las siguientes reglas y políticas de ILM son solo ejemplos. Existen muchas formas de configurar las reglas de ILM. Antes de activar una nueva política, simúlala para confirmar que funcionará según lo previsto y protegerá el contenido frente a posibles pérdidas. Para obtener más información, consulta ["Gestiona objetos con ILM"](#).



Para evitar la pérdida de datos, no utilices una regla de ILM que caduque o elimine datos del nivel de nube FabricPool. Establece el periodo de retención en **para siempre** para garantizar que los objetos de FabricPool no sean eliminados por StorageGRID ILM.

Antes de empezar

- Has revisado la ["prácticas recomendadas para usar ILM con datos de FabricPool"](#).

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de acceso a ILM o root".
- Si has actualizado a StorageGRID 12.0 desde una versión anterior a la 11.7, ya habrás configurado el grupo de almacenamiento que vas a utilizar. En general, deberías crear un grupo de almacenamiento para cada sitio de StorageGRID que vayas a usar para almacenar datos. (A partir de la versión 11.7, los grupos de almacenamiento se crean automáticamente para cada sitio.)



Este requisito previo no se aplica si inicialmente instalaste StorageGRID 11.7 o 11.8. Cuando instalas inicialmente cualquiera de estas versiones, los grupos de almacenamiento se crean automáticamente para cada sitio.

Pasos

1. Crea una regla de 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 bucket	<code>fabricpool-bucket</code> También puedes filtrar por la cuenta de inquilino FabricPool.
Filtros avanzados	Tamaño de objeto superior a 0,2 MB. Nota: FabricPool solo graba objetos de 4 MB, pero debes añadir un filtro de tamaño de objeto porque esta regla utiliza código de borrado.
Hora de referencia	Tiempo de ingesta
Periodo y ubicaciones	Desde el día 0 se conserva para siempre Almacena objetos mediante código de borrado usando el esquema EC 2+1 en Denver y conserva esos objetos en StorageGRID para siempre. Para evitar la pérdida de datos, no utilices una regla de ILM que caduque o elimine datos del nivel de nube FabricPool.
Comportamiento de ingesta	Equilibrado

2. Crea una regla ILM predeterminada que genere dos copias replicadas de cualquier objeto que no cumpla con los criterios de la primera regla. No selecciones ningún filtro básico (cuenta de inquilino o nombre de bucket) ni ningún filtro avanzado.

Definición de regla	Valor de ejemplo
Nombre de la regla	Dos copias replicadas
Nombre del bucket	<i>none</i>
Filtros avanzados	<i>none</i>
Hora de referencia	Tiempo de ingesta
Periodo y ubicaciones	Desde el día 0 se conserva para siempre Almacena los objetos replicando 2 copias en Denver.
Comportamiento de ingesta	Equilibrado

3. Crea una política de ILM y selecciona las dos reglas. Porque la regla de replicación no utiliza ningún filtro, puede ser la regla predeterminada (la última) de la política.
4. Ingiera objetos de prueba en el grid.
5. Simula la política con los objetos de prueba para comprobar su comportamiento.
6. Activa la política.

Cuando se activa esta política, StorageGRID coloca los datos de los objetos de la siguiente manera:

- Los datos nivelados desde FabricPool en `fabricpool-bucket` se codificarán por borrado usando el esquema de codificación de borrado 2+1. Dos fragmentos de datos y un fragmento de paridad se colocarán en tres nodos de almacenamiento diferentes.
- Se replicarán todos los objetos de todos los demás buckets. Se crearán dos copias y se colocarán en dos nodos de almacenamiento diferentes.
- Las copias se conservarán en StorageGRID para siempre. StorageGRID ILM no eliminará estos objetos.

Crea una política de clasificación de tráfico para FabricPool en StorageGRID

Si lo deseas, puedes diseñar una política de clasificación del tráfico de StorageGRID para optimizar la calidad del servicio de la carga de trabajo de FabricPool.

Para obtener más información sobre esta tarea, consulta ["Gestiona las políticas de clasificación del tráfico"](#). Para utilizar el asistente de configuración de FabricPool y completar esta tarea, accede a ["Accede y completa el asistente de configuración de FabricPool"](#).

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).

Acerca de esta tarea

Las mejores prácticas para crear una política de clasificación del tráfico para FabricPool dependen de la carga de trabajo, como se indica a continuación:

- Si planeas clasificar por niveles los datos de la carga de trabajo principal de FabricPool en StorageGRID, debes asegurarte de que la carga de trabajo de FabricPool tenga la mayor parte del ancho de banda. Puedes crear una política de clasificación de tráfico para limitar todas las demás cargas de trabajo.



En general, es más importante dar prioridad a las operaciones de lectura de FabricPool que a las de escritura.

Por ejemplo, si otros clientes de S3 utilizan este sistema StorageGRID, debes crear una política de clasificación de tráfico. Puedes limitar el tráfico de red para los demás buckets, inquilinos, subredes IP o puntos de conexión del equilibrador de carga.

- En general, no deberías imponer límites de calidad de servicio a ninguna carga de trabajo de FabricPool; solo deberías limitar las demás cargas de trabajo.
- Los límites establecidos para otras cargas de trabajo deben tener en cuenta el comportamiento de dichas cargas de trabajo. Los límites impuestos también variarán en función del tamaño y las capacidades de tu grid y del nivel de utilización previsto.

Pasos

1. Selecciona **Configuración > Red > Clasificación del tráfico**.
2. Selecciona **Crear**.
3. Introduce un nombre y una descripción (opcional) para la política y selecciona **Continuar**.
4. En el paso «Add matching rules», añade al menos una regla.
 - a. Selecciona **Add rule**
 - b. En Tipo, selecciona **Punto final del equilibrador de carga** y selecciona el punto final del equilibrador de carga que creaste para FabricPool.

También puedes seleccionar la cuenta de inquilino o el bucket de FabricPool.

- c. Si deseas que esta política de tráfico limite el tráfico para los demás puntos finales, selecciona **Coincidencia inversa**.
5. Si lo deseas, añade uno o varios límites para controlar el tráfico de red al que coincide la regla.



StorageGRID recopila métricas incluso si no agregas ningún límite, así puedes entender las tendencias del tráfico.

- a. Selecciona **Add a limit**.
 - b. Selecciona el tipo de tráfico que deseas limitar y el límite que quieres aplicar.
6. Selecciona **Continuar**.
 7. Lee y revisa la política de clasificación de tráfico. Usa el botón **Anterior** para volver y realizar cambios según sea necesario. Cuando estés satisfecho con la política, selecciona **Guardar y continuar**.

Una vez que hayas terminado

"[Ver métricas de tráfico de red](#)" para comprobar que las políticas hacen cumplir los límites de tráfico que esperas.

Configura ONTAP System Manager para añadir StorageGRID como un cloud tier FabricPool

Una vez que hayas obtenido la información necesaria sobre StorageGRID, puedes ir a ONTAP para añadir StorageGRID como nivel de nube.

Antes de empezar

- Si completaste el asistente de configuración de FabricPool, tienes el `ONTAP_FabricPool_settings_bucketname.txt` archivo que descargaste.
- Si has configurado StorageGRID manualmente, dispones del nombre de dominio completo (FQDN) que estás utilizando para StorageGRID o de la dirección IP virtual (VIP) del grupo HA de StorageGRID, el número de puerto del endpoint del equilibrador de carga, el certificado del equilibrador de carga, el ID de clave de acceso y la clave secreta para el usuario raíz de la cuenta de tenant, y el nombre del bucket que ONTAP usará en ese tenant.

Accede a ONTAP System Manager

Estas instrucciones describen cómo utilizar ONTAP System Manager para añadir StorageGRID como nivel de nube. Puedes completar la misma configuración usando la CLI de ONTAP. Para instrucciones, ve a ["Documentación de ONTAP para FabricPool"](#).

Pasos

1. Accede a System Manager para el clúster ONTAP al que quieres hacer tiering en StorageGRID.
2. Inicia sesión como administrador del clúster.
3. Ve a **ALMACENAMIENTO > Niveles > Add Cloud Tier**.
4. Selecciona **StorageGRID** de la lista de proveedores de almacén de objetos.

Introduce los valores de StorageGRID

Consulta ["Documentación de ONTAP para FabricPool"](#) para más información.

Pasos

1. Rellena el formulario Add Cloud Tier utilizando el archivo `ONTAP_FabricPool_settings_bucketname.txt` o los valores que hayas obtenido manualmente.

Campo	Descripción
Nombre	Introduce un nombre único para este nivel de la nube. Puedes aceptar el valor predeterminado.
Estilo de URL	Si "Nombres de dominio de los endpoints S3 configurados" seleccionas URL de estilo alojamiento virtual. URL de tipo ruta es la opción predeterminada para ONTAP, pero se recomienda utilizar solicitudes de tipo virtual hosted para StorageGRID. Debes utilizar URL de tipo ruta si introduces una dirección IP en lugar de un nombre de dominio en el campo Server name (FQDN).

Campo	Descripción
Nombre del servidor (FQDN)	Introduce el nombre de dominio completo (FQDN) que estás utilizando para StorageGRID o la dirección IP virtual (VIP) del grupo de alta disponibilidad (HA) de StorageGRID. Por ejemplo, <code>s3.storagegrid.company.com</code>. Ten en cuenta lo siguiente: • La dirección IP o el nombre de dominio que especifiques aquí debe coincidir con el certificado que subiste o generaste para el endpoint del balanceador de carga de StorageGRID. • Si facilitas un nombre de dominio, el registro DNS debe estar asociado a cada dirección IP que vayas a utilizar para conectarte a StorageGRID. Consulta "Configura el servidor DNS".
SSL	Activado (por defecto).
Certificado del almacén de objetos	Pega el certificado PEM que estás utilizando para el punto final del equilibrador de carga de StorageGRID, incluyendo: <pre>-----BEGIN CERTIFICATE----- y -----END CERTIFICATE-----.</pre> Nota: Si el certificado de StorageGRID fue emitido por una CA intermedia, debes proporcionar el certificado de la CA intermedia. Si el certificado de StorageGRID fue emitido directamente por la CA raíz, debes proporcionar el certificado de la CA raíz.
Puerto	Introduce el puerto que utiliza el endpoint del equilibrador de carga de StorageGRID. ONTAP utilizará este puerto cuando se conecte a StorageGRID. Por ejemplo, 10433.
Clave de acceso y clave secreta	Introduce el ID de la clave de acceso y la clave secreta de acceso del usuario raíz de la cuenta de inquilino de StorageGRID. Consejo: si generas una nueva clave de acceso y una clave de acceso secreta en StorageGRID en el futuro, introduce las nuevas claves en ONTAP antes de eliminar los valores antiguos de StorageGRID. De lo contrario, es posible que ONTAP pierda temporalmente su acceso a StorageGRID.
Nombre del contenedor	Introduce el nombre del bucket de StorageGRID que has creado para utilizarlo con este nivel de ONTAP.

2. Completa la configuración final de FabricPool en ONTAP.

- Asigna uno o varios agregados al nivel de la nube.
- Opcionalmente, crea una política de organización por niveles de volúmenes.

Configura las entradas del servidor DNS para StorageGRID con FabricPool

Después de configurar los grupos de alta disponibilidad, los puntos de conexión del equilibrador de carga y los nombres de dominio de los puntos de conexión de S3, debes

asegurarte de que el DNS incluya las entradas necesarias para StorageGRID. Debes incluir una entrada de DNS para cada nombre en el certificado de seguridad y para cada dirección IP que puedas usar.

Consulta ["Aspectos a tener en cuenta para el equilibrio de carga"](#).

Entradas DNS para el nombre del servidor StorageGRID

Añade entradas DNS para asociar el nombre del servidor StorageGRID (nombre de dominio completo) a cada dirección IP de StorageGRID que vayas a utilizar. Las direcciones IP que introduzcas en el DNS dependen de si estás utilizando un grupo HA de nodos con equilibrio de carga:

- Si has configurado un grupo de alta disponibilidad (HA), ONTAP se conectará a las direcciones IP virtuales de ese grupo de alta disponibilidad.
- Si no estás usando un grupo de alta disponibilidad (HA), ONTAP puede conectarse al servicio StorageGRID Load Balancer usando la dirección IP de cualquier Gateway Node o Admin Node.
- 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 de rotación cuando se establecen las conexiones.

Entradas DNS para solicitudes de tipo alojamiento virtual

Si has definido ["Nombres de dominio de los endpoints S3"](#) y vas a utilizar solicitudes de tipo virtual hosted-style, añade entradas DNS para todos los nombres de dominio de los endpoints S3 necesarios, incluidos los nombres con comodines.

Mejores prácticas de StorageGRID para FabricPool

Prácticas recomendadas para grupos de alta disponibilidad (HA) de StorageGRID con FabricPool

Antes de asociar StorageGRID como un nivel de cloud de FabricPool, infórmate sobre los grupos de alta disponibilidad (HA) de StorageGRID y revisa las mejores prácticas para usar grupos de HA con FabricPool.

¿Qué es un grupo HA?

Un grupo de alta disponibilidad (HA) es un conjunto de interfaces procedentes 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 de los clientes. Si la interfaz activa del grupo HA falla, una interfaz de respaldo puede gestionar la carga de trabajo con poco impacto en las operaciones de FabricPool.

Cada grupo de HA proporciona acceso de alta disponibilidad a los servicios compartidos en los nodos asociados. Por ejemplo, un grupo de HA que consta de interfaces solo en Gateway Nodes o tanto en Admin Nodes como en Gateway Nodes proporciona acceso de alta disponibilidad al servicio Load Balancer compartido.

Para obtener más información sobre los grupos de alta disponibilidad, consulta ["Administra grupos de alta disponibilidad \(HA\)"](#).

Uso de grupos HA

Las prácticas recomendadas para crear un grupo de alta disponibilidad (HA) de StorageGRID para FabricPool

dependen de la carga de trabajo.

- Si planeas usar FabricPool con datos de cargas de trabajo principales, debes crear un grupo de alta disponibilidad que incluya al menos dos nodos con equilibrio de carga para evitar la interrupción en la recuperación de datos.
- Si planeas usar la política de organización en niveles de volúmenes de solo instantáneas de FabricPool o niveles de rendimiento locales no primarios (por ejemplo, ubicaciones de recuperación ante desastres o destinos de NetApp SnapMirror®), puedes configurar un grupo de HA con un solo nodo.

Estas instrucciones describen cómo configurar un grupo de HA para un esquema de HA activo-backup (un nodo está activo y el otro de backup). Sin embargo, es posible que prefieras utilizar DNS Round Robin o un esquema de HA activo-activo. Para conocer las ventajas de estas otras configuraciones de HA, consulta ["Opciones de configuración para los grupos de alta disponibilidad"](#).

Mejores prácticas para el equilibrio de carga de StorageGRID con FabricPool

Antes de asociar StorageGRID como un nivel de nube de FabricPool, revisa las mejores prácticas para usar balanceadores de carga con FabricPool.

Para obtener información general sobre el balanceador de carga de StorageGRID y el certificado del balanceador de carga, consulta ["Aspectos a tener en cuenta para el equilibrio de carga"](#).

Prácticas recomendadas para el acceso de los inquilinos al punto de conexión del equilibrador de carga utilizado para FabricPool

Puedes controlar qué inquilinos pueden usar un extremo de equilibrador de carga específico para acceder a sus buckets. Puedes permitir todos los inquilinos, permitir algunos inquilinos o bloquear algunos inquilinos. Al crear un extremo de equilibrador de carga para usarlo con FabricPool, selecciona **Permitir todos los inquilinos**. ONTAP cifra los datos que se guardan en los buckets de StorageGRID, por lo que esta capa de seguridad adicional apenas aportaría más seguridad.

Buenas prácticas para el certificado de seguridad

Cuando creas un punto final del equilibrador de carga de StorageGRID para uso con FabricPool, proporcionas el certificado de seguridad que permitirá que ONTAP se autentique con StorageGRID.

En la mayoría de los casos, la conexión entre ONTAP y StorageGRID debe utilizar cifrado TLS (Transport Layer Security). Usar FabricPool sin cifrado TLS es compatible, pero no se recomienda. Cuando selecciones el protocolo de red para el endpoint del equilibrador de carga de StorageGRID, selecciona **HTTPS**. Luego proporciona el certificado de seguridad que permitirá que ONTAP se autentique con StorageGRID.

Para obtener más información sobre el certificado del servidor de un endpoint de equilibrio de carga:

- ["Gestiona certificados de seguridad"](#)
- ["Aspectos a tener en cuenta para el equilibrio de carga"](#)
- ["Directrices de refuerzo de la seguridad para certificados de servidor"](#)

Agregar certificado a ONTAP

Cuando añades StorageGRID como nivel de nube de FabricPool, debes instalar el mismo certificado en el clúster ONTAP, incluidos el certificado raíz y cualquier certificado de autoridad de certificación (CA) subordinada.

Gestiona la caducidad de los certificados



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 organizados en niveles en StorageGRID.

Para evitar problemas relacionados con la caducidad de los certificados, sigue estas recomendaciones:

- Presta especial atención a cualquier alerta que avise de la proximidad de la fecha de caducidad de un certificado, como las alertas **Caducidad del certificado del punto final del equilibrador de carga** y **Caducidad del certificado global del servidor para la API de S3**.
- Mantén siempre sincronizadas las versiones del certificado de StorageGRID y ONTAP. Si sustituyes o renuevas el certificado utilizado para un endpoint del equilibrador de carga, debes sustituir o renovar el certificado equivalente que utiliza ONTAP para el nivel de cloud.
- Utiliza un certificado de CA firmado públicamente. Si utilizas un certificado firmado por una CA, puedes usar la Grid Management API para automatizar la rotación de certificados. Esto te permite reemplazar los certificados que están a punto de caducar sin interrupciones.
- Si has generado un certificado de StorageGRID autofirmado y ese certificado está a punto de caducar, debes reemplazar manualmente el certificado tanto en StorageGRID como en ONTAP antes de que el certificado existente caduque. Si un certificado autofirmado ya ha caducado, desactiva la validación de certificados en ONTAP para evitar la pérdida de acceso.

Consulta ["Base de conocimientos de NetApp: cómo configurar un nuevo certificado de servidor autofirmado de StorageGRID en una implementación de FabricPool de ONTAP existente"](#) para obtener instrucciones.

Prácticas recomendadas para usar StorageGRID ILM con datos de FabricPool

Si usas FabricPool para almacenar datos en niveles en StorageGRID, debes comprender los requisitos para utilizar la gestión del ciclo de vida de la información (ILM) de StorageGRID con los datos de FabricPool.



FabricPool no tiene conocimiento de las reglas ni de las políticas de ILM de StorageGRID. Si la política de ILM de StorageGRID está mal configurada, se puede producir una pérdida de datos. Para obtener información detallada, consulta ["Utiliza las reglas de ILM para gestionar objetos"](#) y ["Crear políticas de ILM"](#).

Pautas para usar ILM con FabricPool

Cuando usas el asistente de configuración de FabricPool, el asistente crea automáticamente una nueva regla de ILM para cada bucket de S3 que creas y añade esa regla a una política inactiva. Se te pedirá que actives la política. La regla creada automáticamente sigue las prácticas recomendadas: utiliza codificación de borrado 2+1 en un solo sitio.

Si estás configurando StorageGRID de forma manual en lugar de usar el asistente de configuración de FabricPool, revisa estas directrices para asegurarte de que tus reglas de ILM y tu política de ILM sean adecuadas para los datos de FabricPool y tus requisitos de negocio. Es posible que necesites crear nuevas reglas y actualizar tus políticas de ILM activas para cumplir con estas directrices.

- Puedes utilizar cualquier combinación de reglas de replicación y de código de borrado para proteger los datos del nivel de la nube.

La práctica recomendada es utilizar la 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 una capacidad de almacenamiento significativamente menor 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 necesitas añadir Storage Nodes durante la expansión del grid. Para obtener más detalles, consulta ["Agrega capacidad de almacenamiento para objetos con código de borrado"](#).

- Cada regla que se aplique a los datos de FabricPool debe utilizar el código de borrado o crear al menos dos copias replicadas.



Una regla de ILM que crea solo una copia replicada para cualquier periodo 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 grave. También pierdes temporalmente el acceso al objeto durante procedimientos de mantenimiento como las actualizaciones.

- Si necesitas ["elimina los datos de FabricPool de StorageGRID"](#), utiliza ONTAP para recuperar todos los datos del volumen FabricPool y ascenderlo al nivel de rendimiento.



Para evitar la pérdida de datos, no utilices una regla de ILM que haga caducar o elimine los datos del nivel de nube de FabricPool. Establece el periodo de retención de cada regla de ILM en **forever** para asegurarte de que el ILM de StorageGRID no elimine los objetos de FabricPool.

- No crees reglas que trasladen los datos del nivel cloud de FabricPool fuera del bucket a otra ubicación. No puedes usar un Cloud Storage Pool para mover datos de FabricPool a otro almacén de objetos.



No se admite el uso de Cloud Storage Pools con FabricPool debido a la latencia adicional para recuperar un objeto del destino de Cloud Storage Pool.

- A partir de ONTAP 9.8, puedes crear opcionalmente etiquetas de objetos para ayudar a clasificar y ordenar los datos organizados por niveles y así facilitar su gestión. Por ejemplo, puedes asignar etiquetas solo a los volúmenes de FabricPool conectados a StorageGRID. Luego, cuando creas reglas de ILM en StorageGRID, puedes usar el filtro avanzado de Etiqueta de objeto para seleccionar y ubicar estos datos.

Mejores prácticas para la configuración global de StorageGRID con FabricPool

Al configurar un sistema StorageGRID para usarlo con FabricPool, es posible que debas cambiar otras opciones de StorageGRID. Antes de cambiar una configuración global, considera cómo afectará el cambio a otras aplicaciones S3.

Destinos de mensajes de auditoría y registros

FabricPool suele tener cargas de trabajo con una alta tasa de operaciones de lectura, lo que puede generar un gran volumen de mensajes de auditoría.

- Si no necesitas un registro de las operaciones de lectura de los clientes para FabricPool o cualquier otra aplicación de S3, puedes ir a **Configuración > Supervisión > Servidor de auditoría y syslog**. Cambia el ajuste **Lecturas de clientes a Error** para reducir el número de mensajes de auditoría registrados en el registro de auditoría. Consulta ["Configura la gestión de registros y el servidor syslog externo"](#) para obtener más detalles.
- Si tienes una grid grande, usas varios tipos de aplicaciones S3 o quieres conservar todos los datos de

auditoría, configura un servidor syslog externo y guarda la información de auditoría de forma remota. Usar un servidor externo minimiza el impacto en el rendimiento del registro de mensajes de auditoría sin reducir la integridad de los datos de auditoría. Consulta ["Aspectos a tener en cuenta para un servidor syslog externo"](#) para más detalles.

Cifrado de objetos

Al configurar StorageGRID, puedes habilitar opcionalmente ["Opción global para el cifrado de objetos almacenados"](#) si necesitas cifrar los datos para otros clientes de StorageGRID. Los datos que se transfieren por niveles desde FabricPool a StorageGRID ya están cifrados, por lo que no es necesario que habilites la configuración de StorageGRID. Las claves de cifrado del lado del cliente pertenecen a ONTAP.

Compresión de objetos

Al configurar StorageGRID, no actives la ["Opción global para comprimir objetos almacenados"](#). Los datos que se transfieren de FabricPool a StorageGRID ya están comprimidos. Usar la opción de StorageGRID no reducirá aún más el tamaño de un objeto.

Bloqueo de objetos de S3

Si la configuración global de S3 Object Lock está habilitada para tu sistema StorageGRID, no habilites ["Bloqueo de objetos de S3"](#) cuando crees buckets de FabricPool. S3 Object Lock no es compatible con los buckets de FabricPool.

Consistencia del bucket

Para los buckets de FabricPool, la consistencia recomendada es **Read-after-new-write**, que es la consistencia predeterminada para un bucket nuevo. No edites los buckets de FabricPool para que usen **Available** o **Strong-site**.

FabricPool organización en niveles

Si un nodo de StorageGRID utiliza almacenamiento asignado desde un sistema NetApp ONTAP, comprueba que el volumen no tenga habilitada una política de organización por niveles de FabricPool. Por ejemplo, si un nodo de StorageGRID se ejecuta en un host de VMware, asegúrate de que el volumen que respalda el datastore para el nodo de StorageGRID no tenga habilitada una política de organización por niveles de FabricPool. Desactivar la organización por niveles de FabricPool para los volúmenes utilizados con nodos de StorageGRID simplifica la resolución de problemas y las operaciones de almacenamiento.



Nunca uses FabricPool para transferir ningún dato relacionado con StorageGRID de vuelta al propio StorageGRID. Transferir datos de StorageGRID de vuelta a StorageGRID aumenta la complejidad de la resolución de problemas y de las operaciones.

Eliminar datos de FabricPool de StorageGRID

Si necesitas eliminar los datos de FabricPool que se encuentran actualmente almacenados en StorageGRID, debes usar ONTAP para recuperar todos los datos del volumen FabricPool y promoverlos al nivel de rendimiento.

Antes de empezar

- Has revisado las instrucciones y consideraciones en ["Promociona los datos al nivel de rendimiento"](#).
- Estás utilizando ONTAP 9.8 o una versión posterior.

- Estás usando un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios de StorageGRID para la cuenta de inquilino FabricPool que tiene el ["Gestiona todos los buckets o permiso de acceso a raíz"](#).

Acerca de esta tarea

Estas instrucciones explican cómo transferir datos desde StorageGRID de vuelta a FabricPool. Realizas este procedimiento usando ONTAP y StorageGRID Tenant Manager.

Pasos

1. Desde ONTAP, ejecuta el comando `volume modify`.

Establece `tiering-policy` en `none` para detener la nueva clasificación por niveles y establece `cloud-retrieval-policy` en `promote` para devolver a StorageGRID todos los datos que se habían clasificado por niveles anteriormente.

Consulta ["Promociona todos los datos de un volumen de FabricPool al nivel de rendimiento"](#).

2. Espera a que finalice la operación.

Puedes usar el comando `volume object-store` con la opción `tiering` para ["Comprueba el estado de la promoción del nivel de rendimiento"](#).

3. Cuando haya finalizado la operación de promoción, inicia sesión en StorageGRID Tenant Manager con la cuenta de inquilino FabricPool.
4. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.
5. Confirma que el depósito FabricPool ahora está vacío.
6. Si el bucket está vacío, ["eliminar el bucket"](#).

Después de que termines

Al eliminar el bucket, ya no se podrá continuar con la organización en niveles de FabricPool a StorageGRID. Sin embargo, porque el nivel local sigue vinculado al nivel en la nube de StorageGRID, ONTAP System Manager mostrará mensajes de error indicando que el bucket es inaccesible.

Para evitar estos mensajes de error, realiza una de las siguientes acciones:

- Utiliza FabricPool Mirror para asociar un nivel de nube diferente al agregado.
- Mueve los datos del agregado FabricPool a un agregado que no sea FabricPool y luego elimina el agregado que ya no se use.

Consulta la ["Documentación de ONTAP para FabricPool"](#) para obtener instrucciones.

Usa inquilinos y clientes de StorageGRID

Utiliza una cuenta de inquilino

Utiliza una cuenta de StorageGRID

Una cuenta de inquilino te permite utilizar la API de REST del Servicio de Almacenamiento Sencillo (S3) para almacenar y recuperar objetos en un sistema StorageGRID.

¿Qué es una cuenta de inquilino?

Cada cuenta de cliente tiene sus propios grupos federados o locales, usuarios, buckets de S3 y objetos.

Puedes usar las cuentas de inquilino para segregar los objetos almacenados por diferentes entidades. Por ejemplo, puedes usar varias cuentas de inquilino para cualquiera de estos casos de uso:

- **Caso de uso empresarial:** Si el sistema StorageGRID se utiliza en el ámbito empresarial, el almacenamiento de objetos de la grid podría estar segmentado por los distintos departamentos de la organización. Por ejemplo, podría haber cuentas de inquilino para el departamento de Marketing, el departamento de Customer Support, el departamento de Human Resources, y así sucesivamente.



Si usas el protocolo de cliente S3, también puedes usar buckets de S3 y políticas de bucket para segregar objetos entre los departamentos de una empresa. No necesitas crear cuentas de inquilino separadas. Consulta las instrucciones para implementar "[Buckets de S3 y políticas de bucket](#)" para obtener más información.

- **Caso de uso de proveedor de servicios:** si un proveedor de servicios utiliza el sistema StorageGRID, el almacenamiento de objetos del grid podría estar segregado por las diferentes entidades que alquilan el almacenamiento. Por ejemplo, podría haber cuentas de inquilino para Company A, Company B, Company C, y así sucesivamente.

Cómo crear una cuenta de inquilino

Las cuentas de inquilino las crea un "[Administrador de la grid StorageGRID usando Grid Manager](#)". Al crear una cuenta de inquilino, el administrador de grid especifica lo siguiente:

- Información básica, incluido el nombre del inquilino, el tipo de cliente (S3) y la cuota de almacenamiento opcional.
- Permisos de la cuenta de inquilino, como si la cuenta de inquilino puede usar los servicios de la plataforma S3, configurar su propia fuente de identidad, usar S3 Select o usar una conexión de federación de grid.
- El acceso a raíz inicial para el inquilino, en función de si el sistema StorageGRID utiliza grupos y usuarios locales, federación de identidades o inicio de sesión único (SSO).

Además, los administradores de la grid pueden activar la configuración de S3 Object Lock para el sistema StorageGRID si las cuentas de inquilinos de S3 deben cumplir con requisitos normativos. Cuando S3 Object Lock está activado, todas las cuentas de inquilinos de S3 pueden crear y gestionar buckets compatibles.

Configura clientes de S3

Después de un ["Se ha creado la cuenta de inquilino de S3"](#), puedes acceder al Tenant Manager para realizar tareas como las siguientes:

- Configura la federación de identidades (a menos que la fuente de identidades se comparta con la grid)
- Gestiona grupos y usuarios
- Utiliza la federación de grid para la clonación de cuentas y la replicación entre grid
- Gestiona claves de acceso de S3
- Crear y gestionar buckets de S3
- Usa los servicios de la plataforma S3
- Usa S3 Select
- Supervisa el uso del almacenamiento



Aunque puedes crear y gestionar buckets de S3 con el Tenant Manager, debes usar un ["Cliente S3"](#) o ["Consola de S3"](#) para ingestar y gestionar objetos.

Cómo iniciar y cerrar sesión

Inicia sesión en StorageGRID Tenant Manager

Accedes al Tenant Manager introduciendo la URL del tenant en la barra de direcciones de un ["navegador web compatible"](#).

Antes de empezar

- Ya tienes tus datos de acceso.
- Dispones de una URL para acceder al Tenant Manager, facilitada por el administrador de tu grid. La URL tendrá un aspecto similar a 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 Admin Node o la dirección IP virtual de un grupo HA de Admin Nodes. También puede incluir un número de puerto, el ID de cuenta del tenant de 20 dígitos o ambos.

- Si la URL no incluye el ID de cuenta de 20 dígitos del arrendatario, dispones de dicho ID de cuenta.
- Estás usando un ["navegador web compatible"](#).
- Las cookies están activadas en tu navegador web.
- Pertenece a un grupo de usuarios que tiene ["permisos de acceso específicos"](#).

Pasos

1. Inicia un ["navegador web compatible"](#).

2. En la barra de direcciones del navegador, introduce la URL para acceder a Tenant Manager.
3. Si te aparece una alerta de seguridad, instala el certificado utilizando el asistente de instalación del navegador.
4. Inicia sesión en Tenant Manager.

La pantalla de inicio de sesión que aparece depende de la URL que hayas introducido y de si se ha configurado el inicio de sesión único (SSO) para StorageGRID.

No usas SSO

Si StorageGRID no utiliza el inicio de sesión único, aparece una de las siguientes pantallas:

- La página de inicio de sesión de Grid Manager. Selecciona el enlace **Inicio de sesión de inquilino**.
- La página de inicio de sesión de Tenant Manager. Es posible que el campo **Cuenta** ya esté completado.
 - i. Si no aparece el ID de cuenta de 20 dígitos del arrendatario, selecciona el nombre de la cuenta del arrendatario si figura en la lista de cuentas recientes o introduce el ID de cuenta.
 - ii. Introduce tu nombre de usuario y contraseña.
 - iii. Selecciona **Sign in**.

Aparece el panel de control de Tenant Manager.

- iv. Si has recibido una contraseña inicial de otra persona, selecciona **username > Cambiar contraseña** para proteger tu cuenta.

Uso de SSO

Si StorageGRID está usando el inicio de sesión único (SSO), aparece una de las siguientes pantallas:

- La página de inicio de sesión único (SSO) de tu organización.

Introduce tus credenciales estándar de SSO y selecciona **Sign in**.

- La página de inicio de sesión único (SSO) de Tenant Manager.
 - i. Si no aparece el ID de cuenta de 20 dígitos del arrendatario, selecciona el nombre de la cuenta del arrendatario si figura en la lista de cuentas recientes o introduce el ID de cuenta.
 - ii. Selecciona **Sign in**.
 - iii. Inicia sesión con tus credenciales estándar de SSO en la página de inicio de sesión único de tu organización.

Aparece el panel de control de Tenant Manager.

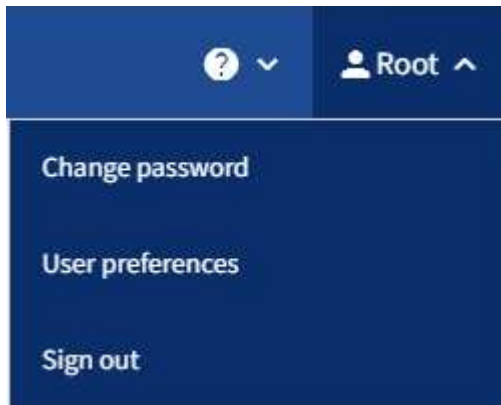
Sign out de StorageGRID Tenant Manager

Cuando hayas terminado de trabajar con Tenant Manager, debes cerrar la sesión para garantizar que los usuarios no autorizados no puedan acceder al sistema StorageGRID. Cerrar el navegador podría no cerrar tu sesión en el sistema, según la configuración de

las cookies del navegador.

Pasos

1. Busca el menú desplegable del nombre de usuario en la esquina superior derecha de la interfaz de usuario.



2. Selecciona el nombre de usuario y luego selecciona **Cerrar sesión**.

- Si no se utiliza el SSO:

Has cerrado sesión en el nodo de administración. Se muestra la página de inicio de sesión de Tenant Manager.



Si has iniciado sesión en más de un nodo de administración, debes cerrar la sesión en cada uno de ellos.

- Si el SSO está activado:

Se ha cerrado la sesión en todos los nodos de administración a los que estabas accediendo. Se muestra la página de inicio de sesión de StorageGRID. El nombre de la cuenta de tenant a la que acabas de acceder aparece como predeterminado en el menú desplegable **Recent Accounts**, y se muestra el **Account ID** del tenant.



Si el SSO está activado y además has iniciado sesión en Grid Manager, también debes cerrar la sesión en Grid Manager para cerrar la sesión en el SSO.

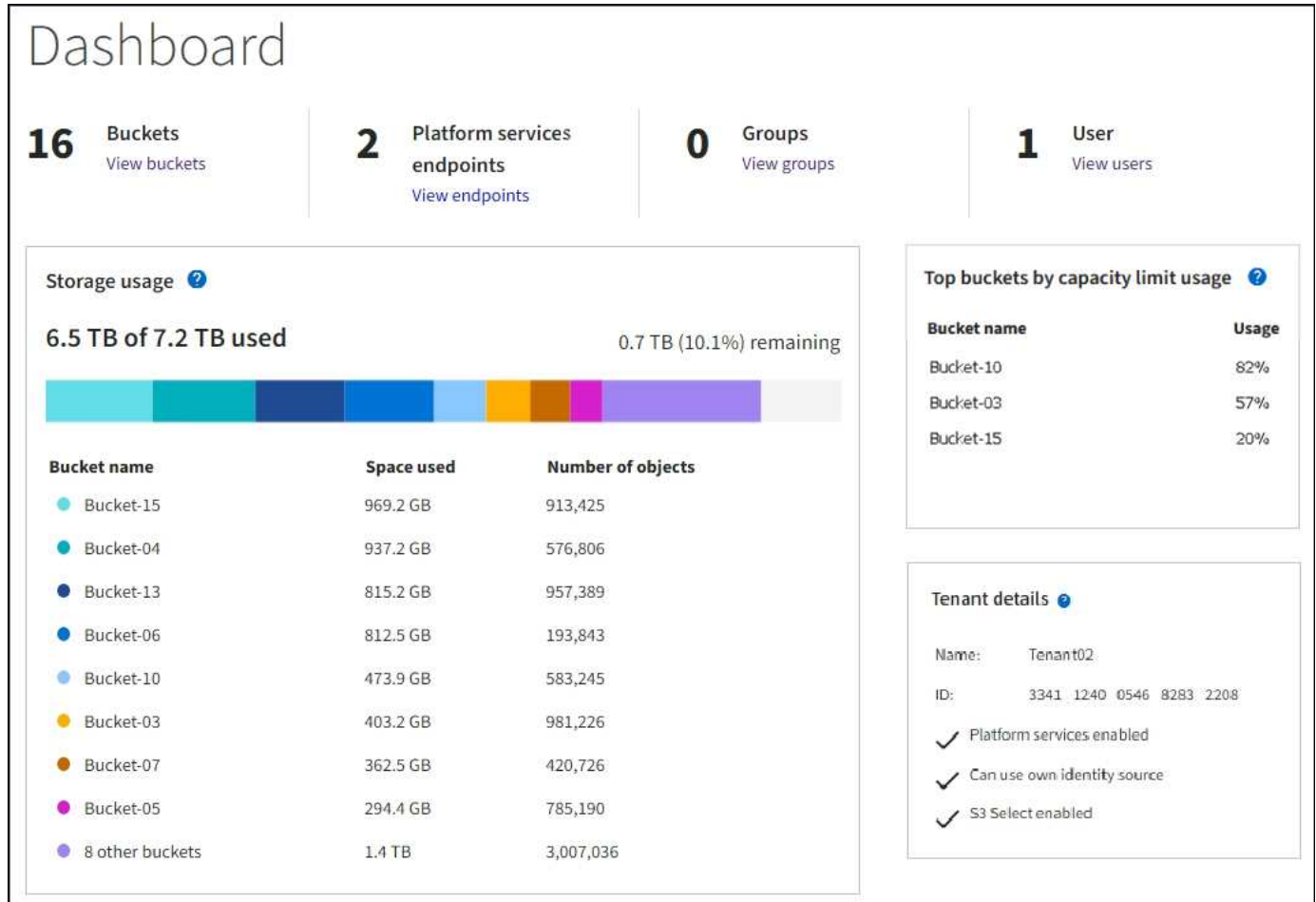
Panel de control de Tenant Manager en StorageGRID

El panel de control de Tenant Manager ofrece una visión general de la configuración de la cuenta de un tenant y de la cantidad de espacio utilizado por los objetos en los buckets S3 del tenant. Si el tenant tiene una cuota, el panel de control muestra cuánto de la cuota se ha utilizado y cuánto queda disponible. Si hay algún error relacionado con la cuenta del tenant, los errores se muestran en el panel de control.



El tamaño lógico de todos los objetos pertenecientes a este inquilino incluye las subidas multiparte incompletas y en curso. El tamaño no incluye el espacio físico adicional utilizado para las políticas de ILM. Los valores de espacio utilizado son estimaciones. Estas estimaciones se ven afectadas por el momento en que se realizan las ingestas, la conectividad de red y el estado de los nodos.

Cuando los objetos se han subido, el panel de control se ve como en el siguiente ejemplo:



Información de la cuenta del inquilino

En la parte superior del panel de control se muestra el número de buckets o contenedores, grupos y usuarios configurados. También se muestra el número de puntos de conexión de los servicios de la plataforma, en caso de que se haya configurado alguno. Selecciona los enlaces para ver los detalles.

En función del "[permisos de gestión de inquilinos](#)" que tengas y de las opciones que hayas configurado, el resto del panel de control muestra diversas combinaciones de directrices, uso del almacenamiento, información sobre los objetos y detalles del inquilino.

Almacenamiento y uso de cuotas

El panel «Uso del almacenamiento» contiene la siguiente información:

- La cantidad de datos de objetos del 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, se muestra la cantidad total de espacio disponible para los datos de objetos 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 comprueba la cuota cuando un inquilino comienza a cargar objetos y rechaza nuevas cargas si el inquilino ha superado la cuota. Sin embargo, StorageGRID no tiene en cuenta el tamaño de la carga actual al determinar si se ha superado la cuota. Si se eliminan objetos, es posible que temporalmente se impida al inquilino cargar nuevos objetos hasta que se recalcule el uso de la cuota. El cálculo del uso de la cuota puede tardar 10 minutos o más.

- Un gráfico de barras que representa los tamaños relativos de los cubos o contenedores más grandes.

Puedes situar el cursor sobre cualquiera de los segmentos del gráfico para ver el espacio total que ocupa ese bucket o contenedor.



- Para corresponder con el gráfico de barras, una lista de los buckets o contenedores más grandes, incluyendo la cantidad total de datos de objetos y el número de objetos de cada bucket 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 buckets o contenedores, todos los demás buckets o contenedores se agrupan en una única entrada al final de la lista.



Para cambiar las unidades de los valores de almacenamiento que se muestran en el Tenant Manager, selecciona el menú desplegable de usuario situado en la esquina superior derecha del Tenant Manager y luego selecciona **User preferences**.

Alertas de uso de cuotas

Si se han activado las alertas de uso de cuotas en el Grid Manager, estas alertas aparecerán en el Tenant Manager cuando la cuota sea baja o se haya superado, como sigue:

- Si se ha consumido el 90 % o más de la cuota de un inquilino, se activa la alerta **Alto consumo de la cuota del inquilino**.

Plantéate pedirle al administrador de la grid que aumente la cuota.

- Si superas tu cuota, aparecerá un aviso indicándote que no puedes subir nuevos objetos.

Uso del límite de capacidad

Si has establecido un límite de capacidad para tus buckets, el panel de control de Tenant Manager muestra una lista de los buckets con mayor uso del límite de capacidad.

Si no se establece ningún límite para un bucket, su capacidad es ilimitada. Sin embargo, si tu cuenta de inquilino tiene una cuota de almacenamiento total y se alcanza dicha cuota, no podrás añadir más objetos independientemente del límite de capacidad restante en un bucket.

Errores de endpoint

Si has utilizado el Grid Manager para configurar uno o más endpoints para usarlos con los servicios de plataforma, el panel de control de Tenant Manager muestra una alerta si ha ocurrido algún error en algún endpoint 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 en los endpoints de los servicios de plataforma](#)", selecciona **Endpoints** para mostrar la página Endpoints.

API de gestión de inquilinos

Conoce la API de gestión de inquilinos de StorageGRID

Puedes realizar tareas de administración de sistemas utilizando la API de REST de administración de inquilinos en lugar de la interfaz de usuario de Tenant Manager. Por ejemplo, es posible que quieras usar la API para automatizar operaciones o para crear varias entidades, como usuarios, de forma más rápida.

La API de gestión de inquilinos:

- Utiliza la plataforma de API de código abierto Swagger. Swagger ofrece una interfaz de usuario intuitiva que permite tanto a desarrolladores como a usuarios sin conocimientos de programación interactuar con la API. La interfaz de usuario de Swagger proporciona información detallada y documentación completa

sobre cada operación de la API.

- Utiliza ["control de versiones para permitir actualizaciones sin interrupciones"](#).

Para acceder a la documentación de Swagger de la API de gestión de inquilinos:

1. Inicia sesión en Tenant Manager.
2. En la parte superior de Tenant Manager, selecciona el icono de ayuda y selecciona **API documentation**.

Operaciones de la API

La API de gestión de inquilinos organiza las operaciones de la API disponibles en las siguientes secciones:

- **cuenta:** Operaciones en la cuenta del inquilino actual, incluyendo obtener información sobre el uso del almacenamiento.
- **auth:** Operaciones para realizar la autenticación de la sesión del usuario.

La API de gestión de inquilinos es compatible con el esquema de autenticación Bearer Token. Para que un inquilino inicie sesión, debes proporcionar un nombre de usuario, una contraseña y un accountId 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 ("Authorization: Bearer token").

Para obtener información sobre cómo mejorar la seguridad de autenticación, consulta ["Protégete contra la falsificación de solicitudes entre sitios"](#).



Si el inicio de sesión único (SSO) está habilitado para el sistema StorageGRID, debes realizar pasos diferentes para autenticarte. Consulta ["Instrucciones para usar la API de administración de Grid"](#).

- **config:** Operaciones relacionadas con el lanzamiento del producto y las versiones de la Tenant Management API. Puedes consultar la versión de lanzamiento del producto y las versiones principales de la API compatibles con dicho lanzamiento.
- **contenedores:** Operaciones en buckets de S3.
- **funciones-desactivadas:** Operaciones para ver funciones que podrían haberse desactivado.
- **puntos finales:** Operaciones para gestionar un punto final. Los puntos finales permiten que un bucket de S3 utilice un servicio externo para la replicación de StorageGRID CloudMirror, notificaciones o integración de búsqueda.
- **grid-federation-connections:** Operaciones en conexiones de federación de grid y replicación entre grids.
- **grupos:** Operaciones para gestionar grupos de inquilinos locales y para recuperar grupos de inquilinos federados desde una fuente de identidad externa.
- **fuentes-de-identidad:** Operaciones para configurar una fuente de identidad externa y para sincronizar manualmente la información de grupos y usuarios federados.
- **ilm:** Operaciones sobre la configuración de la 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 gestionar las claves de acceso a S3 de los usuarios del inquilino.
- **s3-object-lock:** Operaciones sobre la configuración global de S3 Object Lock, usadas para admitir el cumplimiento normativo.
- **Usuarios:** Operaciones para ver y gestionar usuarios de inquilinos.

Detalles de la operación

Al desplegar cada operación de la API, podrás ver su acción HTTP, la URL del endpoint, una lista de los 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>

Realizar solicitudes a la API



Cualquier operación de la API que realices a través de la página web de la documentación de la API es una operación en tiempo real. Ten cuidado de no crear, actualizar ni eliminar por error datos de configuración u otros datos.

Pasos

1. Selecciona la acción HTTP para ver los detalles de la solicitud.

2. Comprueba si la solicitud requiere parámetros adicionales, como un ID de grupo o de usuario. Luego, obtén estos valores. Puede que primero tengas que enviar otra solicitud a la API para obtener la información que necesitas.
3. Comprueba si es necesario modificar el cuerpo de la solicitud de ejemplo. Si es así, puedes seleccionar **Modelo** para conocer los requisitos de cada campo.
4. Selecciona **Pruébalo**.
5. Introduce los parámetros necesarios o modifica el cuerpo de la solicitud según sea necesario.
6. Selecciona **Ejecutar**.
7. Revisa el código de respuesta para determinar si la solicitud fue exitosa.

Versionado de la API de gestión de inquilinos de StorageGRID

La API de gestión de inquilinos utiliza un sistema de versiones para permitir actualizaciones sin interrupciones.

Por ejemplo, esta URL de solicitud especifica la versión 4 de la API.

`https://hostname_or_ip_address/api/v4/authorize`

La versión principal de la API se incrementa cuando se realizan cambios que *no son compatibles* con las versiones anteriores. La versión secundaria de la API se incrementa cuando se realizan cambios que *sí son compatibles* con las versiones anteriores. Los cambios compatibles incluyen la adición de nuevos endpoints o nuevas propiedades.

El siguiente ejemplo ilustra cómo se incrementa la versión de la API en función del tipo de cambios realizados.

Tipo de cambio en la API	Versión anterior	Nueva versión
Compatible con versiones anteriores	2,1	2,2
No es compatible con versiones anteriores	2,1	3,0

Al instalar el software StorageGRID por primera vez, solo se habilita la versión más reciente de la API. Sin embargo, al actualizar a una nueva versión funcional de StorageGRID, sigues teniendo acceso a la versión anterior de la API durante al menos una versión funcional de StorageGRID.



Puedes configurar las versiones compatibles. Consulta la sección **config** de la documentación de la API de Swagger para el ["API de gestión de grid"](#) para más información. Debes desactivar la compatibilidad con la versión anterior después de actualizar todos los clientes de la API para que usen la versión más reciente.

Las solicitudes obsoletas se marcan como en desuso de las siguientes maneras:

- El encabezado de respuesta es "Deprecated: true"
- El cuerpo de la respuesta JSON incluye "deprecated": true
- Se añade una advertencia de obsolescencia a nms.log. Por ejemplo:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Averigua qué versiones de la API son compatibles en la versión actual

Utiliza la solicitud de API `GET /versions` para devolver una lista de las versiones principales de la 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
  ]
}
```

Especifica una versión de la API para una solicitud

Puedes especificar la versión de la API utilizando un parámetro de ruta (`/api/v4`) o un encabezado (`Api-Version: 4`). Si proporcionas ambos valores, el valor del encabezado tiene prioridad sobre el de la ruta.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protégete contra la falsificación de petición en sitios cruzados en StorageGRID

Puedes ayudar a proteger StorageGRID contra los ataques de falsificación de solicitudes entre sitios (CSRF) utilizando tokens CSRF para reforzar la autenticación que usa cookies. Grid Manager y Tenant Manager activan automáticamente esta función de seguridad; otros clientes de la API pueden elegir si desean activarla al iniciar sesión.

Un atacante que pueda provocar el envío de una solicitud a otro sitio (por ejemplo, mediante un formulario HTTP POST) puede hacer que se realicen ciertas solicitudes utilizando las cookies del usuario que ha iniciado sesión.

StorageGRID ayuda a proteger contra los ataques CSRF mediante el uso de tokens CSRF. Cuando está habilitado, el contenido de una cookie específica debe coincidir con el contenido de un encabezado específico o de un parámetro específico del cuerpo de POST.

Para habilitar la función, establece el parámetro `csrfToken` en `true` durante la autenticación. El valor predeterminado es `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Cuando es verdadero, se establece una cookie `GridCsrfToken` con un valor aleatorio para los inicios de sesión en el Grid Manager, y la cookie `AccountCsrfToken` se establece con un valor aleatorio para los inicios de sesión en el Tenant Manager.

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:

- La cabecera `X-Csrf-Token`, con el valor de la cabecera establecido en el valor de la cookie de token CSRF.
- Para los puntos finales que aceptan un cuerpo codificado en formato form-encoded: un parámetro del cuerpo de la solicitud codificado en formato form-encoded. `csrfToken`

Para configurar la protección contra CSRF, utiliza ["API de gestión de grid"](#) o ["API de gestión de inquilinos"](#).



Las solicitudes que tengan configurada una cookie con un token CSRF también aplicarán el encabezado `"Content-Type: application/json"` a cualquier solicitud que requiera un cuerpo de solicitud en formato JSON como protección adicional contra los ataques CSRF.

Usa conexiones de federación de grid

Clona grupos de inquilinos y usuarios en StorageGRID

Si se ha creado o modificado un inquilino para que utilice una conexión de federación de grid, ese inquilino se replica desde un sistema StorageGRID (el inquilino de origen) a otro sistema StorageGRID (el inquilino réplica). Después de que el inquilino se haya replicado, cualquier grupo y usuario añadido al inquilino de origen se clona en el inquilino réplica.

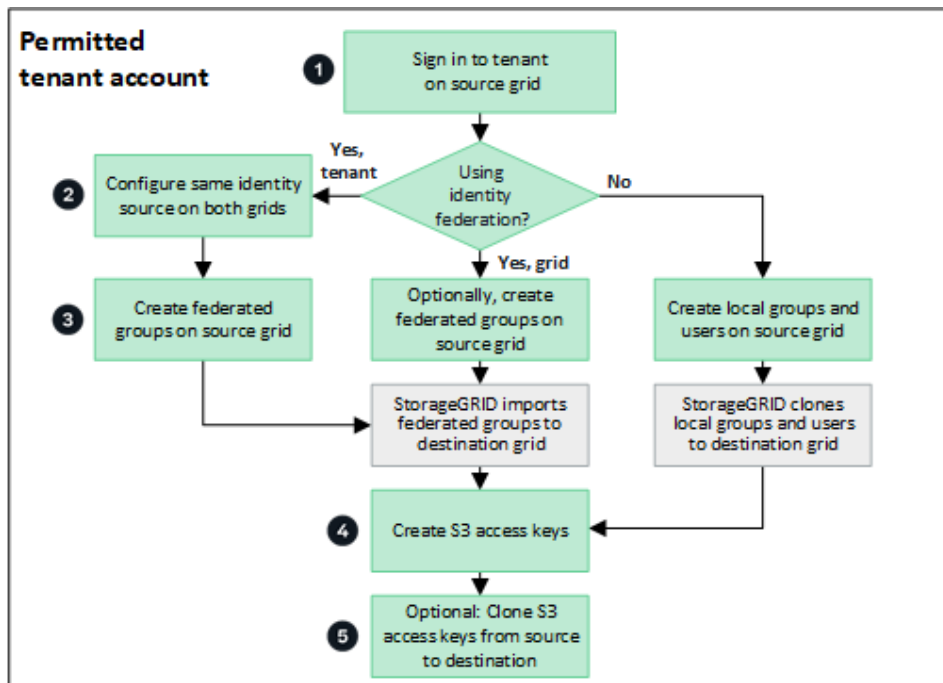
El sistema StorageGRID en el que se crea originalmente el inquilino es la *red de origen* de dicho inquilino. El sistema StorageGRID en el que se replica el inquilino es la *red de destino* de dicho inquilino. Ambas cuentas de inquilino tienen el mismo ID de cuenta, nombre, descripción, cuota de almacenamiento y permisos asignados, pero el inquilino de destino no dispone inicialmente de una contraseña de usuario raíz. Para obtener más información, consulta ["¿Qué es un clon de cuenta?"](#) y ["Gestiona los inquilinos autorizados"](#).

Es necesario clonar la información de la cuenta del inquilino para ["replicación entre grids"](#) de los objetos de los buckets. Tener los mismos grupos de inquilinos y usuarios en ambas grids garantiza que puedas acceder a los buckets y objetos correspondientes en cualquiera de las grids.

Flujo de trabajo del inquilino para la clonación de una cuenta

Si tu cuenta de inquilino tiene el permiso **Use grid federation connection**, revisa el diagrama del flujo de

trabajo para ver los pasos que deberás seguir para clonar grupos, usuarios y claves de acceso a S3.



Estos son los pasos principales del flujo de trabajo:

1

Inicia sesión en el tenant

Inicia sesión en la cuenta de inquilino en la grid de origen (la grid donde se creó inicialmente el inquilino).

2

Si lo deseas, configura la federación de identidades

Si tu cuenta de inquilino tiene el permiso **Usar fuente de identidad propia** para utilizar grupos y usuarios federados, configura la misma fuente de identidad (con los mismos ajustes) tanto para la cuenta de inquilino de origen como para la de destino. Los grupos y usuarios federados no se pueden clonar a menos que ambas grids utilicen la misma fuente de identidad. Para obtener instrucciones, consulta ["Usa la federación de identidades"](#).

3

Crear grupos y usuarios

Al crear grupos y usuarios, empieza siempre por la grid de origen del inquilino. Cuando añades un nuevo grupo, StorageGRID lo clona automáticamente en la grid de destino.

- Si la federación de identidades está configurada para todo el sistema StorageGRID o para tu cuenta de inquilino, ["crear nuevos grupos de inquilinos"](#) importando los grupos federados desde la fuente de identidades.
- Si no utilizas la federación de identidades, ["crear nuevos grupos locales"](#) y luego ["crear usuarios locales"](#).

4

Crear claves de acceso a S3

Puedes ["Crea tus propias claves de acceso"](#) o ["crear las claves de acceso de otro usuario"](#) tanto en la grid de

origen como en la grid de destino para acceder a los buckets en esa grid.

5

Opcionalmente, clona las claves de acceso a S3

Si necesitas acceder a buckets con las mismas claves de acceso en ambas grids, crea las claves de acceso en la grid de origen y luego usa la API de Tenant Manager para clonarlas manualmente en la grid de destino. Para obtener instrucciones, consulta ["Clonar claves de acceso a S3 mediante la API"](#).

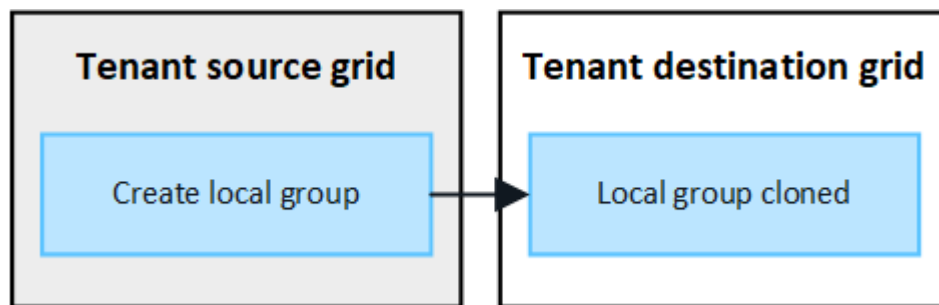
¿Cómo se clonan los grupos, los usuarios y las claves de acceso de S3?

Consulta esta sección para comprender cómo se clonan los grupos, los usuarios y las claves de acceso a S3 entre la grid de origen del tenant y la grid de destino del tenant.

Los grupos locales creados en la grid de origen se clonan

Después de que se crea una cuenta de inquilino y se replica en la grid de destino, StorageGRID clona automáticamente cualquier grupo local que añadas a la grid de origen del inquilino en la grid de destino del mismo.

Tanto el grupo original como su clon tienen el mismo modo de acceso, los mismos permisos de grupo y la misma política de grupo de S3. Para obtener instrucciones, consulta ["Crear grupos para el inquilino de S3"](#).

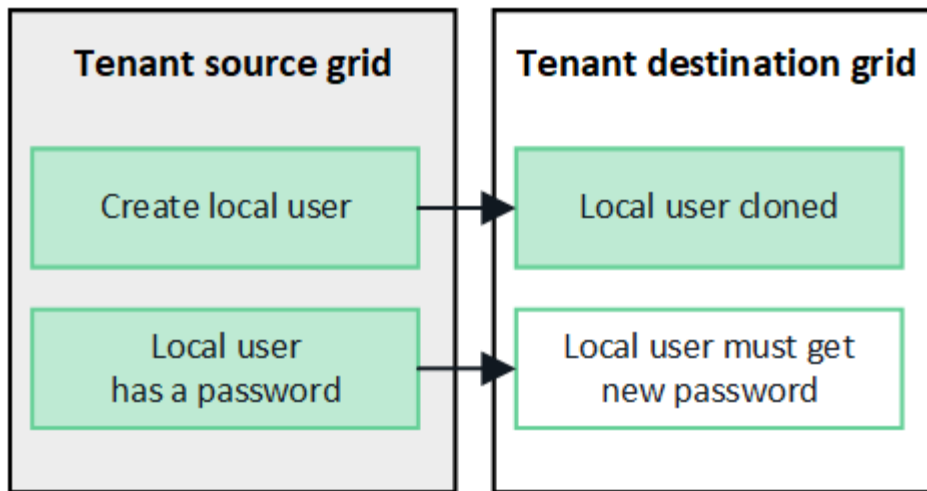


Los usuarios que selecciones al crear un grupo local en la grid de origen no se incluyen cuando el grupo se clona en la grid de destino. Por esta razón, no selecciones usuarios cuando crees el grupo. En su lugar, selecciona el grupo cuando crees los usuarios.

Los usuarios locales creados en el grid de origen se clonan

Al crear 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 de **Denegar acceso**. Ambos usuarios también pertenecen a los mismos grupos. Para obtener instrucciones, consulta ["Gestiona usuarios"](#).

Por motivos de seguridad, las contraseñas de los usuarios locales no se clonan en la grid de destino. Si un usuario local necesita acceder a Tenant Manager en la grid de destino, el usuario raíz de la cuenta del tenant debe añadir una contraseña para ese usuario en la grid de destino. Para obtener instrucciones, consulta ["Gestiona usuarios"](#).

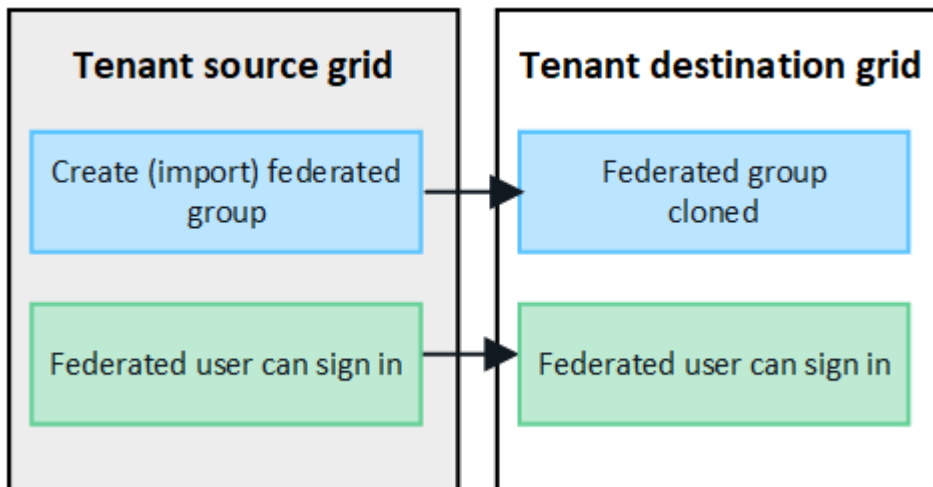


Los grupos federados creados en la grid de origen se clonan

Siempre que se cumplan los requisitos para utilizar la clonación de cuentas con ["inicio de sesión único"](#) y ["federación de identidades"](#), los grupos federados que crees (importes) para el tenant en la grid de origen se clonan automáticamente al tenant en la grid de destino.

Ambos grupos tienen el mismo modo de acceso, permisos de grupo y política de grupo de S3.

Después de que se crean los grupos federados para el inquilino de origen y se clonan en el inquilino de destino, los usuarios federados pueden iniciar sesión en el inquilino en cualquiera de las dos grids.

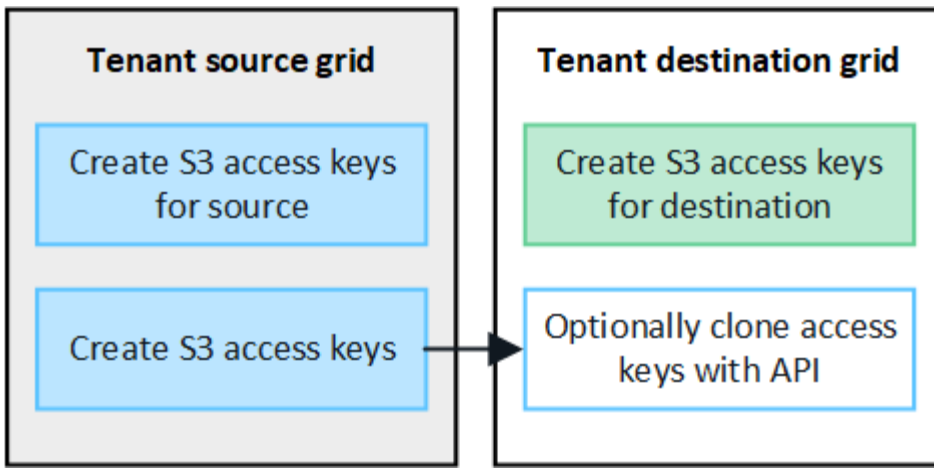


Las claves de acceso de S3 se pueden clonar manualmente

StorageGRID no clona automáticamente las claves de acceso de S3 porque la seguridad mejora al tener claves diferentes en cada grid.

Para gestionar las claves de acceso en las dos grids, puedes hacer cualquiera de las siguientes cosas:

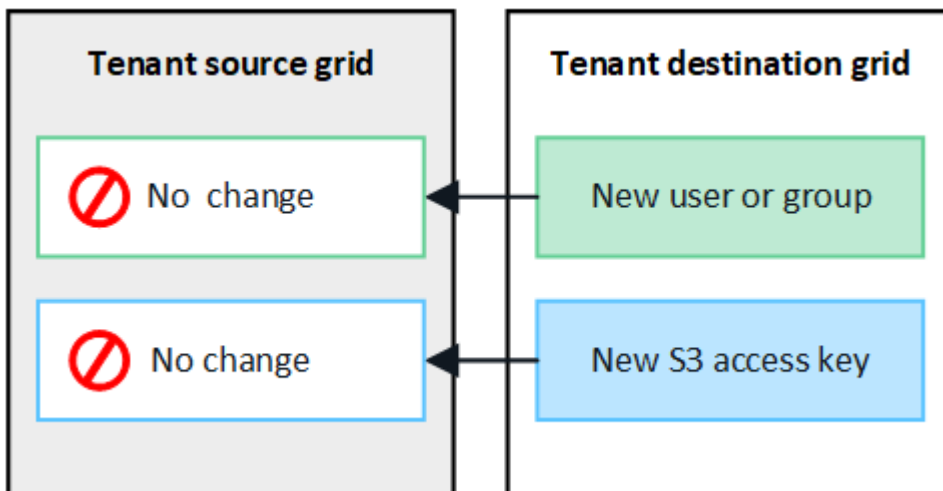
- Si no necesitas usar las mismas claves para cada grid, puedes ["Crea tus propias claves de acceso"](#) o ["crear las claves de acceso de otro usuario"](#) en cada grid.
- Si necesitas utilizar las mismas claves en ambas grids, puedes crear las claves en la grid de origen y luego usar la API de Tenant Manager para ["clonar las llaves"](#) manualmente en la grid de destino.



Al clonar las claves de acceso a S3 de un usuario federado, tanto el usuario como las claves de acceso a S3 se clonan en el inquilino de destino.

Los grupos y usuarios añadidos a la cuadrícula de destino no se clonan

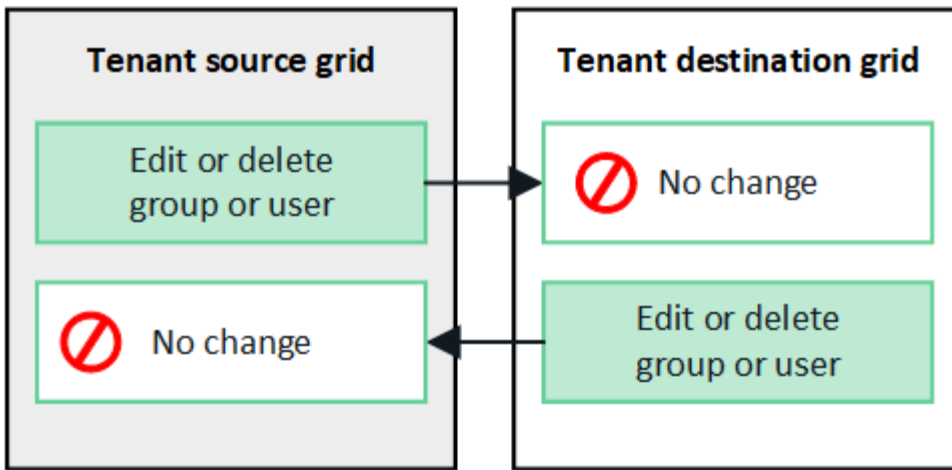
La clonación solo se produce desde la grid de origen del inquilino hacia la grid de destino del inquilino. Si creas o importas grupos y usuarios en la grid de destino del inquilino, StorageGRID no clonará estos elementos de vuelta a la grid de origen del inquilino.



Los grupos, usuarios y claves de acceso editados o eliminados no se clonan

La clonación solo ocurre cuando creas nuevos grupos y usuarios.

Si editas o eliminas grupos, usuarios o claves de acceso en cualquiera de las dos cuadrículas, tus cambios no se clonarán en la otra cuadrícula.



Clona claves de acceso S3 entre grids de StorageGRID usando la Tenant Management API

Si tu cuenta de inquilino StorageGRID tiene el permiso **Usar conexión de federación de grid**, puedes usar la API de gestión de inquilinos para clonar manualmente las claves de acceso S3 del inquilino en el grid de origen al inquilino en el grid de destino.

Antes de empezar

- La cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**.
- La conexión a la federación de grid tiene un **Estado de conexión** de **Conectada**.
- Has iniciado sesión en el Tenant Manager en la grid de origen del inquilino usando una ["navegador web compatible"](#).
- Pertences a un grupo de usuarios que tiene ["Gestiona tus propias credenciales de S3 o el permiso de acceso de usuario raíz"](#).
- Si estás clonando claves de acceso para un usuario local, el usuario ya existe en ambas grids.



Al clonar las claves de acceso a S3 de un usuario federado, tanto el usuario como las claves de acceso a S3 se añaden al inquilino de destino.

Clona tus propias claves de acceso

Puedes clonar tus propias claves de acceso si necesitas acceder a los mismos buckets en ambas grids.

Pasos

1. Utiliza el Tenant Manager en la grid de origen, ["Crea tus propias claves de acceso"](#) y descarga el archivo `.csv`.
2. En la parte superior de Tenant Manager, selecciona el icono de ayuda y selecciona **API documentation**.
3. En la sección **s3**, selecciona el siguiente endpoint:

```
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. Selecciona **Pruébalo**.

5. En el cuadro de texto **cuerpo**, reemplaza las entradas de ejemplo para **accessKey** y **secretAccessKey** con los valores del archivo **.csv** que descargaste.

Asegúrate de mantener las comillas dobles alrededor de cada cadena.



The screenshot shows a REST client interface with a light green header. The header contains the text "body" followed by a red asterisk and the word "required". Below the header, there are two tabs: "Edit Value" and "Model". The "Model" tab is selected, and it displays a JSON object with the following structure:

```
{
  "accessKey": "AKIAIOSFODNN7EXAMPLE",
  "secretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY",
  "expires": "2028-09-04T00:00:00.000Z"
}
```

6. Si la clave va a caducar, sustituye la entrada de ejemplo de **expires** por la fecha y la hora de caducidad en forma de cadena con el formato de fecha y hora ISO 8601 (por ejemplo, 2024-02-28T22:46:33-08:00). Si la clave no va a caducar, introduce **null** como valor para la entrada **expires** (o elimina la línea **Expires** y la coma que la precede).
7. Selecciona **Ejecutar**.
8. Comprueba que el código de respuesta del servidor sea **204**, lo que indica que la clave se clonó correctamente en el grid de destino.

Clonar las claves de acceso de otro usuario

Puedes clonar las claves de acceso de otro usuario si este necesita acceder a los mismos buckets en ambas grids.

Pasos

1. Utiliza el Tenant Manager en la grid de origen, "[crear las claves de acceso a S3 del otro usuario](#)" y descarga el archivo **.csv**.
2. En la parte superior de Tenant Manager, selecciona el icono de ayuda y selecciona **API documentation**.
3. Obtén el ID de usuario. Necesitarás este valor para clonar las claves de acceso del otro usuario.
 - a. En la sección **usuarios**, selecciona el siguiente endpoint:

```
GET /org/users
```
 - b. Selecciona **Pruébalo**.
 - c. Especifica cualquier parámetro que quieras usar cuando busques usuarios.
 - d. Selecciona **Ejecutar**.
 - e. Busca el usuario cuyas claves quieras clonar y copia el número del campo **id**.
4. En la sección **s3**, selecciona el siguiente endpoint:

```
POST /org/users/{userId}/replicate-s3-access-key
```



The screenshot shows a REST client interface with a light green header. The header contains the text "POST" in a green box, followed by 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. Selecciona **Pruébalo**.

6. En el cuadro de texto **userid**, pega el ID de usuario que copiaste.
7. En el cuadro de texto **cuerpo**, sustituye las entradas de ejemplo de **example access key** y **secret access key** por los valores del archivo **.csv** para ese usuario.

Asegúrate de mantener las comillas dobles alrededor de la cadena.
8. Si la clave va a caducar, sustituye la entrada de ejemplo de **expires** por la fecha y la hora de caducidad en forma de cadena con el formato de fecha y hora ISO 8601 (por ejemplo, **2023-02-28T22:46:33-08:00**). Si la clave no va a caducar, introduce **null** como valor para la entrada **expires** (o elimina la línea **Expires** y la coma que la precede).
9. Selecciona **Ejecutar**.
10. Comprueba que el código de respuesta del servidor sea **204**, lo que indica que la clave se clonó correctamente en el grid de destino.

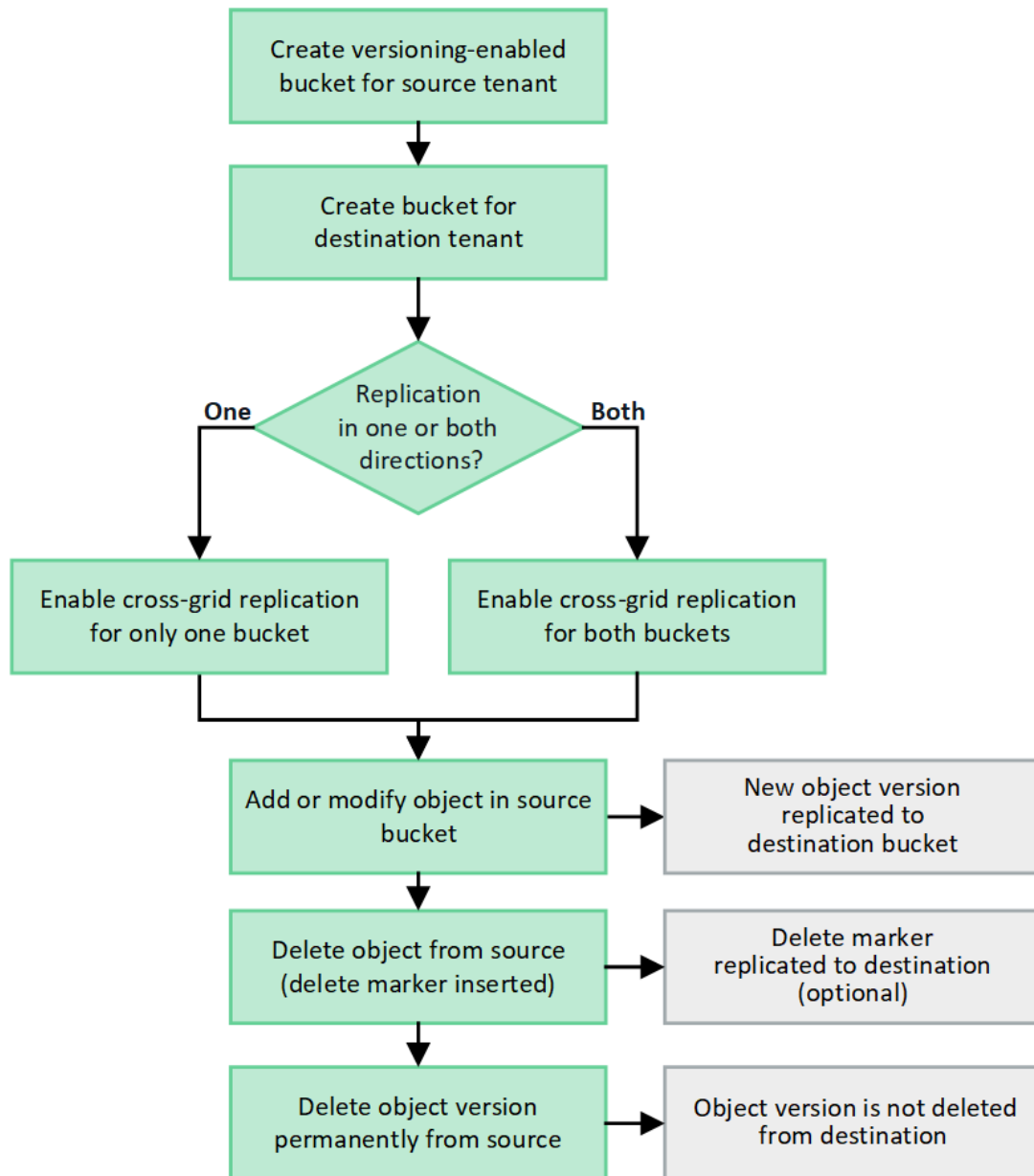
Administra la replicación entre grids en StorageGRID

Si a tu cuenta de inquilino se le asignó el permiso **Utilizar conexión de federación entre redes** al crearse, puedes utilizar la replicación entre redes para replicar automáticamente objetos entre los buckets de la red de origen del inquilino y los buckets de la red de destino del inquilino. La replicación entre redes puede realizarse en una o en ambas direcciones.

Flujo de trabajo para la replicación entre grids

El diagrama de flujo resume los pasos que tienes que seguir para configurar la replicación entre redes entre buckets en dos redes. Estos pasos se describen con más detalle debajo del diagrama.

Tenant user



Configura la replicación entre grids

Antes de que puedas usar la replicación entre grids, debes iniciar sesión en las cuentas de inquilino correspondientes en cada grid y crear dos buckets. Luego, puedes habilitar la replicación entre grids en cualquiera de los buckets o en ambos.

Antes de empezar

- Ya has revisado los requisitos para la replicación entre grids. Consulta "[¿Qué es la replicación entre grids?](#)".
- Estás utilizando un "[navegador web compatible](#)".
- La cuenta de inquilino tiene el permiso **Utilizar conexión de federación entre redes** y existen cuentas de inquilino idénticas en ambas redes. Consulta "[Gestiona los inquilinos permitidos para la conexión de federación de grid](#)".
- El usuario inquilino con el que estás iniciando sesión ya existe en ambos grids y pertenece a un grupo de usuarios que tiene el "[Permiso de acceso raíz](#)".

- Si te estás autenticando en la grid de destino del tenant como usuario local, el usuario raíz de la cuenta del tenant ha establecido una contraseña para tu cuenta de usuario en esa grid.

Crea dos buckets

Como primer paso, inicia sesión en las cuentas de inquilino correspondientes en cada grid y crea un bucket en cada grid.

Pasos

1. Partiendo de cualquiera de las dos grids en la conexión de la federación de grids, crea un nuevo bucket:
 - a. Inicia sesión en la cuenta de inquilino usando las credenciales de un usuario de inquilino que existe en ambas grids.

Si no puedes iniciar sesión en la grid de destino del tenant como usuario local, confirma que el usuario raíz de la cuenta del tenant haya establecido una contraseña para tu cuenta de usuario.

- b. Sigue las instrucciones para ["crear un depósito de S3"](#).



Los nombres de los buckets y las regiones pueden ser diferentes en cada grid.

- c. En la pestaña **Administrar configuración de objetos**, selecciona **Habilitar control de versiones de objetos**.
 - d. Si S3 Object Lock está habilitado para tu sistema StorageGRID, consulta ["Replicación entre grids con S3 Object Lock"](#).
 - e. Selecciona **Create bucket**.
 - f. Selecciona **Finalizar**.
2. Repite estos pasos para crear un bucket para la misma cuenta de inquilino en la otra grid de la conexión de federación de grids.



Según sea necesario, cada bucket puede usar una región diferente.

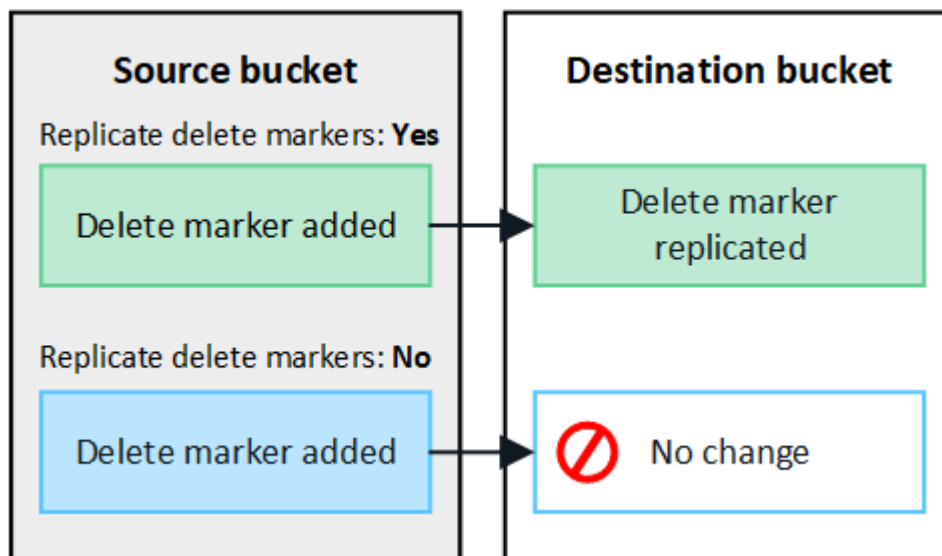
Habilita la replicación entre grids

Debes seguir estos pasos antes de añadir cualquier objeto a cualquiera de los dos buckets.

Pasos

1. A partir de un grid cuyos objetos quieras replicar, activa ["replicación entre grids en una sola dirección"](#):
 - a. Inicia sesión en la cuenta de inquilino para el bucket.
 - b. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.
 - c. Selecciona el nombre del depósito en la tabla para acceder a la página de detalles del depósito.
 - d. Selecciona la pestaña **Replicación entre grids**.
 - e. Selecciona **Habilitar** y revisa la lista de requisitos.
 - f. Si se han cumplido todos los requisitos, selecciona la conexión de federación de grid que quieres usar.
 - g. Si lo deseas, puedes modificar la configuración de **Replicar marcadores de eliminación** para determinar qué ocurre en la grid de destino si un cliente S3 envía una solicitud de eliminación a la grid de origen que no incluye un ID de versión:

- **Sí** (por defecto): Se añade un marcador de eliminación al bucket de origen y se replica en el bucket de destino.
- **No**: Se añade 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 bucket de origen. StorageGRID no replica las solicitudes de eliminación que incluyen un ID de versión, por lo que esa misma versión del objeto no se elimina del destino.

Consulta "[¿Qué es la replicación entre grids?](#)" para obtener más detalles.

- Opcionalmente, cambia la configuración de la categoría de auditoría **Cross-grid replication** para gestionar el volumen de mensajes de auditoría:
 - **Error** (por defecto): Solo se incluyen en la salida de auditoría las solicitudes de replicación entre grids que han fallado.
 - **Normal**: Se incluyen todas las solicitudes de replicación entre grids, lo que aumenta considerablemente el volumen de los resultados de la auditoría.
- Revisa tus selecciones. No puedes cambiar esta configuración a menos que ambos depósitos estén vacíos.
- Selecciona **Activar y probar**.

Al cabo de unos instantes, aparece un mensaje de éxito. Los objetos añadidos a este bucket se replican ahora automáticamente en la otra grid. **Cross-grid replication** aparece como una función habilitada en la página de detalles del bucket.

- Si lo prefieres, ve al bucket correspondiente en la otra grid y "[activar la replicación entre redes en ambas direcciones](#)".

Prueba de replicación entre grids

Si la replicación entre redes está habilitada para un bucket, es posible que tengas que comprobar que la conexión y la replicación entre redes funcionan correctamente y que los buckets de origen y destino siguen cumpliendo todos los requisitos (por ejemplo, que el versionado siga habilitado).

Antes de empezar

- Estás utilizando un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene ["Permiso de acceso raíz"](#).

Pasos

1. Inicia sesión en la cuenta de inquilino para el bucket.
2. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.
3. Selecciona el nombre del depósito en la tabla para acceder a la página de detalles del depósito.
4. Selecciona la pestaña **Replicación entre grids**.
5. Selecciona **Probar conexión**.

Si la conexión es correcta, aparece un mensaje de éxito. En caso contrario, aparece un mensaje de error que tanto tú como el administrador de grid podéis utilizar para resolver el problema. Para obtener más información, consulta ["Solucionar errores de federación de grid"](#).

6. Si la replicación entre grids está configurada para realizarse en ambas direcciones, ve al bucket correspondiente en el otro grid y selecciona **Probar conexión** para comprobar que la replicación entre grids funciona en la otra dirección.

Desactivar la replicación entre grids

Puedes detener de forma permanente la replicación entre grids si ya no deseas copiar objetos a la otra grid.

Antes de desactivar la replicación entre grids, ten en cuenta lo siguiente:

- Desactivar la replicación entre grids no elimina ningún objeto que ya se haya copiado entre grids. Por ejemplo, los objetos de `my-bucket` en el Grid 1 que se hayan copiado en `my-bucket` en el Grid 2 no se eliminan si desactivas la replicación entre grids para ese bucket. Si quieres eliminar estos objetos, debes quitarlos manualmente.
- Si la replicación entre grids estaba habilitada para cada uno de los buckets (es decir, si la replicación se realiza en ambas direcciones), puedes deshabilitar la replicación entre grids para uno de los buckets o para ambos. Por ejemplo, es posible que quieras deshabilitar la replicación de objetos desde `my-bucket` en el Grid 1 a `my-bucket` en el Grid 2, mientras continúas replicando objetos desde `my-bucket` en el Grid 2 a `my-bucket` en el Grid 1.
- Debes desactivar la replicación entre redes antes de poder eliminar el permiso de un inquilino para utilizar la conexión de federación de redes. Consulta ["Gestiona los inquilinos autorizados"](#).
- Si desactivas la replicación entre redes para un depósito que contenga objetos, no podrás volver a activarla a menos que elimines todos los objetos tanto del depósito de origen como del de destino.



No puedes volver a activar la replicación a menos que ambos buckets estén vacíos.

Antes de empezar

- Estás utilizando un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene ["Permiso de acceso raíz"](#).

Pasos

1. Empezando por la grid cuyos objetos ya no quieras replicar, detén la replicación entre grids para el bucket:
 - a. Inicia sesión en la cuenta de inquilino para el bucket.

- b. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.
- c. Selecciona el nombre del depósito en la tabla para acceder a la página de detalles del depósito.
- d. Selecciona la pestaña **Replicación entre grids**.
- e. Selecciona **Desactivar la replicación**.
- f. Si estás seguro de que quieres desactivar la replicación entre grids para este bucket, escribe **Yes** en el cuadro de texto y selecciona **Disable**.

Después de unos instantes, aparece un mensaje de éxito. Los nuevos objetos que añadas a este bucket ya no se podrán replicar automáticamente en el otro grid. La **replicación entre grids** ya no se muestra como una función habilitada en la página Buckets.

2. Si la replicación entre grids se configuró para que ocurra en ambas direcciones, ve al bucket correspondiente en el otro grid y detén la replicación entre grids en la otra dirección.

Ver las conexiones de grid federation en StorageGRID

Si tu cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, puedes ver las conexiones permitidas.

Antes de empezar

- La cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**.
- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene ["Permiso de acceso raíz"](#).

Pasos

1. Selecciona **STORAGE (S3) > Grid federation connections**.

Aparece la página de conexión a la federación de Grid e incluye una tabla que resume la siguiente información:

Columna	Descripción
Nombre de la conexión	Las conexiones de la federación de grid que este inquilino tiene permiso para utilizar.
Buckets con replicación en grid cruzada	Para cada conexión de federación de grids, los buckets de los tenants que tienen habilitada la replicación entre grids. Los objetos añadidos a estos buckets se replicarán en el otro grid de la conexión.
Último error	Para cada conexión de federación de grid, el error más reciente que se haya producido, si lo hubiera, cuando se estaban replicando datos al otro grid. Consulta Borrar el último error .

2. Si lo deseas, selecciona un nombre de depósito para ["ver los detalles del bucket"](#).

Borrar el último error

Puede aparecer un error en la columna **Último error** por alguna de estas razones:

- No se encontró la versión del objeto de origen.
- No se ha encontrado el bucket de origen.
- Se eliminó el bucket de destino.
- El bucket de destino fue recreado por una cuenta diferente.
- El bucket de destino tiene el control de versiones suspendido.
- El bucket de destino fue recreado por la misma cuenta, pero ahora no tiene versiones.



Esta columna solo muestra el último error de replicación entre grids que se haya producido; los errores anteriores que pudieran haberse producido no se mostrarán.

Pasos

1. Si aparece un mensaje en la columna **Último error**, consulta el texto del mensaje.

Por ejemplo, este error indica que el depósito de destino para la replicación entre redes se encontraba en un estado no válido, posiblemente porque se había suspendido el control de versiones o porque se había activado S3 Object Lock.

Grid federation connections		
Clear error Search...		Displaying one result
Connection name	Buckets with cross-grid replication	Last error
Grid 1-Grid 2	my-cgr-bucket	2022-12-07 16:02:20 MST Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-cgr-bucket' to destination bucket 'my-cgr-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 4791585492825418592)

2. Realiza las acciones recomendadas. Por ejemplo, si se suspendió el control de versiones en el bucket de destino para la replicación entre grids, vuelve a habilitar el control de versiones para ese bucket.
3. Selecciona la conexión de la tabla.
4. Selecciona **Borrar error**.
5. Selecciona **Sí** para borrar el mensaje y actualizar el estado del sistema.
6. Espera 5-6 minutos y luego ingiere un nuevo objeto en el bucket. Confirma que el mensaje de error no vuelva a aparecer.



Para asegurarte de que el mensaje de error se borre, espera al menos 5 minutos después de la marca de tiempo en el mensaje antes de ingresar un nuevo objeto.

7. Para determinar si algún objeto no se pudo replicar debido al error del bucket, consulta ["Identifica y vuelve a intentar las operaciones de replicación que hayan fallado"](#).

Gestiona grupos y usuarios

Usa la federación de identidades en StorageGRID

El uso de la federación de identidades agiliza la configuración de grupos de inquilinos y usuarios, y permite a los usuarios de los inquilinos iniciar sesión en la cuenta del inquilino utilizando credenciales que ya conocen.

Configura la federación de identidades para Tenant Manager

Puedes configurar la federación de identidades para el Tenant Manager si quieres que los grupos y usuarios de inquilinos se gestionen en otro sistema como Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server.

Antes de empezar

- Has iniciado sesión en Tenant Manager usando una ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene ["Permiso de acceso raíz"](#).
- Estás utilizando Active Directory, Microsoft Entra ID, OpenLDAP u Oracle Directory Server como proveedor de identidades.



Si deseas utilizar un servicio LDAP v3 que no figure en la lista, ponte en contacto con soporte técnico.

- Si tienes pensado usar OpenLDAP, debes configurar el servidor OpenLDAP. Consulta [Guía para configurar el servidor OpenLDAP](#).
- Si tienes previsto usar Transport Layer Security (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidad debe estar usando TLS 1.2 o 1.3. Consulta ["Algoritmos de cifrado compatibles para las conexiones TLS salientes"](#).

Acerca de esta tarea

Que puedas configurar un servicio de federación de identidades para tu inquilino depende de cómo se haya configurado tu cuenta de inquilino. Es posible que tu inquilino comparta el servicio de federación de identidades que se configuró para Grid Manager. Si ves este mensaje cuando accedes a la página Federación de identidades, no puedes configurar un origen de identidad federado independiente 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.

Ingresa la configuración

Cuando configuras la federación de identidades, proporcionas los valores que StorageGRID necesita para conectarse a un servicio LDAP.

Pasos

1. Selecciona **Gestión de acceso > Federación de identidades**.
2. Selecciona **Habilitar federación de identidades**.
3. En la sección de tipo de servicio LDAP, selecciona el tipo de servicio LDAP que quieres configurar.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Entra ID	OpenLDAP	Other

Selecciona **Other** para configurar los valores de un servidor LDAP que utilice Oracle Directory Server.

4. Si has seleccionado **Other**, rellena los campos de la sección «Atributos LDAP». De lo contrario, pasa al siguiente paso.
 - **Nombre único de usuario:** El nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo equivale a `sAMAccountName` para Active Directory y `uid` para OpenLDAP. Si estás configurando Oracle Directory Server, introduce `uid`.
 - **UUID de usuario:** El nombre del atributo que contiene el identificador único permanente de un usuario LDAP. Este atributo es equivalente a `objectGUID` en Active Directory y `entryUUID` en OpenLDAP. Si estás configurando Oracle Directory Server, introduce `nsuniqueid`. El valor de cada usuario para el atributo especificado debe ser un número hexadecimal de 32 dígitos, ya sea en formato de 16 bytes o de cadena, donde se ignoran los guiones.
 - **Nombre único de 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 estás configurando Oracle Directory Server, introduce `cn`.
 - **UUID del 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 estás configurando Oracle Directory Server, introduce `nsuniqueid`. El valor de cada grupo para el atributo especificado debe ser un número hexadecimal de 32 dígitos, ya sea en formato de 16 bytes o de cadena, donde se ignoran los guiones.
5. Para todos los tipos de servicio LDAP, introduce la información necesaria sobre el servidor LDAP y la conexión de red en la sección Configurar el 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 usar cualquier puerto siempre que tu firewall esté configurado correctamente.

- **Nombre de usuario:** La ruta completa del nombre distintivo (DN) del usuario que se conectará al servidor LDAP.

Para Active Directory, también puedes especificar el Down-Level Logon Name o el User Principal Name.

El usuario especificado debe tener permiso para ver la lista de grupos y usuarios y para acceder a los siguientes atributos:

- `sAMAccountName` o `uid`

- objectGUID, entryUUID, o nsuniqueid
 - cn
 - memberOf o isMemberOf
 - **Active Directory:** objectSid, primaryGroupID, userAccountControl y userPrincipalName
 - **Entra ID:** accountEnabled y userPrincipalName
- **Contraseña:** la contraseña asociada al nombre de usuario.



Si cambias la contraseña en el futuro, debes actualizarla en esta página.

- **DN base del grupo:** La ruta completa del nombre distintivo (DN) de un subárbol LDAP en el que quieres buscar grupos. En el ejemplo de Active Directory (a continuación), todos los grupos cuyo nombre distintivo sea relativo al DN base (DC=storagegrid,DC=example,DC=com) pueden usarse como grupos federados.



Los valores de **Nombre único del grupo** deben ser únicos dentro del **DN base del grupo** al que pertenecen.

- **DN de base de usuarios:** La ruta completa del nombre distintivo (DN) de un subárbol LDAP en el que quieres buscar usuarios.



Los valores de **Nombre único de usuario** deben ser únicos dentro del **User Base DN** al que pertenecen.

- **Formato de nombre de usuario de enlace** (opcional): el patrón de nombre de usuario predeterminado que StorageGRID debe utilizar si no es posible determinar el patrón automáticamente.

Se recomienda especificar el **formato de nombre de usuario de enlace** porque puede permitir que los usuarios inicien sesión si StorageGRID no puede enlazarse con la cuenta de servicio.

Introduce uno de estos patrones:

- **Patrón UserPrincipalName (AD y Entra ID):** [USERNAME]@example.com
- **Patrón de nombre de inicio de sesión de nivel inferior (AD y Entra ID):**
example\[USERNAME]
- **Patrón de nombre distintivo:** CN=[USERNAME],CN=Users,DC=example,DC=com

Incluye [USERNAME] tal y como aparece escrito.

6. En la sección Transport Layer Security (TLS), selecciona una configuración de seguridad.

- **Usar STARTTLS:** Utiliza STARTTLS para proteger las comunicaciones con el servidor LDAP. Esta es la opción recomendada para Active Directory, OpenLDAP u Other, pero no es compatible con Microsoft Entra ID.
- **Usar LDAPS:** La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debes seleccionar esta opción para Microsoft Entra ID.
- **No utilices TLS:** El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Microsoft Entra ID.



El uso de la opción **No usar TLS** no se admite si tu servidor de Active Directory exige la firma LDAP. Debes usar STARTTLS o LDAPS.

7. Si has seleccionado STARTTLS o LDAPS, elige el certificado que se usa para proteger la conexión.
 - **Utilizar el certificado CA del sistema operativo:** Utiliza el certificado CA de Grid predeterminado instalado en el sistema operativo para proteger las conexiones.
 - **Usar certificado CA personalizado:** Usa un certificado de seguridad personalizado.

Si seleccionas esta opción, copia y pega el certificado de seguridad personalizado en el cuadro de texto de certificado de la CA.

Comprueba la conexión y guarda la configuración

Una vez introducidos todos los valores, debes comprobar la conexión antes de poder guardar la configuración. StorageGRID verifica los parámetros de conexión del servidor LDAP y el formato del nombre de usuario de enlace, si has especificado alguno.

Pasos

1. Selecciona **Probar conexión**.
2. Si no proporcionaste un formato para el nombre de usuario de bind:
 - Si los parámetros de conexión son correctos, aparece el mensaje «Prueba de conexión realizada con éxito». Selecciona **Guardar** para guardar la configuración.
 - Aparecerá el mensaje «No se ha podido establecer una conexión de prueba» si la configuración de la conexión no es válida. Selecciona **Cerrar**. Luego, soluciona cualquier problema y vuelve a probar la conexión.
3. Si has especificado un formato de nombre de usuario de enlace, introduce el nombre de usuario y la contraseña de un usuario federado válido.

Por ejemplo, introduce tu propio nombre de usuario y contraseña. No incluyas caracteres especiales 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

myusername

The username of a federated user.

Test password

***** 👁

Cancel Test Connection

- Si los parámetros de conexión son correctos, aparece el mensaje «Prueba de conexión realizada con éxito». Selecciona **Guardar** para guardar la configuración.

- Aparece un mensaje de error si la configuración de la conexión, el formato del nombre de usuario de enlace o el nombre de usuario y la contraseña de prueba no son válidos. Soluciona cualquier problema y vuelve a probar la conexión.

Forzar la sincronización con la fuente de identidades

El sistema StorageGRID sincroniza periódicamente los grupos y usuarios federados desde la fuente de identidades. Puedes forzar la sincronización si quieres habilitar o restringir los permisos de los usuarios lo más rápido posible.

Pasos

1. Ve a la página de federación de identidades.
2. Selecciona **Sync server** en la parte superior de la página.

El proceso de sincronización puede tardar un tiempo dependiendo de tu entorno.



La alerta **Error de sincronización de la federación de identidades** se activa si hay un problema al sincronizar los grupos y usuarios federados desde la fuente de identidades.

Desactivar la federación de identidades

Puedes desactivar de forma temporal o permanente la federación de identidades para grupos y usuarios. Cuando la federación de identidades está desactivada, no hay comunicación entre StorageGRID y el origen de identidad. Sin embargo, se conserva cualquier configuración que hayas realizado, lo que te permitirá volver a activar fácilmente la federación de identidades en el futuro.

Acerca de esta tarea

Antes de desactivar la federación de identidades, debes tener en cuenta lo siguiente:

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que están conectados actualmente seguirán teniendo acceso al sistema StorageGRID hasta que su sesión expire, pero no podrán iniciar sesión después de que su sesión expire.
- No se llevará a cabo la sincronización entre el sistema StorageGRID y la fuente de identidades, y no se generarán alertas para las cuentas que no se hayan sincronizado.
- La casilla de selección **Habilitar federación de identidades** aparece desactivada si el estado del inicio de sesión único (SSO) es **Habilitado** o **Modo Sandbox**. El estado del SSO en la página de inicio de sesión único debe estar **Desactivado** antes de que puedas desactivar la federación de identidades. Consulta ["Desactivar el inicio de sesión único"](#).

Pasos

1. Ve a la página de federación de identidades.
2. Desmarca la casilla **Habilitar federación de identidades**.

Guía para configurar el servidor OpenLDAP

Si deseas utilizar un servidor OpenLDAP para la federación de identidades, debes configurar determinados parámetros en el servidor OpenLDAP.



En el caso de las fuentes de identidad que no sean Active Directory o Microsoft Entra ID, StorageGRID no bloqueará automáticamente el acceso a S3 a los usuarios que hayan sido desactivados externamente. Para bloquear el acceso a S3, elimina cualquier clave de S3 del usuario o elimina al usuario de todos los grupos.

Superposiciones Memberof y refint

Los overlays memberof y refint deben estar habilitados. Para obtener más información, consulta las instrucciones para el mantenimiento de la pertenencia inversa a grupos en ["Documentación de OpenLDAP: Guía del administrador versión 2.4"](#).

Indexación

Debes configurar los siguientes atributos de 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, asegúrate de que los campos mencionados en la ayuda para Nombre de usuario estén indexados para un rendimiento óptimo.

Consulta la información sobre el mantenimiento inverso de la pertenencia a grupos en la ["Documentación de OpenLDAP: Guía del administrador versión 2.4"](#).

Gestiona grupos de inquilinos

Crea grupos para un tenant S3 en StorageGRID

Puedes gestionar los permisos de los grupos de usuarios de S3 importando grupos federados o creando grupos locales.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene ["Permiso de acceso raíz"](#).
- Si tienes previsto importar un grupo federado, tienes ["federación de identidades configurada"](#), y el grupo federado ya existe en la fuente de identidad configurada.
- Si tu cuenta de inquilino tiene el permiso **Utilizar conexión de federación de redes**, has revisado el flujo de trabajo y las consideraciones para ["clonación de grupos de inquilinos y usuarios"](#) y has iniciado sesión en la red de origen del inquilino.

Accede al asistente para crear un grupo

Como primer paso, accede al asistente para crear un grupo.

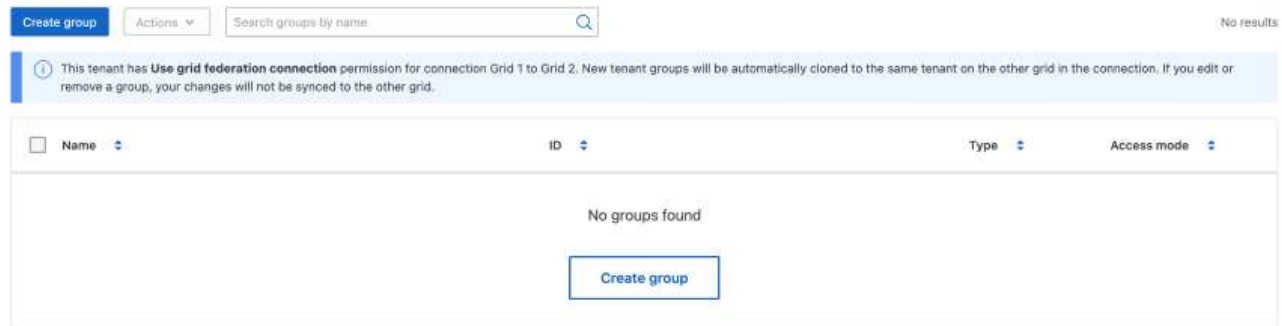
Pasos

1. Selecciona **Gestión de acceso > Grupos**.
2. Si tu cuenta de inquilino tiene el permiso **Usar conexión de federación entre redes**, comprueba que

aparezca un banner azul que indique que los nuevos grupos creados en esta grid se clonarán en el mismo inquilino de la otra grid de la conexión. Si este banner no aparece, es posible que hayas iniciado sesión en la grid de destino del inquilino.

Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.



3. Selecciona **Crear grupo**.

Elige un tipo de grupo

Puedes crear un grupo local o importar un grupo federado.

Pasos

1. Selecciona la pestaña **Grupo local** para crear un grupo local, o selecciona la pestaña **Grupo federado** para importar un grupo desde la fuente de identidades configurada previamente.

Si el inicio de sesión único (SSO) está habilitado para tu sistema StorageGRID, los usuarios que pertenezcan a grupos locales no podrán iniciar sesión en el Tenant Manager, aunque pueden usar aplicaciones cliente para gestionar los recursos del inquilino según los permisos del grupo.

2. Introduce el nombre del grupo.

- **Grupo local:** introduce tanto un nombre para mostrar como un nombre único. Puedes editar el nombre para mostrar más adelante.



Si tu cuenta de inquilino tiene el permiso **Utilizar conexión de federación de grid**, se producirá un error de clonación si ya existe el mismo **Nombre único** para el inquilino en el grid de destino.

- **Grupo federado:** introduce el nombre único. Para Active Directory, el nombre único es el nombre asociado al atributo `sAMAccountName`. Para OpenLDAP, el nombre único es el nombre asociado al atributo `uid`.

3. Selecciona **Continuar**.

Gestiona los permisos de los grupos

Los permisos de grupo controlan qué tareas pueden realizar los usuarios en el Tenant Manager y en la Tenant Management API.

Pasos

1. Para **Modo de acceso**, selecciona una de las siguientes opciones:

- **Lectura/escritura** (por defecto): los usuarios pueden iniciar sesión en Tenant Manager y gestionar la configuración del inquilino.
- **Solo lectura**: los usuarios solo pueden ver la configuración y las funciones. No pueden realizar ningún cambio ni llevar a cabo ninguna operación en el Tenant Manager o la Tenant Management API. 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 todos los ajustes y funciones seleccionados.

2. Selecciona uno o varios permisos para este grupo.

Consulta "[Permisos de gestión de inquilinos](#)".

3. Selecciona **Continuar**.

Configura la política de grupo de S3

La política de grupo determina qué permisos de acceso a S3 tendrán los usuarios.

Pasos

1. Selecciona la política que quieras 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 mediante una política de bucket. Si seleccionas esta opción, solo el usuario raíz 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 mostrar una lista de objetos y leer los datos, metadatos y etiquetas de los objetos. Cuando seleccionas esta opción, aparece en el cuadro de texto la cadena JSON para una política de grupo de solo lectura. No puedes editar esta cadena.
Acceso completo	Los usuarios de este grupo tienen acceso completo a los recursos de S3, incluidos los buckets. Cuando seleccionas esta opción, aparece en el cuadro de texto la cadena JSON de una política de grupo de acceso completo. No puedes editar esta cadena.
Mitigación de ransomware	Esta política de ejemplo se aplica a todos los buckets de este inquilino. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden eliminar de forma permanente objetos de los buckets que tengan habilitado el control de versiones de objetos. Los usuarios de Tenant Manager que tengan el permiso Manage all buckets pueden anular esta política de grupo. Limita el permiso Manage all buckets a usuarios de confianza y utiliza la autenticación multifactor (MFA) donde esté disponible.

Política de grupo	Descripción
Personalizado	A los usuarios del grupo se les conceden los permisos que especifiques en el cuadro de texto.

- Si has seleccionado **Personalizado**, introduce la política de grupo. Cada política de grupo tiene un límite de tamaño de 5,120 bytes. Debes introducir una cadena válida con formato JSON.

Para obtener información detallada sobre las políticas de grupo, incluida la sintaxis del lenguaje y ejemplos, consulta ["Ejemplos de políticas de grupo"](#).

- Si vas a crear un grupo local, selecciona **Continuar**. Si vas a crear un grupo federado, selecciona **Crear grupo** y **Finalizar**.

Agregar usuarios (solo grupos locales)

Puedes guardar el grupo sin añadir usuarios o puedes añadir opcionalmente cualquier usuario local que ya exista.



Si tu cuenta de inquilino tiene el permiso **Utilizar conexión de federación entre redes**, los usuarios que selecciones al crear un grupo local en la grid de origen no se incluyen cuando el grupo se clona en la grid de destino. Por esta razón, no selecciones usuarios al crear el grupo. En su lugar, selecciona el grupo al crear los usuarios.

Pasos

- Si lo deseas, selecciona uno o más usuarios locales para este grupo.
- Selecciona **Crear grupo** y **Finalizar**.

El grupo que has creado aparece en la lista de grupos.

Si tu cuenta de inquilino tiene el permiso **Utilizar conexión de federación de grid** y te encuentras en el grid de origen del inquilino, el nuevo grupo se clona en el grid de destino del inquilino. **Éxito** aparece como el **Estado de la clonación** en la sección de resumen de la página de detalles del grupo.

Permisos de gestión de tenants de StorageGRID

Antes de crear un grupo de inquilinos, piensa qué permisos quieres asignar a ese grupo. Los permisos de gestión de inquilinos determinan qué tareas pueden realizar los usuarios mediante el Tenant Manager o la Tenant Management API. Un usuario puede pertenecer a uno o varios grupos. Los permisos se acumulan si un usuario pertenece a varios grupos.

Para iniciar sesión en Tenant Manager o usar la API de gestión de inquilinos, los usuarios deben pertenecer a un grupo que tenga al menos un permiso. Todos los usuarios que pueden iniciar sesión pueden realizar las siguientes tareas:

- Ver el panel de control
- Cambiar su propia contraseña (para usuarios locales)

En todos los permisos, la configuración del modo de acceso del grupo determina si los usuarios pueden cambiar la configuración y realizar operaciones o si solo pueden ver la configuración y las 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 todos los ajustes y funciones seleccionados.

Puedes asignar los siguientes permisos a un grupo.

Permiso	Descripción	Detalles
Acceso a raíz	Ofrece acceso completo al Tenant Manager y a la Tenant Management API.	
Gestiona tus propias credenciales de S3	Permite a los usuarios crear y eliminar sus propias claves de acceso a S3.	Los usuarios que no tengan este permiso no ven la opción de menú ALMACENAMIENTO (S3) > Mis claves de acceso a S3 .
Ver todos los buckets	Permite a los usuarios ver todos los buckets y las configuraciones de los buckets.	Los usuarios que no tengan ni el permiso «View all buckets» ni el permiso «Manage all buckets» no ven la opción de menú Buckets . Este permiso queda reemplazado por el permiso Manage all buckets. No afecta a las políticas de grupo o de buckets de S3 que usan los clientes de S3 o la S3 Console.
Gestionar todos los buckets	Permite a los usuarios utilizar el Tenant Manager y la Tenant Management API para crear y eliminar buckets de S3 y gestionar la configuración de todos los buckets de S3 en la cuenta de inquilino, independientemente de las políticas de bucket de S3 o de grupo.	Los usuarios que no tengan ni el permiso «View all buckets» ni el permiso «Manage all buckets» no ven la opción de menú Buckets . Este permiso sustituye al permiso View all buckets. No afecta a las políticas de grupo o de buckets de S3 que usan los clientes de S3 o la S3 Console.
Gestionar endpoints	Permite a los usuarios utilizar Tenant Manager o la API de gestión de inquilinos para crear o editar puntos finales de servicios de la plataforma, que se utilizan como destino para los servicios de plataforma de StorageGRID.	Los usuarios que no tengan este permiso no ven la opción de menú Platform services endpoints .
Utiliza la pestaña S3 Console	Cuando se combina con el permiso «Ver todos los buckets» o «Gestionar todos los buckets», permite a los usuarios ver y gestionar objetos desde la pestaña «Consola de S3» de la página de detalles de un bucket.	

Gestiona grupos de inquilinos StorageGRID

Gestiona tus grupos de inquilinos según sea necesario para ver, editar o duplicar un

grupo y más.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene ["Permiso de acceso raíz"](#).

Ver o editar grupo

Puedes consultar y editar la información básica y los detalles de cada grupo.

Pasos

1. Selecciona **Gestión de acceso > Grupos**.
2. Revisa la información que aparece en la página Grupos, donde se muestra la información básica de todos los grupos locales y federados de esta cuenta de tenant.

Si la cuenta del inquilino tiene el permiso **Utilizar conexión de federación de cuadrículas** y estás visualizando grupos en la cuadrícula de origen del inquilino:

- Un mensaje en un banner indica que, si editas o eliminas un grupo, tus cambios no se sincronizarán con la otra cuadrícula.
 - Si es necesario, un mensaje en la barra superior indica si los grupos no se clonaron en el inquilino de la grid de destino. Puedes [volver a intentar clonar un grupo](#) los que fallaron.
3. Si quieres cambiar el nombre del grupo:
 - a. Selecciona la casilla para el grupo.
 - b. Selecciona **Acciones > Editar nombre del grupo**.
 - c. Introduce el nuevo nombre.
 - d. Selecciona **Guardar cambios**.
 4. Si quieres ver más detalles o hacer modificaciones adicionales, haz una de las siguientes cosas:
 - Selecciona el nombre del grupo.
 - Marca la casilla de selección del grupo y selecciona **Acciones > Ver detalles del grupo**.
 5. Consulta la sección «Resumen», que muestra la siguiente información para cada grupo:
 - Nombre para mostrar
 - Nombre único
 - Tipo
 - Modo de acceso
 - Permisos
 - Política de S3
 - Número de usuarios en este grupo
 - Campos adicionales si la cuenta del inquilino tiene el permiso **Usar conexión de federación de cuadrículas** y estás viendo el grupo en la cuadrícula de origen del inquilino:
 - Estado de la clonación, ya sea **Éxito** o **Fracaso**
 - Aparece un banner azul que indica que, si editas o eliminas este grupo, tus cambios no se sincronizarán con la otra grid.

6. Modifica la configuración del grupo según sea necesario. Consulta "[Crear grupos para un inquilino de S3](#)" para ver detalles sobre qué debes ingresar.
 - a. En la sección «Descripción general», cambia el nombre que se muestra seleccionando el nombre o el icono de edición .
 - b. En la pestaña **Permisos de grupo**, actualiza los permisos y selecciona **Guardar cambios**.
 - c. En la pestaña **política de grupo**, haz cualquier cambio y selecciona **Guardar cambios**.

Si lo deseas, selecciona una política de grupo de S3 diferente o introduce la cadena JSON para una política personalizada, según sea necesario.
7. Para añadir uno o más usuarios locales existentes al grupo:
 - a. Selecciona la pestaña Usuarios.



- b. Selecciona **Add users**.
 - c. Selecciona los usuarios existentes que quieras añadir y selecciona **Add users**.

Aparece un mensaje de éxito en la esquina superior derecha.
8. Para eliminar usuarios locales del grupo:
 - a. Selecciona la pestaña Usuarios.
 - b. Selecciona **Eliminar usuarios**.
 - c. Selecciona los usuarios que quieras eliminar y selecciona **Eliminar usuarios**.

Aparece un mensaje de éxito en la esquina superior derecha.
9. Confirma que seleccionaste **Guardar cambios** en cada sección que cambiaste.

Duplicar grupo

Puedes duplicar un grupo ya existente para crear nuevos grupos más rápido.



Si tu cuenta de inquilino tiene el permiso **Utilizar conexión de federación de redes** y duplicas un grupo de la red de origen del inquilino, el grupo duplicado se clonará en la red de destino del inquilino.

Pasos

1. Selecciona **Gestión de acceso > Grupos**.
2. Marca la casilla de verificación del grupo que quieras duplicar.
3. Selecciona **Acciones > Duplicar grupo**.

4. Consulta ["Crear grupos para un inquilino de S3"](#) para obtener más información sobre qué datos debes introducir.
5. Selecciona **Crear grupo**.

Reintentar la clonación del grupo

Para volver a intentar un clon que falló:

1. Selecciona cada grupo en el que aparezca (*Cloning failed*) debajo del nombre del grupo.
2. Selecciona **Acciones > Clonar grupos**.
3. Consulta el estado de la operación de clonación en la página de detalles de cada grupo que estés clonando.

Para obtener más información, consulta ["Clonar grupos de inquilinos y usuarios"](#).

Eliminar uno o varios grupos

Puedes eliminar uno o más grupos. Los usuarios que pertenezcan únicamente a un grupo que se elimine ya no podrán iniciar sesión en el Tenant Manager ni usar la cuenta de inquilino.



Si tu cuenta de inquilino tiene el permiso **Use grid federation connection** y eliminas un grupo, StorageGRID no eliminará el grupo correspondiente en el otro grid. Si necesitas mantener esta información sincronizada, debes eliminar el mismo grupo de ambos grids.

Pasos

1. Selecciona **Gestión de acceso > Grupos**.
2. Marca la casilla de cada grupo que quieras eliminar.
3. Selecciona **Acciones > Eliminar grupo** o **Acciones > Eliminar grupos**.

Aparece un cuadro de diálogo de confirmación.

4. Selecciona **Eliminar grupo** o **Eliminar grupos**.

Configura AssumeRole

Antes de empezar

Debes ser administrador para configurar AssumeRole.

Acerca de esta tarea

Para configurar AssumeRole, crea el grupo de destino que se va a asumir, si el grupo no existe ya. Edita la política de S3 del grupo para especificar las acciones permitidas al asumir este grupo. Edita la política de confianza de S3 del grupo para especificar los usuarios de confianza a los que se les permite asumir el grupo con la API AssumeRole.

Las credenciales de seguridad temporales creadas al asumir este grupo son válidas durante un periodo de tiempo limitado. La sesión dura entre 15 minutos y 12 horas, y la sesión predeterminada es de 1 hora. Cuando eliminas al usuario de la política de confianza de S3 del grupo, el usuario ya no puede asumir este grupo.

Pasos

1. Selecciona **Gestión de acceso > Grupos**.

2. Haz clic en el nombre del grupo.
3. Selecciona la pestaña **S3 trust policy**.
4. Agrega tu política de confianza de S3, incluyendo una lista de usuarios que pueden realizar AssumeRole.
5. Selecciona **Guardar cambios**.
6. Selecciona la pestaña **política de grupo de S3**.
7. Modifica la política de S3 para especificar únicamente las acciones de S3 necesarias para los usuarios de confianza añadidos en la política de confianza de S3 de este grupo.
8. Selecciona **Guardar cambios**.

Ejemplo de una política de confianza de S3 de AssumeRole

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": [
          "urn:sgws:identity::1234567890:user/user1",
          "arn:aws:iam::1234567890:user/user2"
        ]
      }
    }
  ]
}
```

Una vez completada la configuración, los usuarios incluidos en la política de confianza de S3 pueden realizar AssumeRole y recibir credenciales. Los permisos finales se determinan mediante la política de grupo, la política de bucket y la política de sesión. Para obtener más información, consulta ["Usa políticas de acceso"](#).

Gestiona los usuarios inquilinos de StorageGRID

Puedes crear usuarios locales y asignarlos a grupos locales para determinar a qué funciones pueden acceder estos usuarios. También puedes importar usuarios federados. El Tenant Manager incluye un usuario local predefinido, llamado "root". Aunque puedes añadir y eliminar usuarios locales, no puedes eliminar al usuario raíz.



Si el inicio de sesión único (SSO) está habilitado en tu sistema StorageGRID, los usuarios locales no podrán iniciar sesión en el Tenant Manager ni en la API de gestión de inquilinos, aunque sí podrán utilizar aplicaciones cliente para acceder a los recursos del inquilino, en función de los permisos de grupo.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene ["Permiso de acceso raíz"](#).

- Si tu cuenta de inquilino tiene el permiso **Utilizar conexión de federación de redes**, has revisado el flujo de trabajo y las consideraciones para "[clonación de grupos de inquilinos y usuarios](#)" y has iniciado sesión en la red de origen del inquilino.

Crear un usuario local

Puedes crear un usuario local y asignarlo a uno o varios grupos locales para controlar sus permisos de acceso.

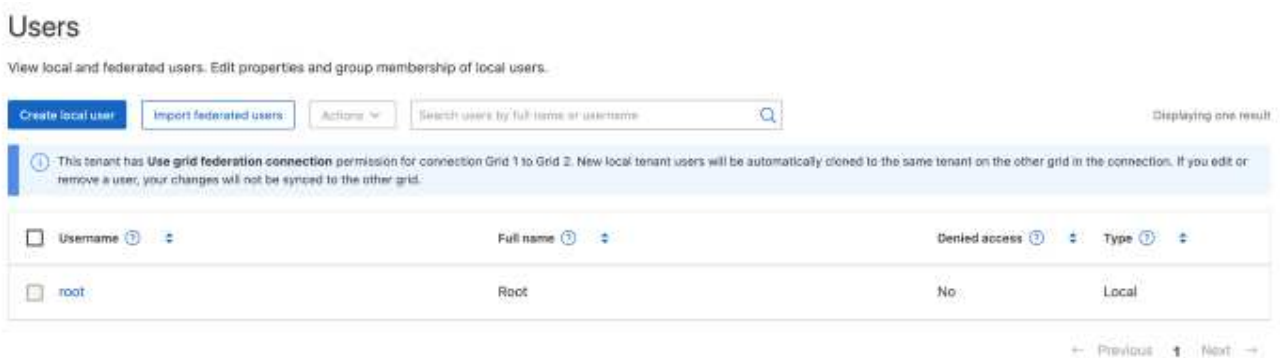
Los usuarios de S3 que no pertenecen a ningún grupo no tienen permisos de gestión ni se les aplican políticas de grupo de S3. Es posible que estos usuarios tengan acceso al bucket de S3 concedido a través de una política de bucket.

Accede al asistente para crear un usuario

Pasos

1. Selecciona **Gestión de acceso > Usuarios**.

Si tu cuenta de inquilino tiene el permiso **Usar conexión de federación de redes**, un banner azul indica que esta es la red de origen del inquilino. Cualquier usuario local que crees en esta red se clonará en la otra red de la conexión.



2. Selecciona **Crear usuario**.

Introduce tus datos de acceso

Pasos

1. En el paso **Introducir credenciales de usuario**, completa los siguientes campos.

Campo	Descripción
Nombre completo	El nombre completo de este usuario, por ejemplo, el nombre y el apellido de una persona o el nombre de una aplicación.
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 tu cuenta de inquilino tiene el permiso Use grid federation connection , se producirá un error de clonación si ya existe el mismo Username para el inquilino en la red de destino.

Campo	Descripción
Contraseña y confirmar contraseña	La contraseña que el usuario usará inicialmente al iniciar sesión.
Denegar el acceso	Selecciona Sí para impedir que este usuario inicie sesión en la cuenta del inquilino, aunque siga perteneciendo a uno o varios grupos. Por ejemplo, selecciona Sí para suspender temporalmente la capacidad de un usuario para iniciar sesión.

2. Selecciona **Continuar**.

Asignar a grupos

Pasos

1. Asigna al usuario a uno o más grupos locales para determinar qué tareas puede realizar.

La asignación de un usuario a grupos es opcional. Si lo prefieres, puedes seleccionar usuarios al crear o editar grupos.

Los usuarios que no pertenezcan a ningún grupo no tendrán permisos de gestión. Los permisos son acumulativos. Los usuarios tendrán todos los permisos de todos los grupos a los que pertenezcan. Consulta "[Permisos de gestión de inquilinos](#)".

2. Selecciona **Crear usuario**.

Si tu cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y estás en el grid de origen del inquilino, el nuevo usuario local se clona en el grid de destino del inquilino. **Éxito** aparece como el **Estado de clonación** en la sección de información general de la página de detalles del usuario.

3. Selecciona **Finalizar** para volver a la página de Usuarios.

Ver o editar usuario local

Pasos

1. Selecciona **Gestión de acceso > Usuarios**.
2. Revisa la información que aparece en la página Usuarios, donde se muestra la información básica de todos los usuarios locales y federados de esta cuenta de inquilino.

Si la cuenta del inquilino tiene el permiso **Utilizar conexión de federación de redes** y estás viendo al usuario en la red de origen del inquilino:

- Un mensaje en la barra superior indica que si editas o eliminas un usuario, tus cambios no se sincronizarán con la otra cuadrícula.
- Si es necesario, un mensaje en la barra superior indica si los usuarios no se clonaron en el tenant de la grid de destino. Puedes [Vuelve a intentar clonar un usuario que falló](#).

3. Si quieres cambiar el nombre completo del usuario:
 - a. Marca la casilla de selección para el usuario.
 - b. Selecciona **Acciones > Editar nombre completo**.

- c. Introduce el nuevo nombre.
 - d. Selecciona **Guardar cambios**.
4. Si quieres ver más detalles o hacer modificaciones adicionales, haz una de las siguientes cosas:
- Selecciona el nombre de usuario.
 - Marca la casilla de selección correspondiente al usuario y selecciona **Acciones > Ver detalles del usuario**.
5. Consulta la sección «Resumen», que muestra la siguiente información para cada usuario:
- Nombre completo
 - Nombre de usuario
 - Tipo de usuario
 - Acceso denegado
 - Modo de acceso
 - Pertenencia al grupo
 - Campos adicionales si la cuenta del cliente tiene el permiso **Usar conexión de federación de cuadrículas** y estás viendo al usuario en la cuadrícula de origen del cliente:
 - Estado de la clonación, ya sea **Éxito** o **Fracaso**
 - Un banner azul que indica que, si editas este usuario, tus cambios no se sincronizarán con la otra grid.
6. Modifica la configuración de usuario según sea necesario. Consulta [Crear usuario local](#) para ver detalles sobre qué debes ingresar.
- a. En la sección «Descripción general», cambia el nombre completo seleccionando el nombre o el icono de edición .
- No puedes cambiar el nombre de usuario.
- b. En la pestaña **Contraseña**, cambia la contraseña del usuario y selecciona **Guardar cambios**.
 - c. En la pestaña **Acceso**, selecciona **No** para permitir que el usuario inicie sesión o selecciona **Sí** para impedir que inicie sesión. Luego, selecciona **Guardar cambios**.
 - d. En la pestaña **Claves de acceso**, selecciona **Crear clave** y sigue las instrucciones para "[crear las claves de acceso a S3 de otro usuario](#)".
 - e. En la pestaña **Grupos**, selecciona **Editar grupos** para agregar al usuario a grupos o quitarlo de ellos. A continuación, selecciona **Guardar cambios**.
7. Confirma que seleccionaste **Guardar cambios** en cada sección que cambiaste.

Importar usuarios federados

Puedes importar uno o varios usuarios federados, hasta un máximo de 100 usuarios, directamente en la página de Usuarios.

Pasos

1. Selecciona **Gestión de acceso > Usuarios**.
2. Selecciona **Importar usuarios federados**.
3. Introduce el UUID o el nombre de usuario de uno o varios usuarios federados.

Si hay varias entradas, añade cada UUID o nombre de usuario en una nueva línea.

4. Selecciona **Importar**.

Si la importación al campo «Usuarios» falla para uno o varios usuarios, realiza los siguientes pasos:

- Despliega **Usuarios no importados** y selecciona **Copiar usuarios**.
- Vuelve a intentar la importación seleccionando **Anterior** y pegando los usuarios copiados en el cuadro de diálogo **Import federated users**.

Después de que cierres el cuadro de diálogo **Importar usuarios federados**, la información de los usuarios federados importados correctamente se muestra en la página Usuarios.

Usuario local duplicado

Puedes duplicar un usuario local para crear un nuevo usuario más rápido.



Si tu cuenta de inquilino tiene el permiso **Utilizar conexión de federación de grid** y duplicas un usuario de la grid de origen del inquilino, el usuario duplicado se clonará en la grid de destino del inquilino.

Pasos

- Selecciona **Gestión de acceso > Usuarios**.
- Marca la casilla correspondiente al usuario que quieras duplicar.
- Selecciona **Acciones > Duplicar usuario**.
- Consulta [Crear usuario local](#) para obtener más información sobre qué datos debes introducir.
- Selecciona **Crear usuario**.

Volver a intentar clonar el usuario

Para volver a intentar un clon que falló:

- Selecciona cada usuario que indique (*Error al clonar*) debajo del nombre de usuario.
- Selecciona **Acciones > Clonar usuarios**.
- Consulta el estado de la operación de clonación en la página de detalles de cada usuario que estés clonando.

Para obtener más información, consulta "[Clonar grupos de inquilinos y usuarios](#)".

Eliminar uno o varios usuarios locales

Puedes eliminar definitivamente a uno o varios usuarios locales que ya no necesiten acceder a la cuenta de inquilino de StorageGRID.



Si tu cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y eliminas a un usuario local, StorageGRID no eliminará al usuario correspondiente en el otro grid. Si necesitas mantener esta información sincronizada, debes eliminar al mismo usuario de ambos grids.



Debes usar la fuente de identidad federada para eliminar usuarios federados.

Pasos

1. Selecciona **Gestión de acceso > Usuarios**.
2. Marca la casilla de selección de cada usuario que quieras eliminar.
3. Selecciona **Actions > Delete user** o **Actions > Delete users**.

Aparece un cuadro de diálogo de confirmación.

4. Selecciona **Eliminar usuario** o **Eliminar usuarios**.

Gestiona claves de acceso de S3

Gestiona claves de acceso S3 en StorageGRID

Cada usuario de una cuenta de inquilino de S3 debe disponer de 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 de S3 se pueden gestionar de la siguiente manera:

- Los usuarios que tengan el permiso **Gestionar tus propias credenciales de S3** pueden crear o eliminar sus propias claves de acceso a S3.
- Los usuarios que tienen el permiso **Root access** pueden gestionar las claves de acceso para la cuenta raíz de S3 y para todos los demás usuarios. Las claves de acceso de Root access proporcionan acceso completo a todos los buckets y objetos del inquilino, a menos que una política de bucket lo deshabilite explícitamente.

StorageGRID admite la autenticación mediante Signature Version 2 y Signature Version 4. No se permite el acceso entre cuentas a menos que una política de bucket lo habilite explícitamente.

Crea tus propias claves de acceso S3 en StorageGRID

Si estás usando un inquilino de S3 y tienes el permiso adecuado, puedes crear tus propias claves de acceso de S3. Debes tener una clave de acceso para acceder a tus buckets y objetos.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Perteneces a un grupo de usuarios que tiene ["Gestiona tus propias credenciales de S3 o el permiso de acceso de usuario raíz"](#).

Acerca de esta tarea

Puedes crear una o más claves de acceso de S3 que te permitan crear y gestionar buckets para tu cuenta de inquilino. Después de crear una nueva clave de acceso, actualiza la aplicación con tu nuevo ID de clave de acceso y la clave de acceso secreta. Por seguridad, no crees más claves de las que necesites y elimina las que no estés usando. Si solo tienes una clave y está a punto de caducar, crea una nueva clave antes de que caduque la anterior y, a continuación, elimina la antigua.

Cada clave puede tener un tiempo de expiración específico o no tener expiración. Sigue estas pautas para el tiempo de expiración:

- Establece un tiempo de expiración para tus claves para limitar tu acceso a un período de tiempo determinado. Configurar un tiempo de expiración corto puede ayudarte a reducir el riesgo si tu ID de clave de acceso y tu clave de acceso secreta se exponen accidentalmente. Las claves expiradas se eliminan automáticamente.
- Si el riesgo de seguridad en tu entorno es bajo y no necesitas crear claves nuevas periódicamente, no tienes que establecer una fecha de caducidad para tus claves. Si más adelante decides crear claves nuevas, elimina las claves antiguas manualmente.



Se puede acceder a los buckets y objetos de S3 de tu cuenta utilizando el access key ID y la secret access key que se muestran para tu cuenta en el Tenant Manager. Por este motivo, protege las claves de acceso como lo harías con una contraseña. Renueva las claves de acceso periódicamente, elimina de tu cuenta cualquier clave que no utilices y nunca las compartas con otros usuarios.

Pasos

1. Selecciona **STORAGE (S3) > Mis claves de acceso**.

Aparece la página «Mis claves de acceso» y se muestran todas las claves de acceso existentes.

2. Selecciona **Crear clave**.
3. Debe realizar una de las siguientes acciones:
 - Selecciona **No establecer una hora de caducidad** para crear una clave que no caduque. (Predeterminado)
 - Selecciona **Establecer una fecha de caducidad** y configura la fecha y la hora de caducidad.



La fecha de caducidad puede ser como máximo de cinco años a partir de la fecha actual. La hora de caducidad puede ser como mínimo de un minuto a partir de la hora actual.

4. Selecciona **Crear clave de acceso**.

Aparece el cuadro de diálogo «Clave de acceso para descargas», donde se muestra tu ID de clave de acceso y tu clave de acceso secreta.

5. Copia el ID de la clave de acceso y la clave de acceso secreta en un lugar seguro, o selecciona **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 cierres este cuadro de diálogo hasta que hayas copiado o descargado esta información. No podrás copiar ni descargar las claves después de que se haya cerrado el cuadro de diálogo.

6. Selecciona **Finalizar**.

La nueva clave aparece en la página My access keys.

7. Si tu cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, de manera opcional puedes usar la API de gestión de inquilinos para clonar manualmente las claves de acceso de S3 desde el inquilino en el grid de origen al inquilino en el grid de destino. Consulta ["Clonar claves de acceso a S3 mediante la API"](#).

Consulta tus claves de acceso a S3 en StorageGRID

Si estás usando un inquilino de S3 y tienes el "[permiso correspondiente](#)", puedes ver una lista de tus claves de acceso de S3. Puedes ordenar la lista por fecha de caducidad para determinar qué claves caducarán pronto. Según sea necesario, puedes "[crear nuevas claves](#)" o "[eliminar claves](#)" que ya no estés usando.



Se puede acceder a los buckets y objetos de S3 de tu cuenta utilizando el access key ID y la secret access key que se muestran para tu cuenta en el Tenant Manager. Por este motivo, protege las claves de acceso como lo harías con una contraseña. Renueva las claves de acceso periódicamente, elimina de tu cuenta cualquier clave que no utilices y nunca las compartas con otros usuarios.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un "[navegador web compatible](#)".
- Pertenece a un grupo de usuarios que tiene el permiso «Gestionar tus propias credenciales de S3» "[permiso](#)".

Pasos

1. Selecciona **STORAGE (S3) > Mis claves de acceso**.
2. En la página «Mis claves de acceso», ordena las claves de acceso existentes por **tiempo de expiración o ID de la clave de acceso**.
3. Según sea necesario, crea nuevas claves o elimina aquellas que ya no utilices.

Si creas nuevas claves antes de que caduquen las existentes, puedes empezar a usar las nuevas claves sin perder temporalmente el acceso a los objetos de la cuenta.

Las claves caducadas se eliminan automáticamente.

Elimina tus propias claves de acceso a S3 en StorageGRID

Si utilizas un inquilino de S3 y tienes los permisos adecuados, puedes eliminar tus propias claves de acceso de S3. Después de eliminar una clave de acceso, ya no se puede usar para acceder a los objetos y buckets en la cuenta del inquilino.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un "[navegador web compatible](#)".
- Tienes el "[Gestiona tus propios permisos de credenciales de S3](#)".



Se puede acceder a los buckets y objetos de S3 de tu cuenta utilizando el access key ID y la secret access key que se muestran para tu cuenta en el Tenant Manager. Por este motivo, protege las claves de acceso como lo harías con una contraseña. Renueva las claves de acceso periódicamente, elimina de tu cuenta cualquier clave que no utilices y nunca las compartas con otros usuarios.

Pasos

1. Selecciona **STORAGE (S3) > Mis claves de acceso**.
2. En la página «Mis claves de acceso», marca la casilla correspondiente a cada clave de acceso que

quieras eliminar.

3. Selecciona **Eliminar clave**.

4. En el cuadro de diálogo de confirmación, selecciona **Delete key**.

Aparece un mensaje de confirmación en la esquina superior derecha de la página.

Crea las claves de acceso S3 de otro usuario en StorageGRID

Si utilizas un inquilino de S3 y tienes el permiso adecuado, puedes crear claves de acceso S3 para otros usuarios, como aplicaciones que necesitan acceso a buckets y objetos.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene ["Permiso de acceso raíz"](#).

Acerca de esta tarea

Puedes crear una o varias claves de acceso de S3 para otros usuarios para que puedan crear y gestionar buckets para su cuenta de inquilino. Después de crear una nueva clave de acceso, actualiza la aplicación con el nuevo ID de clave de acceso y la clave de acceso secreta. Por seguridad, no crees más claves de las que el usuario necesite y elimina las claves que no se estén usando. Si solo tienes una clave y está a punto de caducar, crea una nueva antes de que caduque la antigua y luego elimina la antigua.

Cada clave puede tener un tiempo de expiración específico o no tener expiración. Sigue estas pautas para el tiempo de expiración:

- Establece un plazo de caducidad para las claves para limitar el acceso del usuario a un periodo de tiempo determinado. Establecer un plazo de caducidad corto puede ayudar a reducir el riesgo si el ID de la clave de acceso y la clave secreta de acceso se exponen accidentalmente. Las claves caducadas se eliminan automáticamente.
- Si el riesgo de seguridad en tu entorno es bajo y no necesitas crear nuevas claves periódicamente, no tienes que establecer un plazo de caducidad para las claves. Si más adelante decides crear nuevas claves, elimina las antiguas manualmente.



Puedes acceder a los buckets y objetos de 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 Tenant Manager. Por este motivo, protege las claves de acceso como lo harías con una contraseña. Rota las claves de acceso de forma periódica, elimina de la cuenta las claves que no utilices y no las compartas nunca con otros usuarios.

Pasos

1. Selecciona **Gestión de acceso > Usuarios**.

2. Selecciona el usuario cuyas claves de acceso a S3 deseas gestionar.

Aparece la página de detalles del usuario.

3. Selecciona **Teclas de acceso** y luego selecciona **Crear clave**.

4. Debe realizar una de las siguientes acciones:

- Selecciona **No establecer fecha de caducidad** para crear una clave que no caduque.

(Predeterminado)

- Selecciona **Establecer una fecha de caducidad** y configura la fecha y la hora de caducidad.



La fecha de caducidad puede ser como máximo de cinco años a partir de la fecha actual. La hora de caducidad puede ser como mínimo de un minuto a partir de la hora actual.

5. Selecciona **Crear clave de acceso**.

Aparece el cuadro de diálogo «Download access key», en el que se muestran el access key ID y el secret access key.

6. Copia el ID de la clave de acceso y la clave de acceso secreta en un lugar seguro, o selecciona **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 cierres este cuadro de diálogo hasta que hayas copiado o descargado esta información. No podrás copiar ni descargar las claves después de que se haya cerrado el cuadro de diálogo.

7. Selecciona **Finalizar**.

La nueva clave aparece en la pestaña Claves de acceso de la página de detalles del usuario.

8. Si tu cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, de manera opcional puedes usar la API de gestión de inquilinos para clonar manualmente las claves de acceso de S3 desde el inquilino en el grid de origen al inquilino en el grid de destino. Consulta ["Clonar claves de acceso a S3 mediante la API"](#).

Ver las claves de acceso S3 de otro usuario en StorageGRID

Si utilizas un inquilino de S3 y tienes los permisos adecuados, puedes ver las claves de acceso de S3 de otro usuario. Puedes ordenar la lista por tiempo de expiración para saber qué claves expirarán pronto. Cuando lo necesites, puedes crear nuevas claves y eliminar las que ya no estén en uso.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).



Puedes acceder a los buckets y objetos de 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 Tenant Manager. Por este motivo, protege las claves de acceso como lo harías con una contraseña. Rota las claves de acceso de forma periódica, elimina de la cuenta las claves que no utilices y no las compartas nunca con otros usuarios.

Pasos

1. Selecciona **Gestión de acceso > Usuarios**.
2. En la página «Usuarios», selecciona el usuario cuyas claves de acceso a S3 quieras consultar.
3. En la página «Detalles del usuario», selecciona **Access keys**.

4. Ordena las claves por **tiempo de expiración** o **ID de la clave de acceso**.
5. Según sea necesario, crea nuevas claves y elimina manualmente las claves que ya no estén en uso.

Si creas nuevas claves antes de que caduquen las existentes, el usuario puede empezar 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 a S3 de otro usuario"](#)
- ["Eliminar las claves de acceso a S3 de otro usuario"](#)

Eliminar las claves de acceso S3 de otro usuario en StorageGRID

Si estás usando un inquilino de S3 y tienes los permisos adecuados, puedes eliminar las claves de acceso de S3 de otro usuario. Después de eliminar una clave de acceso, ya no se podrá usar para acceder a los objetos y buckets de la cuenta del inquilino.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).



Puedes acceder a los buckets y objetos de 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 Tenant Manager. Por este motivo, protege las claves de acceso como lo harías con una contraseña. Rota las claves de acceso de forma periódica, elimina de la cuenta las claves que no utilices y no las compartas nunca con otros usuarios.

Pasos

1. Selecciona **Gestión de acceso > Usuarios**.
2. En la página «Usuarios», selecciona el usuario cuyas claves de acceso a S3 quieras gestionar.
3. En la página «Detalles del usuario», selecciona **Claves de acceso** y, a continuación, marca la casilla correspondiente a cada clave de acceso que desees eliminar.
4. Selecciona **Acciones > Eliminar clave seleccionada**.
5. En el cuadro de diálogo de confirmación, selecciona **Delete key**.

Aparece un mensaje de confirmación en la esquina superior derecha de la página.

Gestiona buckets de S3

Crear un bucket S3 de StorageGRID

Puedes utilizar el Tenant Manager para crear buckets de S3 para datos de objetos.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene acceso Root o la autorización Manage all buckets ["permiso"](#).

Estos permisos anulan la configuración de permisos en las políticas de grupo o de bucket.



Los permisos para establecer o modificar las propiedades de S3 Object Lock de buckets u objetos se pueden conceder mediante ["política de bucket o política de grupo"](#).

- Si tienes previsto habilitar S3 Object Lock para un bucket, un administrador de la grid ha habilitado la configuración global de S3 Object Lock para el sistema StorageGRID y has revisado los requisitos para los buckets y objetos de S3 Object Lock.
- Si cada inquilino va a tener 5,000 buckets, cada Storage Node en la grid tiene un mínimo de 64 GB de RAM.



Cada grid puede tener un máximo de 100,000 buckets, incluyendo ["cubos de rama"](#).

Accede al asistente

Pasos

1. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.
2. Selecciona **Create bucket**.

Introduce los datos

Pasos

1. Introduce los datos del bucket.

Campo	Descripción
Nombre del bucket	Un nombre para el bucket que cumpla estas reglas: • Debe ser único en cada sistema StorageGRID (no solo 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 usar letras minúsculas, números y guiones. • No debe contener puntos en las solicitudes de tipo virtual hosted style. Los puntos provocarán problemas con la verificación del certificado comodín del servidor. Para más información, consulta el "Documentación de Amazon Web Services (AWS) sobre las reglas de nomenclatura de los buckets". Nota: No puedes cambiar el nombre del bucket después de crearlo.

Campo	Descripción
Región	La región del bucket. Tu administrador de StorageGRID gestiona las regiones disponibles. La región de un bucket puede afectar a la política de protección de datos que se aplica a los objetos. Por defecto, todos los buckets se crean en la <code>us-east-1</code> región. Si la región por defecto está configurada en una región distinta de <code>us-east-1</code>, esta otra región aparecerá seleccionada inicialmente en el menú desplegable. Nota: No puedes cambiar la región después de crear el bucket.

2. Selecciona **Continuar**.

Gestiona la configuración

Pasos

1. Si lo deseas, activa el control de versiones de objetos para el bucket.

Activa el versionado de objetos si quieres almacenar cada versión de cada objeto en este bucket. Después podrás recuperar las versiones anteriores de un objeto según lo necesites.

Debes activar el control de versiones de los objetos si:

- El bucket se utilizará para la replicación entre grids.
- Quieres crear un "bucket de rama" desde este bucket.

2. Si la configuración global de S3 Object Lock está activada, puedes activar opcionalmente S3 Object Lock para el bucket para almacenar objetos usando un modelo de escritura única y lectura múltiple (WORM).

Activa S3 Object Lock para un bucket solo si necesitas conservar los objetos durante un periodo de tiempo fijo, por ejemplo, para cumplir con ciertos requisitos normativos. S3 Object Lock es una configuración permanente que te ayuda a evitar que los objetos se eliminen o se sobrescriban durante un periodo de tiempo fijo o de forma indefinida.



Una vez habilitada la configuración de S3 Object Lock para un bucket, no se puede deshabilitar. Cualquier persona con los permisos adecuados puede añadir objetos a este bucket que no se pueden modificar. Es posible que no puedas eliminar estos objetos ni el propio bucket.

Si activas S3 Object Lock para un bucket, el control de versiones del bucket se activa automáticamente.

3. Si seleccionaste **Habilitar S3 Object Lock**, puedes habilitar opcionalmente la **retención predeterminada** para este bucket.



Tu administrador de grid debe darte permiso para "utilizar las funciones específicas de S3 Object Lock".

Cuando la **retención predeterminada** está habilitada, los nuevos objetos que añadas al bucket se protegerán automáticamente para evitar que se eliminen o se sobrescriban. El ajuste de **retención predeterminada** no se aplica a los objetos que tienen sus propios periodos de retención.

- a. Si la opción **Retención predeterminada** está activada, especifica un **modo de retención predeterminado** para el depósito.

Modo de retención predeterminado	Descripción
Gobernanza	• Los usuarios con el permiso <code>s3:BypassGovernanceRetention</code> pueden usar el encabezado de solicitud <code>x-amz-bypass-governance-retention: true</code> para omitir la configuración de retención. • Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su <code>retain-until-date</code>. • Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.
Cumplimiento normativo	• El objeto no se puede eliminar hasta que se alcance su fecha de retención. • La fecha límite de retención del objeto se puede ampliar, pero no se puede reducir. • La fecha de retención del objeto no se puede eliminar hasta que se alcance dicha fecha. Nota: El administrador de tu grid debe autorizarte a utilizar el modo de cumplimiento.

- b. Si la opción **Retención predeterminada** está activada, especifica el **período de retención predeterminado** para el bucket.

El **período de retención predeterminado** indica durante cuánto tiempo deben conservarse los nuevos objetos añadidos a este bucket, a partir del momento en que se ingieren. Especifica un valor que sea menor o igual al período máximo de retención para el tenant, según lo haya establecido el administrador del grid.

El administrador de la grid establece un periodo de retención *máximo*, que puede ser un valor de 1 día hasta 100 años, al crear el tenant. Cuando estableces un periodo de retención *por defecto*, no puede superar el valor establecido para el periodo de retención máximo. Si lo necesitas, pídele a tu administrador de la grid que aumente o disminuya el periodo de retención máximo.

4. Si lo deseas, selecciona **Activar límite de capacidad**, introduce un valor y selecciona la unidad 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 el disco).

Si no estableces ningún límite, la capacidad de este bucket es ilimitada. Consulta ["Uso del límite de capacidad"](#) para obtener más información.

5. Si lo deseas, selecciona **Activar límite de recuento de objetos**.

El límite de objetos es el número máximo de objetos que puede contener este bucket. Este valor representa una cantidad lógica (número de objetos). Si no se establece ningún límite, el número de objetos es ilimitado.

6. Selecciona **Create bucket**.

El bucket se crea y se añade a la tabla en la página Buckets.

7. Opcionalmente, selecciona **Ir a la página de detalles del bucket** para ["ver los detalles del bucket"](#) y realizar una configuración adicional.

También puedes ["crear buckets de rama"](#) cuando lo necesites.

Ver detalles del bucket S3 en StorageGRID

Puedes ver los buckets de tu cuenta de inquilino.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el ["Acceso raíz, gestionar todos los buckets o ver todos los buckets"](#). Estos permisos anulan la configuración de permisos en las políticas de grupo o de bucket.

Pasos

1. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.

Aparece la página «Buckets».

2. Revisa la tabla resumen de cada bucket.

Si lo deseas, puedes ordenar la información por cualquier columna o puedes avanzar y retroceder por la lista.



Los valores de «Recuento de objetos», «Espacio utilizado» y «Uso» que se muestran son estimaciones. Estas estimaciones dependen del momento en que se realizan las ingestas, de la conectividad de red y del estado de los nodos. Si los buckets tienen habilitado el versionado, las versiones de los objetos eliminados se incluyen en el recuento de objetos.

Nombre

El nombre único del bucket, que no se puede cambiar.

Funciones activadas

La lista de funciones que están habilitadas para el bucket.

Bloqueo de objetos de S3

Si la función S3 Object Lock está activada para el bucket.

Esta columna solo aparece si S3 Object Lock está habilitado para el grid. Esta columna también muestra información sobre cualquier bucket Compliant heredado.

Región

La región del bucket, que no se puede modificar. Esta columna está oculta de forma predeterminada.

Recuento de objetos

El número de objetos en este bucket. Si los buckets tienen habilitado el control de versiones, las versiones de objetos no actuales se incluyen en este valor.

Cuando se añaden o eliminan objetos, es posible que este valor no se actualice de inmediato.

Espacio utilizado

El tamaño lógico de todos los objetos del bucket. El tamaño lógico no incluye el espacio real requerido para las copias replicadas o con codificación de borrado, ni para los metadatos de los objetos.

Este valor puede tardar hasta 10 minutos en actualizarse.

Uso

El porcentaje utilizado del límite de capacidad del bucket, en caso de que se haya establecido uno.

El valor de uso se basa en estimaciones internas y podría superarse en algunos casos. Por ejemplo, StorageGRID comprueba el límite de capacidad (si está configurado) cuando un inquilino empieza a subir objetos y rechaza nuevas ingestas en este bucket si el inquilino ha superado el límite de capacidad. Sin embargo, StorageGRID no tiene en cuenta el tamaño de la subida actual al determinar si se ha superado el límite de capacidad. Si se eliminan objetos, es posible que un inquilino no pueda subir nuevos objetos temporalmente a este bucket 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 para el bucket.

Fecha de creación

La fecha y la hora en que se creó el bucket. Esta columna está oculta de forma predeterminada.

3. Para ver los detalles de un bucket concreto, selecciona el nombre del bucket en la tabla.
 - a. Consulta la información resumida que aparece en la parte superior de la página web para comprobar los detalles del bucket, como Region y Object count.
 - b. Consulta las barras de uso del límite de capacidad y del límite de número de objetos. Si el uso es del 100% o se acerca al 100%, plantéate aumentar el límite o eliminar algunos objetos.
 - c. Si es necesario, selecciona **Eliminar objetos en el bucket** y **Eliminar el bucket**.



Presta mucha atención a las advertencias que aparecen al seleccionar cada una de estas opciones. Para obtener más información, consulta:

- ["Eliminar todos los objetos de un bucket"](#)
- ["Eliminar un bucket"](#) (el bucket debe estar vacío)

- d. Consulta o modifica la configuración del bucket en cada una de las pestañas según sea necesario.
 - **S3 Console:** visualiza los objetos del bucket. Para obtener más información, consulta ["Usa la consola de S3"](#).
 - **Opciones del bucket:** Ver o cambiar la configuración de las opciones. Algunas opciones, como S3 Object Lock, no se pueden cambiar después de crear el bucket.
 - ["Gestiona la coherencia del bucket"](#)
 - ["Actualizaciones del tiempo de acceso último"](#)
 - ["Límite de capacidad"](#)

- ["Límite de objetos"](#)
- ["Control de versiones de objetos"](#)
- ["Bloqueo de objetos de S3"](#)
- ["Retención predeterminada del bucket"](#)
- ["Gestiona la replicación entre grids"](#) (si está permitido para el inquilino)
- **Servicios de plataforma:** ["Gestiona los servicios de la plataforma"](#) (si están permitidos para el inquilino)
- **Acceso al bucket:** ver o cambiar la configuración de las opciones. Debes tener permisos de acceso específicos.
 - Configura ["CORS para buckets y objetos"](#) para que el bucket y los objetos del bucket estén accesibles para aplicaciones web de otros dominios.
 - ["Controlar el acceso de los usuarios"](#) para un bucket de S3 y los objetos en ese bucket.
- **Ramas:** Ver la lista de buckets de ramas para el bucket. ["Crear un nuevo bucket de rama o gestionar buckets de rama"](#).

Conoce StorageGRID branch buckets

Un «branch bucket» permite acceder a los objetos de un bucket tal y como estaban en un momento determinado.

Creas un bucket de ramificación a partir de un bucket existente. Una vez que creas un bucket de ramificación, el bucket original a partir del cual se creó se denomina *bucket base*. Además, puedes crear un bucket de ramificación a partir de otro bucket de ramificación.

Un bucket de ramificación proporciona acceso a los datos protegidos, pero no sirve como copia de seguridad. Para seguir protegiendo los datos, usa estas funciones en los buckets base:

- ["Bloqueo de objetos de S3"](#)
- ["Replicación entre grids"](#) para buckets base
- ["Políticas de buckets"](#) para buckets con control de versiones para limpiar las versiones antiguas de los objetos

Ten en cuenta las siguientes características de los cubos de ramificación:

- Puedes acceder a los objetos de los buckets de las ramas utilizando ["Consola de S3 para descargar objetos"](#).
- Cuando los clientes acceden a objetos en un bucket rama, ["políticas de acceso"](#) del bucket rama, en lugar de las políticas del bucket base, determinan si se concede o se deniega el acceso.
- Los objetos creados en un bucket base se evalúan en función de cómo se aplican ["Reglas de ILM"](#) al bucket base. Los objetos creados en un bucket de rama se evalúan en función de cómo se aplican las reglas de ILM al bucket de rama.
- La replicación entre grids no es compatible con los buckets de sucursales.
- Los servicios de plataforma no son compatibles con los buckets de sucursales.

Ejemplos de uso de los branch buckets

- Puedes usar un bucket de rama para eliminar objetos corruptos creando un bucket de rama desde un

punto en el tiempo anterior a que ocurriera la corrupción y luego apuntar las aplicaciones al bucket de rama en lugar de al bucket base que contiene los objetos corruptos.

- Estás almacenando datos en un bucket con control de versiones. Hubo una vulnerabilidad accidental que provocó que se ingresaran muchos objetos no deseados después del momento T . Puedes crear un bucket de rama para el valor Before time, T , y redirigir las operaciones de los clientes a ese bucket de rama. Así, solo los objetos ingresados antes del momento Before time T estarán disponibles para los clientes.

Operaciones con objetos en los buckets de rama

- Una operación PUT de objeto en un bucket de rama crea un objeto en la rama.
- Una operación GET sobre un objeto en un bucket de rama recupera un objeto de la rama. Si el objeto no existe en el bucket de rama, el objeto se recupera del bucket base.
- La eliminación de objetos de los buckets de las ramas ocurre de la siguiente manera:

Operación	Objetivo	Resultado	Visibilidad de los objetos en el bucket base	Visibilidad de objetos en el bucket de la rama
Eliminar sin ID de versión	Bucket base	El marcador de eliminación se crea únicamente para el depósito base	HEAD/GET devuelve «El objeto no existe», pero aún se puede acceder a versiones concretas	HEAD/GET devuelve que el objeto existe, y aún se puede acceder a versiones específicas El marcador de borrado se habría creado después del del bucket de la sucursal beforeTime.
Eliminar con el ID de versión	Bucket base	Se elimina la versión específica del objeto tanto en el bucket base como en el bucket de la rama	HEAD/GET devuelve que la versión del objeto no existe	HEAD/GET devuelve que la versión del objeto no existe
Eliminar sin ID de versión	Bucket de rama	El marcador de eliminación se crea únicamente para el bucket de la rama	HEAD/GET devuelve un objeto (el objeto base del bucket no se ve afectado)	HEAD/GET devuelve que el objeto no existe
Eliminar con el ID de versión	Bucket de rama	La versión específica del objeto solo se elimina para el bucket de la rama	HEAD/GET devuelve una versión específica del objeto (el objeto base del bucket no se ve afectado)	HEAD/GET devuelve que la versión del objeto no existe

También consulta ["Cómo se eliminan los objetos versionados de S3"](#).

Administra los buckets de la rama StorageGRID

Utiliza el Tenant Manager para crear y ver detalles de los buckets de sucursal.

Antes de empezar

- Has iniciado sesión en Tenant Manager usando una ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el acceso Root o ["Gestiona el permiso de todos los buckets"](#). Estos permisos anulan la configuración de permisos en las políticas de grupo o de bucket.
- El bucket base desde el que quieres crear una rama tiene ["control de versiones activado"](#).
- Eres el propietario del bucket base.

Acerca de esta tarea

Ten en cuenta la siguiente información sobre los «buckets» de ramas:

- Los permisos para configurar las propiedades de S3 Object Lock de los buckets u objetos pueden ser concedidos por ["política de bucket o política de grupo"](#).
- Si suspendes el control de versiones en el depósito base, el contenido del depósito base ya no será visible en sus depósitos derivados.



Después de que configures y crees un branch bucket, no puedes cambiar la configuración.

Crear bucket de rama

Pasos

1. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.
2. Selecciona el bucket desde el que deseas crear una rama (el "bucket base").
3. En la página de detalles del bucket, selecciona **Branches > Create branch bucket**.

El botón **Crear bucket de rama** está desactivado si el bucket base no tiene activado el control de versiones.

Introduce los datos

Pasos

1. Introduce los datos del «branch bucket».

Campo	Descripción
Nombre del bucket de la rama	Un nombre para el bucket de la rama que cumpla estas reglas: • Debe ser único en cada sistema StorageGRID (no solo 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 usar letras minúsculas, números y guiones. • No debe contener puntos en las solicitudes de tipo virtual hosted style. Los puntos provocarán problemas con la verificación del certificado comodín del servidor. Para más información, consulta el "Documentación de Amazon Web Services (AWS) sobre las reglas de nomenclatura de los buckets". Nota: No puedes cambiar el nombre después de crear el bucket de la rama.
Región (no se puede modificar para los buckets de sucursales)	La región del bucket de la rama. La región del «bucket» de rama debe coincidir con la región del «bucket» base, por lo que este campo está desactivado para los «buckets» de rama.
Antes de tiempo	La hora límite para que las versiones de los objetos creadas en el depósito base sean accesibles desde el depósito de la rama. El depósito de la rama permite acceder a las versiones de los objetos creadas antes de la hora límite. «Before time» debe ser una fecha y una hora que ya hayan pasado. No puede ser una fecha futura.
Tipo de bucket de rama	• Lectura/escritura: Puedes añadir o eliminar objetos o versiones de objetos en el bucket de la rama. • Solo lectura: No puedes modificar los objetos del bucket de la rama. Nota: Solo puedes configurar el tipo de bucket de rama como «solo lectura» si el bucket de rama está vacío. Si el tipo de un bucket de rama ya existente está configurado como «lectura/escritura» y aún no has escrito en él, puedes cambiar el tipo a «solo lectura».

2. Selecciona **Continuar**.

Gestiona la configuración de los objetos (opcional)

La configuración de los objetos de un depósito de rama no afecta las versiones de los objetos en el depósito base.

Pasos

1. Si la configuración global de S3 Object Lock está activada, puedes activar S3 Object Lock para el bucket de la sucursal. Para activar S3 Object Lock, el bucket de la sucursal debe ser un bucket de

lectura/escritura.

Activa S3 Object Lock para un bucket de sucursal solo si necesitas conservar los objetos durante un periodo de tiempo determinado, por ejemplo, para cumplir con ciertos requisitos normativos. S3 Object Lock es una configuración permanente que te ayuda a evitar que los objetos se eliminen o se sobrescriban durante un periodo de tiempo determinado o de forma indefinida.



Una vez habilitada la configuración de S3 Object Lock para un bucket, no se puede deshabilitar. Cualquier persona con los permisos adecuados puede añadir objetos al bucket de la rama que no se pueden cambiar. Puede que no puedas eliminar estos objetos ni el bucket de la rama.

2. Si seleccionaste **Habilitar S3 Object Lock**, opcionalmente habilita la **retención predeterminada** para el bucket de la sucursal.



Tu administrador de grid debe darte permiso para ["utilizar las funciones específicas de S3 Object Lock"](#).

Cuando la **retención predeterminada** está activada, los nuevos objetos añadidos al bucket de la rama quedarán protegidos automáticamente contra su eliminación o sobrescritura. La configuración de **retención predeterminada** no se aplica a los objetos que tienen sus propios periodos de retención.

- a. Si la opción **Retención predeterminada** está activada, especifica un **modo de retención predeterminado** para el bucket de la rama.

Modo de retención predeterminado	Descripción
Gobernanza	• Los usuarios con el permiso <code>s3:BypassGovernanceRetention</code> pueden usar el encabezado de solicitud <code>x-amz-bypass-governance-retention: true</code> para omitir la configuración de retención. • Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su <code>retain-until-date</code>. • Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.
Cumplimiento normativo	• El objeto no se puede eliminar hasta que se alcance su fecha de retención. • La fecha límite de retención del objeto se puede ampliar, pero no se puede reducir. • La fecha de retención del objeto no se puede eliminar hasta que se alcance dicha fecha. Nota: El administrador de tu grid debe autorizarte a utilizar el modo de cumplimiento.

- b. Si la opción **Retención predeterminada** está activada, especifica el **Período de retención predeterminado** para el bucket de la rama.

El **período de retención predeterminado** indica durante cuánto tiempo deben conservarse los

nuevos objetos añadidos al bucket de la rama, a partir del momento en que se incorporan. Especifica un valor que sea menor o igual al período máximo de retención para el tenant, según lo haya establecido el grid administrator.

El administrador de la grid establece un periodo de retención *máximo*, que puede ser un valor de 1 día hasta 100 años, al crear el tenant. Cuando estableces un periodo de retención *por defecto*, no puede superar el valor establecido para el periodo de retención máximo. Si lo necesitas, pídele a tu administrador de la grid que aumente o disminuya el periodo de retención máximo.

3. Si lo deseas, selecciona **Activar límite de capacidad**.

El límite de capacidad es la capacidad máxima disponible para el bucket de la rama. Este valor representa una cantidad lógica (tamaño del objeto), no una cantidad física (tamaño en el disco).

Si no se establece ningún límite, la capacidad del «branch bucket» es ilimitada. Consulta ["Uso del límite de capacidad"](#) para más información.



Esta configuración solo se aplica a los objetos incorporados directamente en el bucket de la rama, y no a los objetos que son visibles desde el bucket base a través del bucket de la rama.

4. Si lo deseas, selecciona **Activar límite de recuento de objetos**.

El límite de objetos es el número máximo de objetos que puede contener el bucket de la rama. Este valor representa una cantidad lógica (número de objetos). Si no se establece ningún límite, el número de objetos es ilimitado.



Esta configuración solo se aplica a los objetos incorporados directamente en el bucket de la rama, y no a los objetos que son visibles desde el bucket base a través del bucket de la rama.

5. Selecciona **Create bucket**.

El bucket de la sucursal se crea y se añade a la tabla en la página Buckets.

6. Si lo deseas, selecciona **Ir a la página de detalles del bucket** para ["Ver detalles del bucket de la rama"](#) y realizar una configuración adicional.

En la página de detalles del bucket, algunas opciones de configuración relacionadas con la modificación de objetos están desactivadas para los buckets de solo lectura.

Aplicar una etiqueta de política ILM a un bucket StorageGRID

Elige una etiqueta de política de ILM para aplicarla a un bucket según tus requisitos de almacenamiento de objetos.

La política de ILM controla dónde se almacenan los datos de los objetos y si se eliminan tras un periodo de tiempo determinado. El administrador de la grid crea las políticas de ILM y las asigna a etiquetas de políticas de ILM cuando se utilizan varias políticas activas.



Evita reasignar con frecuencia la etiqueta de política de un bucket. De lo contrario, podrían producirse problemas de rendimiento.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un "navegador web compatible".
- Perteneces a un grupo de usuarios que tiene el "Acceso raíz, gestionar todos los buckets o ver todos los buckets". Estos permisos anulan la configuración de permisos en las políticas de grupo o de bucket.

Pasos

1. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.

Aparece la página «Buckets». Si lo deseas, puedes ordenar la información por cualquier columna o puedes desplazarte hacia adelante y hacia atrás por la lista.

2. Selecciona el nombre del bucket al que quieras asignar una etiqueta de política de ILM.

También puedes cambiar la asignación de la etiqueta de la política de ILM para un bucket que ya tiene una etiqueta asignada.



Los valores de Recuento de objetos y Espacio usado que se muestran son estimaciones. Estas estimaciones se ven afectadas por el momento de las ingestas, la conectividad de red y el estado de los nodos. Si los buckets tienen habilitado el control de versiones, las versiones de objetos eliminados se incluyen en el recuento de objetos.

3. En la pestaña Opciones del bucket, despliega el acordeón de etiquetas de política de ILM. Este acordeón solo aparece si el administrador de tu grid ha habilitado el uso de etiquetas de política personalizadas.
4. Lee la descripción de cada etiqueta de política para determinar qué etiqueta debe aplicarse al bucket.



Al modificar la etiqueta de política de ILM de un bucket, se activará una reevaluación de ILM de todos los objetos en el bucket. Si la nueva política retiene los objetos por un tiempo limitado, los objetos más antiguos se eliminarán.

5. Selecciona el botón de opción para la etiqueta que quieras asignar al depósito.
6. Selecciona **Guardar cambios**. Se establecerá una nueva etiqueta de S3 en el bucket con la clave `NTAP-SG-ILM-BUCKET-TAG` y el valor del nombre de la etiqueta de la política de ILM.



Asegúrate de que tus aplicaciones S3 no sobrescriban ni eliminen accidentalmente la nueva etiqueta de bucket. Si se omite esta etiqueta al aplicar un nuevo TagSet al bucket, los objetos del bucket volverán a evaluarse según la política de ILM predeterminada.



Configura y modifica las etiquetas de política de ILM usando solo el Tenant Manager o la API de Tenant Manager donde se valida la etiqueta de política de ILM. No modifies la `NTAP-SG-ILM-BUCKET-TAG` etiqueta de política de ILM usando la API `PutBucketTagging` de S3 o la API `DeleteBucketTagging` de S3.



Cambiar la etiqueta de política asignada a un bucket tiene un impacto temporal en el rendimiento mientras se vuelven a evaluar los objetos según la nueva política de ILM.

Gestiona la política de bucket de StorageGRID

Puedes controlar el acceso de los usuarios a un bucket de S3 y a los objetos en ese bucket.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el ["Permiso de acceso raíz"](#). Los permisos «Ver todos los buckets» y «Gestionar todos los buckets» solo permiten la visualización.
- Has comprobado que hay disponible el número necesario de Storage Nodes y sitios. Si no hay dos o más Storage Nodes disponibles en algún sitio, o si un sitio no está disponible, es posible que no puedas realizar cambios en estos ajustes.

Pasos

1. Selecciona **Buckets** y luego selecciona el bucket que quieres gestionar.
2. En la página de detalles del bucket, selecciona **Acceso al bucket > Política del bucket**.
3. Debe realizar una de las siguientes acciones:
 - Introduce una política de bucket marcando la casilla **Habilitar política**. Luego introduce una cadena válida en formato JSON.

Cada política de bucket tiene un límite de tamaño de 20,480 bytes.
 - Modifica una política existente editando la cadena.
 - Desactiva una política desmarcando **Activar política**.

Para obtener información detallada sobre las políticas de buckets, incluida la sintaxis del lenguaje y ejemplos, consulta ["Ejemplos de políticas de bucket"](#).

Gestiona la coherencia de los buckets StorageGRID

Los valores de consistencia pueden usarse para especificar la disponibilidad de los cambios en la configuración de los buckets, así como para lograr un equilibrio entre la disponibilidad de los objetos dentro de un bucket y la consistencia de esos objetos entre los diferentes Storage Nodes y sitios. Puedes cambiar los valores de consistencia para que sean diferentes de los valores predeterminados, así las aplicaciones cliente pueden cumplir con sus necesidades operativas.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el ["Gestiona todos los buckets o permiso de acceso a raíz"](#). Estos permisos anulan la configuración de permisos en las políticas de grupo o de bucket.

Directrices sobre la consistencia de los buckets

La consistencia del bucket se utiliza para determinar la consistencia para las aplicaciones cliente que afectan a los objetos dentro de ese bucket de S3. En general, deberías usar la consistencia **Read-after-new-write** para tus buckets.

Cambiar la consistencia del bucket

Si la consistencia **Read-after-new-write** no cumple los requisitos de la aplicación cliente, puedes cambiar la consistencia configurando la consistencia del bucket o usando el encabezado `Consistency-Control`. El encabezado `Consistency-Control` anula la consistencia del bucket.



Cuando cambias la consistencia de un bucket, solo se garantiza que los objetos que se incorporen después del cambio cumplan con la configuración revisada.

Pasos

1. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.
2. Selecciona el nombre del bucket de la tabla.

Aparece la página de detalles del bucket.

3. En la pestaña **Opciones del bucket**, selecciona el **** acordeón**.
4. Selecciona una consistencia para las operaciones que se realicen sobre los objetos de este bucket.
 - **Todos**: Ofrece el máximo nivel de coherencia. Todos los nodos reciben los datos de forma inmediata o la solicitud fallará.
 - **Strong-global**: Garantiza la consistencia de lectura posterior a la escritura para todas las solicitudes de los clientes en todos los sitios.
 - **Sitio fuerte**: Garantiza la consistencia de lectura después de escritura para todas las solicitudes de los clientes dentro de un sitio.
 - **Lectura tras nueva escritura** (predeterminado): Ofrece consistencia de lectura tras escritura para los nuevos objetos y consistencia eventual para las actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
 - **Disponible**: Proporciona consistencia eventual tanto para los objetos nuevos como para las actualizaciones de objetos. Para los buckets de S3, utilízalo solo cuando sea necesario (por ejemplo, para un bucket que contenga valores de registro que rara vez se leen, o para operaciones HEAD o GET sobre claves que no existen). No es compatible con los buckets de S3 FabricPool.
5. Selecciona **Guardar cambios**.

¿Qué pasa cuando cambias la configuración de los buckets?

Los buckets tienen múltiples configuraciones que afectan el comportamiento de los buckets y de los objetos dentro de esos buckets.

Los siguientes ajustes del bucket utilizan consistencia **fuerte** de forma predeterminada. Si dos o más Storage Nodes no están disponibles en cualquier sitio, o si un sitio no está disponible, es posible que los cambios en estos ajustes no estén disponibles.

- "Eliminación de buckets vacíos en segundo plano"
- "Último tiempo de acceso"
- "Ciclo de vida de bucket"
- "Política de bucket"
- "Etiquetado de buckets"
- "Control de versiones de buckets"
- "Bloqueo de objetos de S3"
- "Cifrado de bucket"



El valor de consistencia para el control de versiones de buckets, S3 Object Lock y el cifrado de buckets no se puede establecer en un valor que no sea de consistencia fuerte.

Los siguientes ajustes del bucket no utilizan consistencia fuerte y ofrecen una mayor disponibilidad para los cambios. Es posible que los cambios en estos ajustes tarden un tiempo en surtir efecto.

- ["Configuración de los servicios de la plataforma: notificación, replicación o integración de búsqueda"](#)
- ["Configura StorageGRID CORS para los buckets y los objetos"](#)
- [Cambiar la consistencia del bucket](#)



Si la consistencia predeterminada que se utiliza al cambiar la configuración del bucket no cumple con los requisitos de la aplicación cliente, puedes cambiar la consistencia usando el `Consistency-Control` header para el ["API de REST de S3"](#) o usando las opciones `reducedConsistency` o `force` en el ["API de gestión de inquilinos"](#).

Activar o desactivar las actualizaciones del tiempo de acceso en StorageGRID

Cuando los administradores de grid crean las reglas de gestión del ciclo de vida de la información (ILM) para un sistema StorageGRID, pueden especificar de forma opcional que se utilice el tiempo de acceso más reciente de un objeto para determinar si ese objeto debe moverse a una ubicación de almacenamiento diferente. Si estás usando un tenant de S3, puedes aprovechar este tipo de reglas habilitando las actualizaciones del tiempo de acceso para los objetos en un bucket de S3.

Estas instrucciones solo se aplican a los sistemas StorageGRID que incluyan al menos una regla ILM que utilice la opción **Tiempo de acceso más reciente** como filtro avanzado o como hora de referencia. Puedes ignorar estas instrucciones si tu sistema StorageGRID no incluye dicha regla. Consulta ["Usa el tiempo de acceso en las reglas de ILM"](#) para más detalles.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el ["Gestiona todos los buckets o permiso de acceso a raíz"](#). Estos permisos anulan la configuración de permisos en las políticas de grupo o de bucket.

Acerca de esta tarea

Tiempo de acceso es una de las opciones disponibles para la instrucción de ubicación **Tiempo de referencia** de una regla de ILM. Al establecer el tiempo de referencia de una regla en tiempo de acceso, los administradores de grid pueden especificar que los objetos se coloquen en determinadas ubicaciones de almacenamiento según cuándo se recuperaron (leyeron o visualizaron) por última vez.

Por ejemplo, para garantizar que los objetos consultados recientemente permanezcan en un almacenamiento más rápido, un administrador de la red puede crear una regla de ILM especificando lo siguiente:

- Los objetos que se hayan recuperado en el último mes deben permanecer en los nodos de almacenamiento locales.
- Los objetos que no se hayan consultado en el último mes deben trasladarse a una ubicación fuera del sitio.

De forma predeterminada, las actualizaciones del tiempo de acceso están desactivadas. Si tu sistema StorageGRID incluye una regla ILM que utiliza la opción **tiempo de acceso** y quieres que esta opción se aplique a los objetos de este bucket, debes activar las actualizaciones del tiempo de acceso para los buckets S3 especificados en esa regla.



Actualizar el tiempo de acceso al recuperar un objeto puede reducir el rendimiento de StorageGRID, especialmente en el caso de los objetos pequeños.

Se produce un impacto en el rendimiento con las actualizaciones del tiempo de acceso porque StorageGRID debe realizar estos pasos adicionales cada vez que se recuperan objetos:

- Actualiza los objetos con nuevas marcas de tiempo
- Añade los objetos a la cola de ILM para que puedan volver a evaluarse según las reglas y la política actuales de ILM

La tabla resume el comportamiento que se aplica a todos los objetos del bucket cuando el tiempo de acceso está desactivado o activado.

Tipo de solicitud	Comportamiento si el tiempo de acceso más reciente está desactivado (por defecto)		Comportamiento si está activado el tiempo de acceso más reciente	
	¿Se actualizó el último tiempo de acceso?	¿Objeto añadido a la cola de evaluación de ILM?	¿Se actualizó el último tiempo de acceso?	¿Objeto añadido a la cola de evaluación de ILM?
Solicitud para recuperar los metadatos de un objeto cuando se emite una operación HEAD	No	No	No	No
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 para obtener una lista de objetos o versiones de objetos	No	No	No	No
Solicitud para copiar un objeto de un bucket a otro	• No, para la copia original • Sí, para la copia de destino	• No, para la copia original • Sí, para la copia de destino	• Sí, para la copia original • Sí, para la copia de destino	• Sí, para la copia original • Sí, para la copia de destino

Solicitud para completar una subida en varias partes	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado	Sí, para el objeto ensamblado

Pasos

1. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.
2. Selecciona el nombre del bucket de la tabla.

Aparece la página de detalles del bucket.

3. En la pestaña **Opciones del bucket**, selecciona el acordeón **Actualizaciones del tiempo de acceso**.
4. Activar o desactivar las actualizaciones del tiempo de acceso.
5. Selecciona **Guardar cambios**.

Cambiar el versionado de objetos para un bucket S3 en StorageGRID

Si utilizas un inquilino de S3, puedes cambiar el estado de control de versiones de los buckets de S3.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el ["Gestiona todos los buckets o permiso de acceso a raíz"](#). Estos permisos anulan la configuración de permisos en las políticas de grupo o de bucket.
- Has comprobado que hay disponible el número necesario de Storage Nodes y sitios. Si no hay dos o más Storage Nodes disponibles en algún sitio, o si un sitio no está disponible, es posible que no puedas realizar cambios en estos ajustes.

Acerca de esta tarea

Puedes activar o suspender el control de versiones de objetos para un bucket. Una vez que actives el control de versiones para un bucket, este no podrá volver a un estado sin control de versiones. Sin embargo, puedes suspender el control de versiones para el bucket.

- Desactivado: la gestión de versiones nunca se ha activado
- Activado: el control de versiones está activado
- Suspendido: la gestión de versiones estaba activada anteriormente y ahora está suspendida

Para obtener más información, consulta lo siguiente:

- ["Control de versiones de objetos"](#)
- ["Normas y políticas de ILM para objetos versionados en S3 \(Ejemplo 4\)"](#)
- ["Cómo se eliminan los objetos"](#)

Pasos

1. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.
2. Selecciona el nombre del bucket de la tabla.

Aparece la página de detalles del bucket.

3. En la pestaña **Opciones del bucket**, selecciona el acordeón **Control de versiones de objetos**.
4. Selecciona un estado de control de versiones para los objetos en este bucket.

El control de versiones de objetos debe permanecer habilitado para un bucket utilizado para la replicación entre grids. Si S3 Object Lock o la conformidad heredada están habilitados, las opciones de **control de versiones de objetos** están deshabilitadas.

Opción	Descripción
Habilitar el control de versiones	Activa el versionado de objetos si quieres almacenar cada versión de cada objeto en este bucket. Después podrás recuperar las versiones anteriores de un objeto según lo necesites. Los objetos que ya se encontraban en el bucket tendrán una versión cuando un usuario los modifique.
Suspender el control de versiones	Suspende el control de versiones de objetos si ya no quieres que se creen nuevas versiones de objetos. Aún puedes recuperar las versiones de objetos existentes.

5. Selecciona **Guardar cambios**.

Usa S3 Object Lock para retener objetos en StorageGRID

Puedes utilizar S3 Object Lock si los buckets y los objetos deben cumplir los requisitos normativos de retención.



El administrador de tu grid debe concederte permiso para utilizar funciones específicas de S3 Object Lock.

¿Qué es S3 Object Lock?

La función S3 Object Lock de StorageGRID es una solución de protección de objetos equivalente a S3 Object Lock en Amazon Simple Storage Service (Amazon S3).

Cuando la configuración global de S3 Object Lock está habilitada para un sistema StorageGRID, una cuenta de inquilino de S3 puede crear buckets con o sin S3 Object Lock habilitado. Si un bucket tiene S3 Object Lock habilitado, el control de versiones de buckets es obligatorio y se habilita automáticamente.

Un bucket sin S3 Object Lock solo puede tener objetos sin una configuración de retención especificada. Ningún objeto ingerido tendrá configuración de retención.

Un bucket con S3 Object Lock puede tener objetos con y sin ajustes de retención especificados por las aplicaciones cliente de S3. Algunos objetos incorporados tendrán ajustes de retención.

Un bucket con S3 Object Lock y la retención predeterminada configurada puede contener objetos cargados con ajustes de retención especificados y nuevos objetos sin ajustes de retención. Los nuevos objetos usan la configuración predeterminada, porque la configuración de retención no se ha configurado a nivel de objeto.

Efectivamente, todos los objetos recién ingeridos tienen ajustes de retención cuando se configura la retención predeterminada. Los objetos existentes sin ajustes de retención de objetos no se ven afectados.

Modos de retención

La función Object Lock de StorageGRID S3 admite dos modos de retención para aplicar distintos niveles de protección a los objetos. Estos modos son equivalentes a los modos de retención de Amazon S3.

- En modo de cumplimiento:
 - El objeto no se puede eliminar hasta que se alcance su fecha de retención.
 - La fecha límite de retención del objeto se puede ampliar, pero no se puede reducir.
 - La fecha de retención del objeto no se puede eliminar hasta que se alcance dicha fecha.
- En modo de gobernanza:
 - Los usuarios con permisos especiales pueden utilizar un encabezado de omisión en las solicitudes para modificar determinados ajustes de retención.
 - Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su retain-until-date.
 - Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

Configuración de retención para las versiones de los objetos

Si se crea un depósito con S3 Object Lock activado, los usuarios pueden usar la aplicación cliente de S3 para especificar de forma opcional los siguientes parámetros de retención para cada objeto que se añada al depósito:

- **Modo de retención:** cumplimiento normativo o gobernanza.
- **Fecha límite de conservación:** Si la fecha límite de conservación de una versión de un objeto es posterior a la fecha actual, el objeto se puede recuperar, pero no se puede eliminar.
- **Retención legal:** Al aplicar una retención legal a la versión de un objeto, dicho objeto queda bloqueado de inmediato. Por ejemplo, podrías necesitar aplicar una retención legal a un objeto relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de caducidad, sino que permanece vigente hasta que se elimine de forma explícita. Las retenciones legales son independientes de la retain-until-date.



Si un objeto está sujeto a una retención legal, nadie puede eliminar el objeto, independientemente de su modo de retención.

Para obtener detalles sobre la configuración de los objetos, consulta ["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#).

Configuración predeterminada de retención para los buckets

Si se crea un bucket con S3 Object Lock activado, los usuarios pueden, si lo desean, especificar los siguientes ajustes predeterminados para el bucket:

- **Modo de retención predeterminado:** cumplimiento o gobernanza.
- **Período de retención predeterminado:** cuánto tiempo deben conservarse las nuevas versiones de objetos añadidas a este bucket, a partir del día en que se añaden.

La configuración predeterminada del depósito solo se aplica a los objetos nuevos que no tienen su propia

configuración de retención. Los objetos existentes en el depósito no se ven afectados cuando añades o cambias esta configuración predeterminada.

Consulta ["Crear un depósito de S3"](#) y ["Actualizar la retención predeterminada de S3 Object Lock"](#).

Tareas de S3 Object Lock

Las siguientes listas para administradores de grid y usuarios de inquilinos contienen las tareas a grandes rasgos para usar la función S3 Object Lock.

Administrador de grid

- Activa la configuración global de S3 Object Lock para todo el sistema StorageGRID.
- Asegúrate de que las políticas de gestión del ciclo de vida de la información (ILM) sean *conformes*; es decir, que cumplan con ["Requisitos de los buckets con S3 Object Lock activado"](#).
- Si es necesario, permite que un inquilino utilice Compliance como modo de retención. De lo contrario, solo se permite el modo Governance.
- Si es necesario, establece un periodo máximo de retención para un tenant.

Usuario arrendatario

- Revisa las consideraciones para los buckets y objetos con S3 Object Lock.
- Si es necesario, ponte en contacto con el administrador de grid para activar la configuración global de S3 Object Lock y establecer los permisos.
- Crea buckets con S3 Object Lock activado.
- Opcionalmente, configura los ajustes de retención predeterminados para un bucket:
 - Modo de retención predeterminado: Governance o Compliance, si lo permite el administrador del grid.
 - Período de retención predeterminado: debe ser menor o igual al período máximo de retención establecido por el administrador de grid.
- Utiliza la aplicación cliente de S3 para añadir objetos y, si lo deseas, configurar la retención específica de cada objeto:
 - Modo de retención. Gobernanza o Cumplimiento, si lo permite el administrador de la grid.
 - Fecha de retención: debe ser menor o igual a lo permitido por el periodo máximo de retención establecido por el administrador de grid.

Requisitos para los buckets con S3 Object Lock activado

- Si la configuración global de S3 Object Lock está habilitada para el sistema StorageGRID, puedes usar el Tenant Manager, la API de gestión de inquilinos o la API de REST de S3 para crear buckets con S3 Object Lock habilitado.
- Si tienes pensado utilizar S3 Object Lock, debes habilitar S3 Object Lock al crear el bucket. No puedes habilitar S3 Object Lock en un bucket ya existente.
- Cuando se habilita S3 Object Lock para un bucket, StorageGRID habilita automáticamente el control de versiones para ese bucket. No puedes deshabilitar S3 Object Lock ni suspender el control de versiones para el bucket.
- Si lo deseas, puedes especificar un modo de retención y un periodo de retención predeterminados para cada bucket usando el Tenant Manager, la Tenant Management API o la API de REST de S3. La configuración de retención predeterminada del bucket solo se aplica a los nuevos objetos añadidos al bucket que no tengan su propia configuración de retención. Puedes anular esta configuración

predeterminada especificando un modo de retención y una retain-until-date para cada versión del objeto cuando se suba.

- La configuración del ciclo de vida de los buckets es compatible con los buckets que tienen activada la función S3 Object Lock.
- CloudMirror replication no es compatible con los buckets con S3 Object Lock habilitado.

Requisitos para los objetos en buckets con S3 Object Lock activado

- Para proteger una versión de un objeto, puedes especificar ajustes de retención predeterminados para el bucket, o puedes especificar ajustes de retención para cada versión del objeto. Los ajustes de retención a nivel de objeto se pueden especificar usando la aplicación cliente de S3 o la API de REST de S3.
- Los ajustes de retención se aplican a las versiones individuales de los objetos. Una versión de un objeto puede tener tanto una configuración de «retención hasta una fecha» como una de «retención legal», una de ellas pero no la otra, o ninguna de las dos. Al especificar una configuración de «retención hasta una fecha» o de «retención legal» para un objeto, solo se protege la versión especificada en la solicitud. Puedes crear nuevas versiones del objeto, mientras que la versión anterior del objeto permanece bloqueada.

Ciclo de vida de los objetos en los buckets con S3 Object Lock activado

Cada objeto que se guarda en un bucket con S3 Object Lock activado pasa por estas etapas:

1. Ingesta de objetos

Cuando se añade una versión de un objeto a un bucket que tiene activado S3 Object Lock, la configuración de retención se aplica de la siguiente manera:

- Si especificas la configuración de retención para el objeto, se aplica la configuración a nivel de objeto. Se ignora cualquier configuración predeterminada del bucket.
- Si no se especifican ajustes de retención para el objeto, se aplican los ajustes predeterminados del bucket, si existen.
- Si no se especifican ajustes de retención para el objeto o el depósito, el objeto no está protegido por S3 Object Lock.

Si se aplican los parámetros de retención, quedan protegidos tanto el objeto como cualquier metadato definido por el usuario en S3.

2. Retención y eliminación de objetos

StorageGRID almacena varias copias de cada objeto protegido durante el periodo de retención especificado. El número exacto y el tipo de copias de objeto y las ubicaciones de almacenamiento se determinan por las reglas de cumplimiento en las políticas de ILM activas. Si un objeto protegido puede eliminarse antes de que se alcance su fecha de retención depende de su modo de retención.

- Si un objeto está sujeto a una retención legal, nadie puede eliminar el objeto, independientemente de su modo de retención.

¿Puedo seguir gestionando los buckets Compliant heredados?

La función S3 Object Lock sustituye a la función Compliance que estaba disponible en versiones anteriores de StorageGRID. Si creaste buckets conformes usando una versión anterior de StorageGRID, puedes seguir gestionando la configuración de esos buckets; sin embargo, ya no puedes crear nuevos buckets conformes. Para obtener instrucciones, consulta ["NetApp base de conocimientos: cómo gestionar los buckets Compliant"](#)

Actualizar la retención predeterminada de S3 Object Lock en StorageGRID

Si activaste S3 Object Lock al crear el bucket, puedes editar el bucket para cambiar la configuración de retención predeterminada. Puedes activar (o desactivar) la retención predeterminada y establecer un modo de retención y un periodo de retención predeterminados.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el ["Gestiona todos los buckets o permiso de acceso a raíz"](#). Estos permisos anulan la configuración de permisos en las políticas de grupo o de bucket.
- S3 Object Lock está habilitado de forma global para tu sistema StorageGRID, y habilitaste S3 Object Lock al crear el bucket. Consulta ["Utiliza S3 Object Lock para conservar los objetos"](#).

Pasos

1. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.
2. Selecciona el nombre del bucket de la tabla.

Aparece la página de detalles del bucket.

3. En la pestaña **Opciones del bucket**, selecciona el acordeón **S3 Object Lock**.
4. Opcionalmente, activa o desactiva la **retención predeterminada** para este bucket.

Los cambios en esta configuración no se aplican a los objetos que ya están en el bucket ni a los objetos que puedan tener sus propios períodos de retención.

5. Si la opción **Retención predeterminada** está activada, especifica un **modo de retención predeterminado** para el depósito.

Modo de retención predeterminado	Descripción
Gobernanza	• Los usuarios con el permiso <code>s3:BypassGovernanceRetention</code> pueden usar el encabezado de solicitud <code>x-amz-bypass-governance-retention: true</code> para omitir la configuración de retención. • Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su <code>retain-until-date</code>. • Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

Modo de retención predeterminado	Descripción
Cumplimiento normativo	• El objeto no se puede eliminar hasta que se alcance su fecha de retención. • La fecha límite de retención del objeto se puede ampliar, pero no se puede reducir. • La fecha de retención del objeto no se puede eliminar hasta que se alcance dicha fecha. Nota: El administrador de tu grid debe autorizarte a utilizar el modo de cumplimiento.

6. Si la opción **Retención predeterminada** está activada, especifica el **período de retención predeterminado** para el bucket.

El **período de retención predeterminado** indica durante cuánto tiempo deben conservarse los nuevos objetos añadidos a este bucket, a partir del momento en que se ingieren. Especifica un valor que sea menor o igual al período máximo de retención para el tenant, según lo haya establecido el administrador del grid.

El administrador de la grid establece un periodo de retención *máximo*, que puede ser un valor de 1 día hasta 100 años, al crear el tenant. Cuando estableces un periodo de retención *por defecto*, no puede superar el valor establecido para el periodo de retención máximo. Si lo necesitas, pídele a tu administrador de la grid que aumente o disminuya el periodo de retención máximo.

7. Selecciona **Guardar cambios**.

Configura CORS para buckets S3 en StorageGRID

Puedes configurar el intercambio de recursos entre orígenes (CORS) para un bucket de S3 si quieres que ese bucket y los objetos en ese bucket sean accesibles para aplicaciones web en otros dominios.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Para las solicitudes de configuración GET CORS, perteneces a un grupo de usuarios que tiene el ["Gestionar todos los buckets o Ver todos los buckets permiso"](#). Estos permisos prevalecen sobre la configuración de permisos en las políticas de grupo o de bucket.
- Para las solicitudes de configuración PUT CORS, perteneces a un grupo de usuarios que tiene ["Gestiona el permiso de todos los buckets"](#). Este permiso anula la configuración de permisos en las políticas de grupo o de bucket.
- El ["Permiso de acceso raíz"](#) proporciona acceso a todas las solicitudes de configuración de CORS.

Acerca de esta tarea

El intercambio de recursos de origen cruzado (CORS) es un mecanismo de seguridad que permite a las aplicaciones web cliente de un dominio acceder a recursos de un dominio diferente. Por ejemplo, supón que usas un bucket de S3 llamado `Images` para almacenar gráficos. Al configurar CORS para el bucket `Images`, puedes permitir que las imágenes de ese bucket se muestren en el sitio web `http://www.example.com`.

Habilitar CORS para un bucket

Pasos

1. Usa 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
 - Solo permite que el dominio `http://www.example.com` envíe solicitudes GET, POST y DELETE
 - Se admiten 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 archivo XML de configuración de CORS, consulta ["Documentación de Amazon Web Services \(AWS\): Guía del usuario de Amazon Simple Storage Service"](#).

2. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.
3. Selecciona el nombre del bucket de la tabla.

Aparece la página de detalles del bucket.

4. En la pestaña **Acceso al bucket**, selecciona el acordeón **Cross-Origin Resource Sharing (CORS)**.
5. Marca la casilla **Habilitar CORS**.
6. Pega el XML de configuración de CORS en el cuadro de texto.
7. Selecciona **Guardar cambios**.

Modificar la configuración de CORS

Pasos

1. Actualiza el archivo XML de configuración de CORS en el cuadro de texto o selecciona **Clear** para empezar de nuevo.
2. Selecciona **Guardar cambios**.

Desactivar la configuración de CORS

Pasos

1. Desmarca la casilla **Habilitar CORS**.
2. Selecciona **Guardar cambios**.

Información relacionada

["Configura StorageGRID CORS para una interfaz de gestión"](#)

Eliminar objetos de un bucket S3 de StorageGRID

Puedes utilizar el Tenant Manager para eliminar los objetos de uno o varios buckets.

Consideraciones y requisitos

Antes de seguir estos pasos, ten en cuenta lo siguiente:

- Cuando eliminas los objetos de un bucket, StorageGRID elimina de forma permanente todos los objetos y todas las versiones de objetos de cada bucket seleccionado en todos los nodos y sitios de tu sistema StorageGRID. StorageGRID también elimina los metadatos de objetos relacionados. No podrás recuperar esta información.
- Eliminar todos los objetos de un bucket puede llevar minutos, días o incluso semanas, dependiendo del número de objetos, de las copias de los mismos y de las operaciones simultáneas.
- Si un bucket tiene **"S3 Object Lock activado"**, podría permanecer en el estado **Eliminando objetos: solo lectura** durante *años*.



Un bucket que utilice S3 Object Lock permanecerá en el estado **Eliminación de objetos: solo lectura** hasta que se alcance la fecha de retención de todos los objetos y se eliminen todas las retenciones legales.

- Mientras se están eliminando objetos, el estado del depósito es **Eliminando objetos: solo lectura**. En este estado, no puedes añadir nuevos objetos al depósito.
- Una vez eliminados todos los objetos, el bucket permanece en estado de solo lectura. Puedes realizar una de las siguientes acciones:
 - Vuelve a poner el bucket en modo de escritura y reutilízalo para nuevos objetos
 - Eliminar el bucket
 - Mantén el bucket en modo de solo lectura para reservar su nombre para un uso futuro
- Si en un bucket se ha habilitado el control de versiones de objetos, los marcadores de eliminación creados en StorageGRID 11.8 o versiones posteriores se pueden eliminar mediante la operación Delete objects in bucket.
- Si en un bucket está habilitado el control de versiones de objetos, la operación de eliminación de objetos no eliminará los marcadores de eliminación creados en StorageGRID 11.7 o versiones anteriores. Consulta la información sobre cómo eliminar objetos de un bucket en ["Cómo se eliminan los objetos versionados de S3"](#).
- Si utilizas **"replicación entre grids"**, ten en cuenta lo siguiente:
 - El uso de esta opción no elimina ningún objeto del bucket en la otra grid.
 - Si seleccionas esta opción para el depósito de origen, se activará la alerta **Error de replicación entre redes** si añades objetos al depósito de destino en la otra red. Si no puedes garantizar que nadie vaya a añadir objetos al depósito en la otra red, ["desactivar la replicación entre grids"](#) para ese depósito

antes de eliminar todos los objetos del depósito.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz". Este permiso anula la configuración de permisos de las políticas de grupo o de bucket.

Pasos

1. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.

Aparece la página «Buckets» y muestra todos los buckets de S3 existentes.

2. Utiliza el menú **Acciones** o la página de detalles de un bucket concreto.

Menú de acciones

- a. Marca la casilla de cada bucket del que quieras eliminar objetos.
- b. Selecciona **Actions > Delete objects in bucket**.

Página de detalles

- a. Selecciona el nombre de un bucket para ver sus detalles.
- b. Selecciona **Eliminar objetos en el bucket**.

3. Cuando aparezca el cuadro de diálogo de confirmación, revisa los detalles, escribe **Yes** y selecciona **OK**.
4. Espera a que comience la operación de eliminación.

Al cabo de unos minutos:

- En la página de detalles del bucket aparece un banner de estado amarillo. La barra de progreso indica el porcentaje de objetos que se han eliminado.
- **(solo lectura)** aparece tras el nombre del depósito en la página de detalles del depósito.
- **(Eliminación de objetos: solo lectura)** aparece junto al nombre del bucket en la página Buckets.

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

Success

Starting to delete objects from one 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)

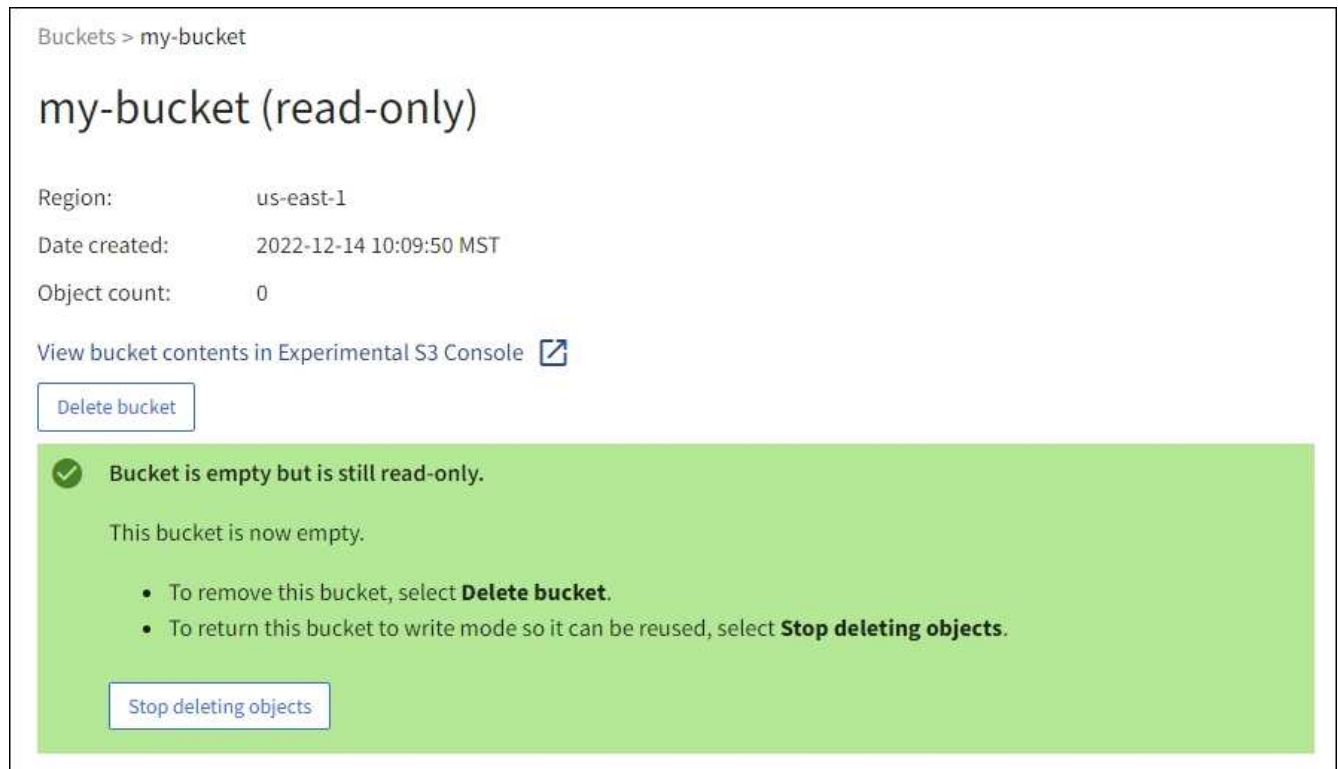
Stop deleting objects

5. Si fuera necesario mientras se está ejecutando la operación, selecciona **Detener la eliminación de objetos** para detener el proceso. Luego, si lo deseas, selecciona **Eliminar objetos del bucket** para reanudar el proceso.

Al seleccionar **Dejar de eliminar objetos**, el bucket vuelve al modo de escritura; sin embargo, no puedes acceder ni restaurar ningún objeto que se haya eliminado.

6. Espera a que finalice la operación.

Cuando el bucket está vacío, se actualiza la barra de estado, pero el bucket sigue siendo de solo lectura.



7. Debe realizar una de las siguientes acciones:

- Sal de la página para mantener el depósito en modo de solo lectura. Por ejemplo, podrías mantener un depósito vacío en modo de solo lectura para reservar el nombre del depósito para su uso futuro.
- Elimina el depósito. Puedes seleccionar **Eliminar depósito** para eliminar un solo depósito o volver a la página Buckets y seleccionar **Acciones > Eliminar** buckets para eliminar más de uno.



Si no puedes eliminar un bucket con control de versiones después de haber eliminado todos los objetos, es posible que queden marcadores de eliminación. Para eliminar el bucket, debes eliminar todos los marcadores de eliminación restantes.

- Vuelve a poner el bucket en modo de escritura y, si lo deseas, reutilízalo para nuevos objetos. Puedes seleccionar **Dejar de eliminar objetos** para un único bucket o volver a la página Buckets y seleccionar **Action > Dejar de eliminar objetos** para más de un bucket.

Eliminar un bucket S3 de StorageGRID

Puedes utilizar el Tenant Manager para eliminar uno o varios buckets de S3 que estén vacíos.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Gestiona todos los buckets o permiso de acceso a raíz". Estos permisos anulan la configuración de permisos en las políticas de grupo o de bucket.
- Los buckets que quieres eliminar están vacíos. Si los buckets que quieres eliminar *no* están vacíos, "eliminar objetos del bucket".

Acerca de esta tarea

Estas instrucciones describen cómo eliminar un depósito de S3 mediante Tenant Manager. También puedes

eliminar depósitos de S3 usando el ["API de gestión de inquilinos"](#) o el ["API de REST de S3"](#).

No puedes eliminar un bucket de 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, consulta ["Cómo se eliminan los objetos"](#).

Pasos

1. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.

Aparece la página «Buckets» y muestra todos los buckets de S3 existentes.

2. Utiliza el menú **Acciones** o la página de detalles de un bucket concreto.

Menú de acciones

- a. Marca la casilla de selección correspondiente a cada bucket que quieras eliminar.
- b. Selecciona **Acciones > Eliminar buckets**.

Página de detalles

- a. Selecciona el nombre de un bucket para ver sus detalles.
- b. Selecciona **Eliminar depósito**.

3. Cuando aparezca el cuadro de diálogo de confirmación, selecciona **Yes**.

StorageGRID comprueba que cada bucket esté vacío y, a continuación, elimina cada bucket. Esta operación puede tardar unos minutos.

Si un bucket no está vacío, aparece un mensaje de error. Debes ["Eliminar todos los objetos y cualquier marcador de eliminación en el bucket"](#) antes de poder eliminar el bucket.

Usa la consola S3 en StorageGRID

Puedes utilizar la consola de S3 para ver y gestionar los objetos de un bucket de S3.

La consola de S3 te permite:

- Subir, descargar, renombrar, copiar, mover y eliminar objetos
- Ver, revertir, descargar y eliminar versiones de objetos
- Buscar objetos por prefijo
- Gestiona etiquetas de objetos
- Ver metadatos del objeto
- Ver, crear, renombrar, copiar, mover y eliminar carpetas

La consola de S3 ofrece una experiencia de usuario mejorada para los casos más habituales. No está diseñada para sustituir las operaciones de la CLI o la API en todas las situaciones.



Si al utilizar la consola de S3 las operaciones tardan demasiado (por ejemplo, minutos u horas), plantéate lo siguiente:

- Reducir el número de objetos seleccionados
- Utilizar métodos no gráficos (API o CLI) para acceder a tus datos

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Si quieres gestionar objetos, perteneces a un grupo de usuarios que tiene el permiso de acceso Root. O bien, perteneces a un grupo de usuarios que tiene el permiso de usar la pestaña S3 Console y el permiso de ver todos los buckets o el permiso de gestionar todos los buckets. Consulta ["Permisos de gestión de inquilinos"](#).
- Se ha configurado una política de grupo o de bucket de S3 para el usuario. Consulta ["Usa políticas de acceso a buckets y de grupo"](#).
- Conoces el ID de la clave de acceso y la clave de acceso secreta del usuario. Opcionalmente, tienes un archivo `.csv` que contiene esta información. Consulta el ["Instrucciones para crear claves de acceso"](#).

Pasos

1. Selecciona **Storage > Buckets > *bucket name***.
2. Selecciona la pestaña Consola de S3.
3. Pega el ID de la clave de acceso y la clave de acceso secreta en los campos. Si no, selecciona **Cargar claves de acceso** y selecciona tu archivo `.csv`.
4. Selecciona **Sign in**.
5. Aparece la tabla de objetos de «bucket». Puedes gestionar los objetos según sea necesario.

Información adicional

- **Búsqueda por prefijo:** La función de búsqueda por prefijo solo busca objetos que empiecen por una palabra concreta en relación con la carpeta actual. La búsqueda no incluye objetos que contengan la palabra en otra parte. Esta regla también se aplica a los objetos dentro de las carpetas. Por ejemplo, una búsqueda de `folder1/folder2/somefile-` mostraría los objetos que están dentro de la carpeta `folder1/folder2/` y que empiezan por la palabra `somefile-`.
- **Arrastrar y soltar:** Puedes arrastrar y soltar archivos desde el gestor de archivos de tu ordenador a la consola de S3. Sin embargo, no puedes subir carpetas.
- **Operaciones con carpetas:** Cuando mueves, copias o cambias el nombre de una carpeta, todos los objetos en la carpeta se actualizan uno a uno, lo que puede llevar tiempo.
- **Eliminación permanente cuando el control de versiones del bucket está desactivado:** Cuando sobrescribes o eliminas un objeto en un bucket con el control de versiones desactivado, la operación es permanente. Consulta ["Cambiar el control de versiones de objetos para un bucket"](#).

Gestiona los servicios de la plataforma S3

Servicios de plataforma S3

Conoce los servicios de plataforma para StorageGRID

Antes de implementar los servicios de plataforma, revisa la descripción general y las consideraciones para usar estos servicios.

Para obtener información sobre S3, consulta ["Usa la API de REST de S3"](#).

Descripción general de los servicios de la plataforma

Los servicios de la plataforma StorageGRID pueden ayudarte a implementar una estrategia de nube híbrida, ya que te permiten enviar notificaciones de eventos y copias de objetos S3 y de los metadatos de dichos objetos a destinos externos.

Dado que la ubicación de destino de los servicios de plataforma suele encontrarse fuera de tu implementación de StorageGRID, estos servicios te ofrecen la potencia y la flexibilidad que supone el uso de recursos de almacenamiento externos, servicios de notificación y servicios de búsqueda o análisis para tus datos.

Se puede configurar cualquier combinación de servicios de la plataforma para un único bucket de S3. Por ejemplo, podrías configurar tanto ["Servicio CloudMirror"](#) como ["notificaciones"](#) en un bucket de S3 de StorageGRID, de modo que puedas replicar objetos específicos en Amazon Simple Storage Service (S3), mientras envías una notificación sobre cada uno de esos objetos a una aplicación de monitorización de terceros que te ayude a realizar un seguimiento de tus gastos en AWS.



El uso de los servicios de la plataforma debe habilitarse para cada cuenta de inquilino por un administrador de StorageGRID usando Grid Manager o la API de gestión de la red.

Cómo se configuran los servicios de plataforma

Los servicios de plataforma se comunican con endpoints externos que configures mediante el ["Administrador de inquilinos"](#) o el ["API de gestión de inquilinos"](#). Cada endpoint representa un destino externo, como un bucket de StorageGRID S3, un bucket de Amazon Web Services, un tema de Amazon SNS, un endpoint de webhook o un clúster de Elasticsearch alojado localmente, en AWS o en otro lugar.

Una vez que hayas creado un endpoint externo, puedes habilitar un servicio de plataforma para un bucket añadiendo una configuración XML al bucket. La configuración XML identifica los objetos sobre los que debe actuar el bucket, la acción que debe realizar el bucket y el endpoint que debe utilizar el bucket para el servicio.

Debes añadir configuraciones XML independientes para cada servicio de plataforma que quieras configurar. Por ejemplo:

- Si quieres que todos los objetos cuyas claves empiecen por `/images` se repliquen en un bucket de Amazon S3, debes añadir una configuración de replicación al bucket de origen.
- Si además quieres enviar notificaciones cuando estos objetos se almacenen en el bucket, debes añadir una configuración de notificaciones.
- Si deseas indexar los metadatos de estos objetos, debes añadir la configuración de notificación de metadatos que se utiliza para implementar la integración de la búsqueda.

El formato del archivo XML de configuración está regido por las S3 REST APIs que se usan para implementar los servicios de plataforma de StorageGRID:

Servicio de plataforma	API de REST de S3	Consulta
CloudMirror replicación	• GetBucketReplication • PutBucketReplication	• "CloudMirror replicación" • "Operaciones en cubos"
Notificaciones	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "Notificaciones" • "Operaciones en cubos"
Integración de búsqueda	• Obtener configuración de notificaciones de metadatos del bucket • PUT Bucket configuración de notificación de metadatos	• "Integración de búsqueda" • "Operaciones personalizadas de StorageGRID"

Aspectos a tener en cuenta al utilizar los servicios de la plataforma

Consideración	Detalles
Supervisión de los endpoints 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 periodo prolongado y existe una gran acumulación de solicitudes pendientes, las solicitudes adicionales de los clientes (como las solicitudes PUT) a StorageGRID fallarán. Debes volver a intentar estas solicitudes fallidas cuando el punto final vuelva a estar disponible.
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 supera la velocidad a la que el extremo de destino puede recibirlas. La limitación solo se produce cuando hay una acumulación de solicitudes en espera de enviarse al extremo de destino. El único efecto visible es que las solicitudes S3 entrantes tardarán más en ejecutarse. Si empiezas a notar una ralentización significativa del rendimiento, deberías reducir la tasa de consumo o usar un endpoint con mayor capacidad. Si la acumulación de solicitudes sigue aumentando, las operaciones S3 de los clientes (como las solicitudes PUT) acabarán fallando. Las solicitudes de CloudMirror tienen más probabilidades de verse afectadas por el rendimiento del punto final de destino porque normalmente implican más transferencia de datos que las solicitudes de integración de búsqueda o de notificación de eventos.

Consideración	Detalles
Garantías de orden	StorageGRID garantiza el orden de las operaciones realizadas sobre un objeto dentro de un sitio. Siempre que todas las operaciones realizadas sobre un objeto se lleven a cabo dentro del mismo sitio, el estado final del objeto (para replicación) siempre será igual al estado en StorageGRID. StorageGRID hace todo lo posible por ordenar las solicitudes cuando se realizan operaciones en varios sitios de StorageGRID. Por ejemplo, si escribes un objeto inicialmente en el sitio A y luego sobrescribes el mismo objeto en el sitio B, no se garantiza que el objeto final replicado por CloudMirror en el bucket de destino sea el objeto más reciente.
Eliminaciones de objetos impulsadas por ILM	Para que el comportamiento de eliminación coincida con el de AWS CRR y Amazon Simple Notification Service, no se envían solicitudes de CloudMirror ni de notificación de eventos cuando se elimina un objeto del bucket de origen debido a las reglas de ILM de StorageGRID. Por ejemplo, no se envían solicitudes de CloudMirror ni de notificación de eventos si una regla de 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 los endpoints de Kafka	En el caso de los puntos finales de Kafka, no se admite el TLS mutuo. Por lo tanto, si en la configuración de tu broker de Kafka tienes <code>ssl.client.auth</code> configurado como <code>required</code> en tu configuración, esto podría provocar problemas en la configuración de los puntos finales de Kafka. La autenticación de los endpoints de Kafka utiliza los siguientes tipos de autenticación. Estos tipos son diferentes de los que se usan para la autenticación de otros endpoints, como Amazon SNS, y requieren credenciales de nombre de usuario y contraseña. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 Nota: La configuración del proxy de almacenamiento no se aplica a los endpoints de los servicios de la plataforma Kafka.

Consideraciones para usar el servicio de replicación de CloudMirror

Consideración	Detalles
Estado de la replicación	StorageGRID no admite el encabezado <code>x-amz-replication-status</code> .

Consideración	Detalles
Tamaño del objeto	El tamaño máximo de los objetos que se pueden replicar en un bucket de destino mediante el servicio de replicación CloudMirror es de 5 TiB, que es el mismo que el tamaño de objeto máximo <i>admitido</i>. Nota: El tamaño máximo <i>recomendado</i> para una sola operación de PutObject es de 5 GiB (5,368,709,120 bytes). Si tienes objetos que superan los 5 GiB, utiliza en su lugar la subida en varias partes.
Control de versiones de los buckets e identificadores de versión	Si el bucket de S3 de origen en StorageGRID tiene activado el control de versiones, también debes activar el control de versiones en el bucket de destino. Al utilizar el control de versiones, ten en cuenta que el orden de las versiones de los objetos en el bucket de destino es un esfuerzo máximo y no está garantizado por el servicio CloudMirror, debido a las limitaciones del protocolo S3. Nota: Los identificadores de versión del depósito de origen en StorageGRID no guardan relación con los identificadores de versión del depósito de destino.
Etiquetado de versiones de objetos	El servicio CloudMirror no replica ninguna solicitud de PutObjectTagging o DeleteObjectTagging que incluya un identificador de versión, debido a las limitaciones del protocolo S3. Porque los identificadores de versión del origen y del destino no están relacionados, no hay forma de garantizar que se replique una actualización de etiqueta en un identificador de versión específico. Por el contrario, el servicio CloudMirror sí replica las solicitudes PutObjectTagging o DeleteObjectTagging que no especifican un identificador de versión. Estas solicitudes actualizan las etiquetas de la clave más reciente (o de la versión más reciente si el bucket está versionado). Las incorporaciones normales con etiquetas (no las actualizaciones de etiquetas) también se replican.
Cargas multiparte y valores ETag	Al replicar objetos que se cargaron mediante una carga multiparte, el servicio CloudMirror no conserva las partes. Como resultado, el valor ETag para el objeto replicado será diferente al valor ETag 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 intentas ingestar 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.
Depósito con S3 Object Lock activado	La replicación no es compatible con los buckets de origen o destino que tengan activado S3 Object Lock.

Conoce el servicio de replicación StorageGRID CloudMirror

Puedes habilitar la replicación CloudMirror para un bucket de S3 si quieres que StorageGRID replique los objetos especificados que se agreguen al bucket en uno o más buckets de destino externos.

Por ejemplo, podrías usar la replicación CloudMirror para reflejar registros específicos de clientes en Amazon S3 y luego aprovechar los servicios de AWS para hacer análisis de tus datos.



CloudMirror replication no es compatible si el bucket de origen tiene activado S3 Object Lock.

CloudMirror e ILM

La replicación de CloudMirror funciona de forma independiente a las políticas de ILM activas del grid. El servicio CloudMirror replica los objetos a medida que se guardan en el bucket de origen y los entrega en el bucket de destino lo antes posible. La entrega de los objetos replicados se activa cuando la ingesta del objeto se realiza correctamente.

CloudMirror y la replicación entre grids

La replicación CloudMirror tiene importantes similitudes y diferencias con la función de replicación entre grids. Consulta ["Compara la replicación entre grids y la replicación CloudMirror"](#).

CloudMirror y buckets de S3

La replicación de CloudMirror normalmente se configura para usar un bucket de S3 externo como destino. Sin embargo, también puedes configurar la replicación para usar otro despliegue de StorageGRID o cualquier servicio compatible con S3.

Buckets existentes

Cuando habilitas la replicación de CloudMirror para un bucket existente, solo los nuevos objetos añadidos a ese bucket se replican. Los objetos existentes en el bucket no se replican. Para forzar la replicación de los objetos existentes, puedes actualizar los metadatos del objeto existente realizando una copia del objeto.



Si usas la replicación de CloudMirror para copiar objetos a un destino de Amazon S3, ten en cuenta que Amazon S3 limita el tamaño de los metadatos definidos por el usuario en cada cabecera de solicitud PUT a 2 KB. Si un objeto tiene metadatos definidos por el usuario de más de 2 KB, ese objeto no se replicará.

Varios depósitos de destino

Para replicar objetos de un solo bucket en varios buckets de destino, especifica el destino de cada regla en el XML de configuración de replicación. No puedes replicar un objeto en más de un bucket al mismo tiempo.

Depósitos con o sin control de versiones

Puedes configurar la replicación de CloudMirror en buckets con o sin versiones. Los buckets de destino pueden tener o no versiones. Puedes utilizar cualquier combinación de buckets con y sin versiones. Por ejemplo, podrías especificar un bucket con versiones como destino para un bucket de origen sin versiones, o viceversa. También puedes replicar entre buckets sin versiones.

Eliminación, bucles de replicación y eventos

Comportamiento de borrado

Es igual que el comportamiento de eliminación del servicio Amazon S3, Cross-Region Replication (CRR). Eliminar un objeto en un bucket de origen nunca elimina un objeto replicado en el de destino. Si tanto el bucket de origen como el de destino tienen control de versiones, se replica el delete marker. Si el bucket de destino no tiene control de versiones, al eliminar un objeto en el bucket de origen no se replica el delete marker en el bucket de destino ni se elimina el objeto de destino.

Protección contra los bucles de replicación

A medida que los objetos se replican en el bucket de destino, StorageGRID los marca como "réplicas". Un bucket de StorageGRID de destino no volverá a replicar los objetos marcados como réplicas, lo que te protege de bucles de replicación accidentales. Este marcado de réplicas es interno de StorageGRID y no te impide aprovechar AWS CRR cuando utilizas un bucket de Amazon S3 como destino.



La cabecera personalizada utilizada para marcar una réplica es `x-ntap-sg-replica`. Esta marca evita un reflejo en cascada. StorageGRID sí admite un CloudMirror bidireccional entre dos grids.

Eventos en el bucket de destino

No se garantizan la unicidad ni el orden de los eventos en el bucket de destino. Es posible que se entregue más de una copia idéntica de un objeto de origen en el destino como resultado de las operaciones realizadas para garantizar el éxito de la entrega. En casos poco comunes, cuando el mismo objeto se actualiza de forma simultánea desde dos o más sitios de StorageGRID diferentes, es posible que el orden de las operaciones en el bucket de destino no coincida con el orden de los eventos en el bucket de origen.

Conoce las notificaciones de eventos de StorageGRID para buckets S3

Puedes activar las notificaciones de eventos para un bucket de S3 si deseas que StorageGRID envíe notificaciones sobre eventos específicos a un clúster de Kafka, un endpoint de webhook o Amazon Simple Notification Service.

Por ejemplo, podrías configurar alertas para que se envíen a los administradores sobre cada objeto añadido a un bucket, donde los objetos representan archivos de registro asociados con un evento crítico del sistema.

Las notificaciones de eventos se crean en el bucket de origen tal como se especifica en la configuración de notificaciones y se entregan en el destino. Si un evento asociado a un objeto se realiza correctamente, se crea una notificación sobre ese evento y se pone en cola para su entrega.

No se garantiza la unicidad ni el orden de las notificaciones. Puede que se entregue más de una notificación de un evento al destino como resultado de las operaciones realizadas para garantizar el éxito de la entrega. Y como la entrega es asíncrona, no se garantiza que el orden de las notificaciones en el destino coincida con el orden de los eventos en el bucket de origen, especialmente para operaciones que se originan en diferentes sitios de StorageGRID. Puedes usar la clave `sequencer` en el mensaje del evento para determinar el orden de los eventos de 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:ObjectCreated:`
 - `s3:ObjectCreated:Put`
 - `s3:ObjectCreated:Post`
 - `s3:ObjectCreated:Copy`
 - `s3:ObjectCreated:CompleteMultipartUpload`
 - `s3:ObjectRemoved:`
 - `s3:ObjectRemoved>Delete`
 - `s3:ObjectRemoved>DeleteMarkerCreated`
 - `s3:ObjectRestore:post`

- 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
eventSource	sgws:s3
awsRegion	<i>no incluido</i>
x-amz-id-2	<i>no incluido</i>
arn	urn:sgws:s3:::bucket_name

Conoce el servicio de integración de búsquedas de StorageGRID

Puedes habilitar la integración de búsqueda para un bucket de S3 si deseas utilizar un servicio externo de búsqueda y análisis de datos para los metadatos de tus objetos.

El servicio de integración de búsqueda es un servicio personalizado de StorageGRID que envía de forma automática y asíncrona los metadatos de los objetos S3 a un endpoint de destino cada vez que se crea o se elimina un objeto, o bien cuando se actualizan sus metadatos o etiquetas. A continuación, puedes utilizar herramientas sofisticadas de búsqueda, análisis de datos, visualización o aprendizaje automático proporcionadas por el servicio de destino para buscar, analizar y obtener información valiosa de los datos de tus objetos.

Por ejemplo, podrías configurar tus buckets para que envíen los metadatos de los objetos de S3 a un servicio remoto de Elasticsearch. Luego, podrías usar Elasticsearch para realizar búsquedas en todos los buckets y hacer análisis sofisticados de los patrones presentes en los metadatos de tus objetos.

Aunque la integración con Elasticsearch se puede configurar en un bucket con S3 Object Lock activado, los metadatos de S3 Object Lock (incluidos Retain Until Date y Legal Hold status) de los objetos no se incluirán en los metadatos enviados a Elasticsearch.



Dado que el servicio de integración de búsqueda hace que los metadatos de los objetos se envíen a un destino, su archivo XML de configuración se denomina "XML de configuración de notificación de metadatos". Este archivo XML de configuración es diferente del "XML de configuración de notificación" que se utiliza para habilitar las notificaciones de eventos.

Integración de búsqueda y depósitos de S3

Puedes habilitar el servicio de integración de búsqueda para cualquier bucket, tanto versionado como no versionado. La integración de búsqueda se configura asociando la configuración XML de notificación de metadatos con el bucket, lo que especifica sobre qué objetos se debe actuar y el destino de los metadatos de los objetos.

Las notificaciones de metadatos se generan en forma de un documento JSON nombrado con el nombre del bucket, el nombre del objeto y el ID de versión, si lo hay. 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 de usuario.



Para las etiquetas y los metadatos de usuario, StorageGRID pasa las fechas y los números a Elasticsearch como cadenas o como notificaciones de eventos de S3. Para configurar Elasticsearch para que interprete estas cadenas como fechas o números, sigue las instrucciones de Elasticsearch para el mapeo dinámico de campos y para el mapeo de formatos de fecha. Debes habilitar los mapeos dinámicos de campos en el índice antes de configurar el servicio de integración de búsqueda. Una vez indexado un documento, no puedes editar los tipos de campo del documento en el índice.

Notificaciones de búsqueda

Las notificaciones de metadatos se generan y se ponen en cola para su envío cada vez que:

- Se crea un objeto.
- Un objeto se elimina, incluso cuando los objetos se eliminan como resultado de la operación de la política de ILM de la grid.
- Se añaden, actualizan o eliminan metadatos o etiquetas de los objetos. En cada actualización se envía siempre el conjunto completo de metadatos y etiquetas, no solo los valores modificados.

Una vez que añadas el archivo XML de configuración de notificaciones de metadatos a un bucket, se enviarán notificaciones por cualquier objeto nuevo que crees y por cualquier objeto que modifiques al actualizar sus datos, metadatos de usuario o etiquetas. Sin embargo, no se envían notificaciones para los objetos que ya estaban en el bucket. Para asegurarte de que los metadatos de todos los objetos del bucket se envíen al destino, deberías hacer una de las siguientes cosas:

- Configura el servicio de integración de búsqueda inmediatamente después de crear el bucket y antes de añadir cualquier objeto.
- Realiza una acción sobre todos los objetos que ya están en el bucket para que se envíe un mensaje de notificación de metadatos al destino.

Servicio de integración de búsqueda y Elasticsearch

El servicio de integración de búsqueda de StorageGRID admite un clúster de 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 archivo XML de configuración del servicio. Utiliza el "[Herramienta NetApp Interoperability Matrix Tool](#)" para determinar las versiones compatibles de Elasticsearch.

Gestiona los puntos de conexión de los servicios de la plataforma

Configura los endpoints de servicios de plataforma en StorageGRID

Antes de poder configurar un servicio de plataforma para un bucket, debes configurar al menos un endpoint como destino para el servicio de plataforma.

El acceso a los servicios de la plataforma lo habilita un administrador de StorageGRID para cada inquilino. Para crear o usar un endpoint de servicios de la plataforma, debes ser un usuario inquilino con permiso de Manage endpoints o acceso Root, en una grid cuya red haya sido configurada para permitir que los Storage Nodes accedan a recursos de endpoint externos. Para un solo inquilino, puedes configurar un máximo de 500 endpoints de servicios de la plataforma. Contacta a tu administrador de StorageGRID para más información.

¿Qué es un endpoint de servicios de plataforma?

Un punto final de servicios de la plataforma especifica la información que StorageGRID necesita para acceder

al destino externo.

Por ejemplo, si quieres replicar objetos de un bucket de StorageGRID a un bucket de Amazon S3, creas un punto de conexión de servicios de la plataforma que incluye 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 endpoint, por lo que debes configurar al menos un endpoint para cada servicio de plataforma que tengas pensado utilizar. Después de definir un endpoint de servicios de plataforma, utilizas el URN del endpoint como destino en el XML de configuración que se usa para habilitar el servicio.

Puedes usar el mismo endpoint como destino para más de un bucket de origen. Por ejemplo, podrías configurar varios buckets de origen para enviar metadatos de objetos al mismo endpoint de integración de búsqueda para poder realizar búsquedas en varios buckets. También puedes configurar un bucket de origen para que use más de un endpoint como destino, lo que te 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.

Endpoints para la replicación de CloudMirror

StorageGRID admite endpoints de replicación que representan buckets de S3. Estos buckets pueden estar alojados en Amazon Web Services, en el mismo despliegue de StorageGRID o en uno remoto, o en otro servicio.

Puntos finales para notificaciones

StorageGRID es compatible con Amazon SNS, Kafka y endpoints de webhook. Simple Queue Service (SQS) y los endpoints de AWS Lambda no son compatibles.

Para los endpoints de Kafka, no se admite el TLS mutuo. Como resultado, si tienes `ssl.client.auth` configurado como `required` en la configuración de tu broker de Kafka, podría causar problemas en la configuración del endpoint de Kafka.

Puntos finales del servicio de integración de búsqueda

StorageGRID admite puntos finales de integración de búsqueda que representan clústeres de Elasticsearch. Estos clústeres de Elasticsearch pueden estar ubicados en un centro de datos local o alojados en una nube de AWS o en cualquier otro lugar.

El punto final de integración de búsqueda hace referencia a un índice y un tipo específicos de Elasticsearch. Debes crear el índice en Elasticsearch antes de crear el punto final en StorageGRID o la creación del punto final fallará. No necesitas crear el tipo antes de crear el punto final. StorageGRID creará el tipo si es necesario cuando envíe los metadatos del objeto al punto final.

Información relacionada

["Administrar StorageGRID"](#)

Especifica un URN para un endpoint de servicios de plataforma StorageGRID

Al crear un punto final de servicios de plataforma, debes especificar un nombre de recurso único (URN). Utilizarás el URN para hacer referencia al punto final cuando crees un archivo XML de configuración para el servicio de plataforma. El URN de cada punto final debe ser único.

StorageGRID valida los endpoints de servicios de plataforma a medida que los creas. Antes de crear un endpoint de servicios de plataforma, confirma que el recurso especificado en el endpoint existe y que se puede acceder a él.

Elementos URN

El URN para un endpoint de servicios de plataforma debe comenzar con `arn:aws` o con `urn:mystore`, de la siguiente manera:

- Si el servicio está alojado en Amazon Web Services (AWS), utiliza `arn:aws`
- Si el servicio está alojado en Google Cloud Platform (GCP), usa `arn:aws`
- Si el servicio está alojado localmente, usa `urn:mystore`

Por ejemplo, si estás especificando el URN para un endpoint de CloudMirror alojado en StorageGRID, el URN podría comenzar con `urn:sgws`.

El siguiente elemento del URN especifica el tipo de servicio de plataforma, como se indica a continuación:

Servicio	Tipo
CloudMirror replicación	s3
Notificaciones	sns, kafka, o webhook
Integración de búsqueda	es

Por ejemplo, para continuar especificando la URN de un endpoint de CloudMirror alojado en StorageGRID, añadirías `s3` para obtener `urn:sgws:s3`.

Para la mayoría de los endpoints, el elemento final del URN identifica el recurso de destino específico en la URI de destino, por ejemplo, `sns-topic-name`.

En el caso de los endpoints de webhook, el recurso de destino es la propia URI de destino.

Servicio	Recurso específico
CloudMirror replicación	bucket-name
Notificaciones	sns-topic-name o kafka-topic-name Nota: En el caso de los puntos finales de webhook, el último elemento del URN puede ser cualquier cadena, siempre y cuando el URN del punto final sea único.
Integración de búsqueda	domain-name/index-name/type-name Nota: Si el clúster de Elasticsearch no está configurado para crear índices automáticamente, deberás crear el índice manualmente antes de crear el endpoint.

URNs 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 endpoint de integración de búsqueda de AWS, el `domain-name` debe incluir la cadena literal `domain/`, como se muestra aquí.

URNs para servicios alojados localmente

Cuando utilices servicios alojados localmente en lugar de servicios en la nube, puedes 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. Puedes dejar en blanco los elementos indicados como opcionales, o puedes especificarlos de cualquier forma que te ayude a identificar el recurso y hacer que el URN sea único. Por ejemplo:

- Replicación de CloudMirror:

```
urn:mysite:s3:optional:optional:bucket-name
```

Para un endpoint de CloudMirror alojado en StorageGRID, puedes especificar un URN válido que comience con `urn:sgws:`

```
urn:sgws:s3:optional:optional:bucket-name
```

- Notificaciones:

Especifica un endpoint de Amazon Simple Notification Service:

```
urn:mysite:sns:optional:optional:sns-topic-name
```

Especifica un endpoint de Kafka:

```
urn:mysite:kafka:optional:optional:kafka-topic-name
```

Especifica un endpoint de webhook:

```
urn:mysite:webhook:optional:optional:webhook-name
```

- Integración de búsqueda:

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```



Para los endpoints de integración de búsqueda alojados localmente, el `domain-name` elemento puede ser cualquier cadena siempre que el URN del endpoint sea único.

Crear un endpoint de servicios de plataforma StorageGRID

Debes crear al menos un punto final del tipo correcto antes de poder habilitar un servicio de plataforma.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Los servicios de la plataforma fueron habilitados para tu cuenta de inquilino por un administrador de StorageGRID.
- Pertenece a un grupo de usuarios que tiene el ["Gestiona endpoints o permisos de acceso de usuario raíz"](#).
- Se ha creado el recurso al que hace referencia el endpoint de los servicios de la plataforma:
 - CloudMirror replication: depósito S3
 - Notificación de eventos: tema de Amazon Simple Notification Service (Amazon SNS), tema de Kafka o endpoint de webhook
 - Notificación de búsqueda: índice de Elasticsearch, si el clúster de destino no está configurado para crear índices automáticamente.
- Dispones de la información sobre el recurso de destino:
 - Servidor y puerto del Identificador Unificado de Recursos (URI)



Si planeas usar un bucket alojado en un sistema StorageGRID como endpoint para la replicación de CloudMirror, contacta al administrador del grid para saber qué valores necesitas ingresar.

- Nombre único de recurso (URN)

["Especifica el URN para el endpoint de los servicios de plataforma"](#)

- Credenciales de autenticación (si son necesarias):

Puntos finales de integración de búsqueda

Para los puntos finales de integración de búsqueda, puedes utilizar las siguientes credenciales:

- Clave de acceso: ID de clave de acceso y clave secreta de acceso
- HTTP básico: nombre de usuario y contraseña

CloudMirror puntos finales de replicación

Para los puntos finales de replicación de CloudMirror, puedes utilizar las siguientes credenciales:

- Clave de acceso: ID de clave de acceso y clave secreta de acceso
- CAP (Portal de acceso C2S): URL de credenciales temporales, certificados de servidor y de cliente, claves de cliente y una frase de contraseña opcional para la clave privada del cliente.

Puntos de conexión de Amazon SNS

Para los puntos de conexión de Amazon SNS, puedes utilizar las siguientes credenciales:

- Clave de acceso: ID de clave de acceso y clave secreta de acceso

Puntos de conexión de Kafka

Para los puntos finales de Kafka, puedes 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 requiere la verificación del certificado)

- Si las funciones de seguridad de Elasticsearch están activadas, tienes el privilegio monitor cluster para pruebas de conectividad, y el privilegio write index o ambos privilegios index y delete index para actualizaciones de documentos.

Pasos

1. Selecciona **STORAGE (S3) > Puntos de conexión de los servicios de la plataforma**. Aparece la página Puntos de conexión de los servicios de la plataforma.
2. Selecciona **Crear endpoint**.
3. Introduce un nombre de visualización que describa brevemente el endpoint y su finalidad.

El tipo de servicio de plataforma que admite el endpoint aparece junto al nombre de este cuando aparece en la página Endpoints, así que no necesitas incluir esa información en el nombre.

4. En el campo **URI**, especifica el identificador único de recurso (URI) del endpoint.

Utiliza uno de los siguientes formatos:

```
https://host:port
http://host:port
```

Si no especificas un puerto, se usan los siguientes puertos predeterminados:

- Puerto 443 para las URI HTTPS y puerto 80 para las URI HTTP (la mayoría de los endpoints)
- Puerto 9092 para URI de HTTPS y HTTP (solo endpoints 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 de la IP virtual (VIP) del grupo de alta disponibilidad (HA) de StorageGRID, y `10443` representa el puerto definido en el endpoint del equilibrador de carga.



Siempre que sea posible, debes conectarte a un grupo de alta disponibilidad (HA) de nodos con equilibrio de carga para evitar un punto único de fallo.

Del mismo modo, el URI de un bucket alojado en AWS podría ser:

```
https://s3-aws-region.amazonaws.com
```



Si el endpoint se utiliza para el servicio de replicación CloudMirror, no incluyas el nombre del bucket en la URI. Incluyes el nombre del bucket en el campo **URN**.

5. Introduce el nombre único de recurso (URN) del endpoint.



No puedes cambiar el URN de un endpoint después de que se ha creado.

6. Selecciona **Continuar**.

7. Selecciona un valor para **Tipo de autenticación**.



Si quieres autenticación para los endpoints de webhook, configura Mutual Transport Layer Security (mTLS) en [Paso 9](#).

Puntos finales de integración de búsqueda

Introduce o sube las credenciales de un endpoint de integración de búsqueda.

Las credenciales que facilites deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Permite el acceso anónimo al destino. Solo funciona con endpoints que tengan la seguridad desactivada.	Sin autenticación.
Clave de acceso	Utiliza credenciales al estilo de 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 con el destino.	• Nombre de usuario • Password

CloudMirror puntos finales de replicación

Introduce o carga las credenciales para un extremo de replicación de CloudMirror.

Las credenciales que facilites deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Permite el acceso anónimo al destino. Solo funciona con endpoints que tengan la seguridad desactivada.	Sin autenticación.
Clave de acceso	Utiliza credenciales al estilo de AWS para autenticar las conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta
CAP (Portal de acceso C2S)	Utiliza certificados y claves para autenticar las conexiones con el destino.	• URL de credenciales temporales • Certificado CA del servidor (carga de archivo PEM) • Certificado de cliente (carga de archivo PEM) • Clave privada del cliente (carga de archivo PEM, formato cifrado con OpenSSL o formato de clave privada sin cifrar) • Contraseña de la clave privada del cliente (opcional)

Puntos de conexión de Amazon SNS

Introduce o sube las credenciales para un endpoint de Amazon SNS.

Las credenciales que facilites deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Permite el acceso anónimo al destino. Solo funciona con endpoints que tengan la seguridad desactivada.	Sin autenticación.
Clave de acceso	Utiliza credenciales al estilo de AWS para autenticar las conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta

Puntos de conexión de Kafka

Introduce o sube las credenciales para un endpoint de Kafka.

Las credenciales que facilites deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Permite el acceso anónimo al destino. Solo funciona con endpoints que tengan la seguridad desactivada.	Sin autenticación.
SASL/PLAIN	Utiliza un nombre de usuario y una contraseña en texto sin cifrar para autenticar las conexiones con el destino.	• Nombre de usuario • Password
SASL/SCRAM-SHA-256	Utiliza un nombre de usuario y una contraseña mediante un protocolo de desafío-respuesta y el algoritmo de hash SHA-256 para autenticar las conexiones con el destino.	• Nombre de usuario • Password
SASL/SCRAM-SHA-512	Utiliza un nombre de usuario y una contraseña mediante un protocolo de desafío-respuesta y el algoritmo de hash SHA-512 para autenticar las conexiones con el destino.	• Nombre de usuario • Password

Selecciona **Usar autenticación mediante delegación** si el nombre de usuario y la contraseña proceden de un token de delegación obtenido de un clúster de Kafka.

8. Selecciona **Continuar**.

9. Selecciona un botón de opción en **Verificar certificados** para elegir cómo se verifica la conexión TLS con el endpoint.

La mayoría de los endpoints

Comprueba la conexión TLS para la integración de Search, la replicación de CloudMirror, Amazon SNS o los endpoints de Kafka.

Tipo de verificación del certificado	Descripción
TLS	Valida el certificado del servidor para las conexiones TLS al recurso de endpoint.
Deshabilitado	La verificación de certificados está desactivada. Esta opción no es segura.
Usa un certificado de CA personalizado	El certificado CA personalizado se utiliza para verificar la identidad del servidor al conectarse al endpoint.
Utiliza el certificado CA del sistema operativo	Utiliza el certificado CA de Grid predeterminado instalado en el sistema operativo para proteger las conexiones.

Solo endpoints de webhook

Comprueba la conexión TLS de los puntos finales de los webhooks.

Tipo de verificación del certificado	Descripción
TLS	Valida el certificado del servidor para las conexiones TLS al recurso de endpoint.
mTLS	Valida los certificados del cliente y del servidor para las conexiones Mutual TLS con el recurso endpoint.
Deshabilitado	La verificación de certificados está desactivada. Esta opción no es segura.
Usa un certificado de CA personalizado	El certificado CA personalizado se utiliza para verificar la identidad del servidor al conectarse al endpoint.

Al seleccionar **mTLS**, estas opciones pasan a estar disponibles.

Tipo de verificación del certificado	Descripción
No verificar el certificado del servidor	Desactiva la verificación del certificado del servidor, lo que significa que no se verifica la identidad del servidor. Esta opción no es segura.
Certificado de cliente	El certificado de cliente se utiliza para verificar la identidad del cliente al conectarse al endpoint.

Tipo de verificación del certificado	Descripción
Clave privada del cliente	La clave privada del certificado de cliente. Si está cifrada, debe usar el formato tradicional PKCS #1 (no se admite el formato PKCS #8).
Contraseña de la clave privada del cliente	La frase de contraseña para descifrar la clave privada del cliente. Si la clave privada no está cifrada, deja esto en blanco.

10. Selecciona **Probar y crear endpoint**.

- Aparece un mensaje de éxito si se puede acceder al endpoint con las credenciales especificadas. La conexión con el endpoint se valida desde un nodo en cada sitio.
- Aparece un mensaje de error si falla la validación del endpoint. Si necesitas modificar el endpoint para corregir el error, selecciona **Return to endpoint details** y actualiza la información. Luego, selecciona **Test and create endpoint**.



La creación del endpoint falla si los servicios de plataforma no están habilitados para tu cuenta de inquilino. Contacta con tu administrador de StorageGRID.

Una vez que hayas configurado un punto final, puedes utilizar su URN para configurar un servicio de la plataforma.

Información relacionada

- ["Especifica el URN para el endpoint de los servicios de plataforma"](#)
- ["Configura la replicación de CloudMirror"](#)
- ["Configura las notificaciones de eventos"](#)
- ["Configura el servicio de integración de búsqueda"](#)

Prueba la conexión para un endpoint de servicios de plataforma StorageGRID

Si la conexión a un servicio de la plataforma ha cambiado, puedes probar la conexión del endpoint para validar que el recurso de destino existe y que se puede acceder a él usando las credenciales que especificaste.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el ["Gestiona endpoints o permisos de acceso de usuario raíz"](#).

Acerca de esta tarea

StorageGRID no comprueba que las credenciales tengan los permisos correctos.

Pasos

1. Selecciona **STORAGE (S3) > Platform services endpoints**.

Aparece la página «Puntos finales de los servicios de la plataforma» y muestra la lista de puntos finales de

los servicios de la plataforma que ya se han configurado.

2. Selecciona el punto final cuya conexión quieras comprobar.

Aparece la página de detalles del endpoint.

3. Selecciona **Probar conexión**.

- Aparece un mensaje de éxito si se puede acceder al endpoint con las credenciales especificadas. La conexión con el endpoint se valida desde un nodo en cada sitio.
- Aparece un mensaje de error si falla la validación del endpoint. Si necesitas modificar el endpoint para corregir el error, selecciona **Configuration** y actualiza la información. Luego, selecciona **Test and save changes**.

Edita un punto final de servicios de plataforma en StorageGRID

Puedes editar la configuración de un punto final de servicios de la plataforma para cambiar su nombre, su URI u otros detalles. Por ejemplo, es posible que tengas que actualizar credenciales caducadas o cambiar el URI para que apunte a un índice de Elasticsearch de respaldo en caso de conmutación por error. No puedes cambiar el URN de un punto final de servicios de la plataforma.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el ["Gestiona endpoints o permisos de acceso de usuario raíz"](#).

Pasos

1. Selecciona **STORAGE (S3) > Platform services endpoints**.

Aparece la página «Puntos finales de los servicios de la plataforma» y muestra la lista de puntos finales de los servicios de la plataforma que ya se han configurado.

2. Selecciona el punto final que quieras editar.

Aparece la página de detalles del endpoint.

3. Selecciona **Configuración**.

4. Si es necesario, cambia la configuración del endpoint.



No puedes cambiar el URN de un endpoint después de que se ha creado.

- a. Para cambiar el nombre que se muestra para el punto final, selecciona el icono de edición .
- b. Modifica el URI según sea necesario.
- c. Si es necesario, cambia el tipo de autenticación.
 - Para la autenticación mediante clave de acceso, modifica la clave según sea necesario seleccionando **Editar clave S3** y pegando un nuevo access key ID y una nueva secret access key. Si necesitas cancelar los cambios, selecciona **Deshacer edición de clave S3**.
 - Para la autenticación en CAP (C2S Access Portal), cambia la URL de las credenciales temporales o la frase de contraseña opcional de la clave privada del cliente y sube los nuevos archivos de

certificado y clave según sea necesario.



La clave privada del cliente debe estar en formato cifrado con OpenSSL o en formato de clave privada sin cifrar.

d. Si es necesario, cambia el método para verificar certificados.

5. Selecciona **Probar y guardar cambios**.

- Aparece un mensaje de éxito si se puede acceder al punto final utilizando las credenciales especificadas. La conexión con el punto final se verifica desde un nodo de cada sitio.
- Aparece un mensaje de error si falla la validación del punto final. Modifica el punto final para corregir el error y luego selecciona **Probar y guardar cambios**.

Eliminar un endpoint de servicios de plataforma de StorageGRID

Puedes eliminar un endpoint si ya no quieres usar el servicio de plataforma asociado.

Antes de empezar

- Has iniciado sesión en el Tenant Manager con un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el ["Gestiona endpoints o permisos de acceso de usuario raíz"](#).

Pasos

1. Selecciona **STORAGE (S3) > Platform services endpoints**.

Aparece la página «Puntos finales de los servicios de la plataforma» y muestra la lista de puntos finales de los servicios de la plataforma que ya se han configurado.

2. Marca la casilla de selección correspondiente a cada endpoint que quieras eliminar.



Si eliminas un endpoint de servicios de plataforma que está en uso, el servicio de plataforma asociado se deshabilitará para cualquier bucket que use dicho endpoint. Cualquier solicitud que aún no se haya completado se descartará. Se seguirán generando nuevas solicitudes hasta que cambies la configuración de tu bucket para que ya no haga referencia al URN eliminado. StorageGRID notificará estas solicitudes como errores irrecuperables.

3. Selecciona **Acciones > Eliminar endpoint**.

Aparece un mensaje de confirmación.

4. Selecciona **Eliminar punto final**.

Soluciona errores en el punto final de los servicios de la plataforma StorageGRID

Si se produce un error cuando StorageGRID intenta comunicarse con un endpoint de servicios de plataforma, aparecerá un mensaje en el panel de control. En la página Endpoints de servicios de plataforma, la columna Último error indica hace cuánto tiempo se produjo el error. No se mostrará ningún error si los permisos asociados a las credenciales de un endpoint son incorrectos.

Determina si se ha producido un error

Si se ha producido algún error en los puntos finales de los servicios de la plataforma en los últimos 7 días, el panel de control de Tenant Manager muestra un mensaje de alerta. Puedes ir a la página de puntos finales de los 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 de control también aparece en la parte superior de la página de endpoints de servicios de la plataforma. Para ver un mensaje de error más detallado:

Pasos

1. En la lista de endpoints, selecciona el endpoint que presenta el error.
2. En la página de detalles del punto final, selecciona **Conexión**. Esta pestaña muestra únicamente el error más reciente de un punto final e indica cuánto tiempo hace que se produjo el error. Los errores que incluyen el icono de la X roja  ocurrieron en los últimos 7 días.

Comprueba si el error sigue vigente

Es posible que algunos errores sigan apareciendo en la columna **Último error** incluso después de haberse resuelto. Para ver si un error sigue activo o para forzar la eliminación de un error resuelto de la tabla:

Pasos

1. Selecciona el punto final.

Aparece la página de detalles del endpoint.
2. Selecciona **Conexión** > **Probar conexión**.

Al seleccionar **Probar conexión**, StorageGRID valida que el endpoint de servicios de plataforma exista y que se pueda acceder a él con las credenciales actuales. La conexión con el endpoint se valida desde un nodo en cada sitio.

Resolver errores de endpoint

Puedes usar el mensaje **Último error** en la página de detalles del endpoint para ayudarte a determinar qué está causando el error. Algunos errores pueden requerir que edites el endpoint para resolver el problema. Por ejemplo, puede ocurrir un error de CloudMirroring si StorageGRID no puede acceder al bucket de destino de Amazon S3 porque no tiene los permisos de acceso correctos o la clave de acceso ha expirado. El mensaje es "Either the endpoint credentials or the destination access needs to be updated," y los detalles son "AccessDenied" o "InvalidAccessKeyId".

Si necesitas modificar el endpoint para solucionar un error, al seleccionar **Probar y guardar cambios** StorageGRID valida el endpoint actualizado y confirma que se puede acceder a él con las credenciales actuales. La conexión con el endpoint se valida desde un nodo de cada sitio.

Pasos

1. Selecciona el punto final.
2. En la página de detalles del punto final, selecciona **Configuración**.
3. Modifica la configuración del punto final según sea necesario.

4. Selecciona **Conexión** > **Probar conexión**.

Credenciales de endpoint con permisos insuficientes

Cuando StorageGRID valida un punto final de servicios de la plataforma, comprueba que las credenciales de dicho punto final puedan utilizarse para contactar con el recurso de destino y realiza una comprobación básica de permisos. Sin embargo, StorageGRID no valida todos los permisos necesarios para determinadas operaciones de los servicios de la plataforma. Por este motivo, si recibes un error al intentar usar un servicio de la plataforma (como "403 Forbidden"), revisa los permisos asociados a las credenciales del punto final.

Información relacionada

- [Administrar StorageGRID](#) > [Solucionar problemas de los servicios de la plataforma](#)
- ["Crear un endpoint de servicios de plataforma"](#)
- ["Probar la conexión para el endpoint de los servicios de la plataforma"](#)
- ["Editar el endpoint de los servicios de plataforma"](#)

Configura la replicación CloudMirror en StorageGRID

Para habilitar la replicación de CloudMirror para un bucket, creas y aplicas un XML de configuración de replicación de bucket válido.

Antes de empezar

- Los servicios de la plataforma fueron habilitados para tu cuenta de inquilino por un administrador de StorageGRID.
- Ya has creado un bucket que servirá como origen de replicación.
- El punto final que pretendes utilizar como destino para la replicación de CloudMirror ya existe y tienes su URN.
- Pertenece a un grupo de usuarios que tiene el ["Gestiona todos los buckets o permiso de acceso a raíz"](#). Estos permisos anulan la configuración de permisos de las políticas de grupo o de bucket al configurar el bucket mediante Tenant Manager.

Acerca de esta tarea

La replicación de CloudMirror copia objetos desde un bucket de origen a un bucket de destino especificado en un endpoint.

Para obtener información general sobre la replicación de buckets y cómo configurarla, consulta ["Documentación de Amazon Simple Storage Service \(S3\): replicación de objetos"](#). Para obtener información sobre cómo StorageGRID implementa GetBucketReplication, DeleteBucketReplication y PutBucketReplication, consulta la ["Operaciones en cubos"](#).



La replicación de CloudMirror tiene importantes similitudes y diferencias con la función de replicación entre grids. Para obtener más información, consulta ["Compara la replicación entre grids y la replicación CloudMirror"](#).

Ten en cuenta los siguientes requisitos y características cuando configures la replicación de CloudMirror:

- Al crear y aplicar un archivo XML válido de configuración de replicación de un bucket, este debe usar el URN de un endpoint de bucket de S3 para cada destino.
- La replicación no es compatible con los buckets de origen o destino que tengan activado S3 Object Lock.

- Si activas la replicación CloudMirror en un bucket que contiene objetos, los nuevos objetos añadidos al bucket se replican, pero los objetos ya existentes en el bucket no se replican. Debes actualizar los objetos existentes para activar la replicación.
- Si especificas una clase de almacenamiento en el XML de configuración de replicación, StorageGRID usará esa clase al realizar operaciones en el endpoint de S3 de destino. El endpoint de destino también debe admitir la clase de almacenamiento especificada. Asegúrate de seguir las recomendaciones proporcionadas por el proveedor del sistema de destino.

Pasos

1. Activa la replicación para tu depósito de origen:

- Utiliza un editor de texto para crear el archivo XML de configuración de replicación necesario para habilitar la replicación, como se especifica en la API de replicación de S3.
- Al configurar el XML:
 - Ten en cuenta que StorageGRID solo admite la V1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso del elemento `Filter` para las reglas y sigue las convenciones de la V1 para la eliminación de versiones de objetos. Consulta la documentación de Amazon sobre la configuración de replicación para obtener más detalles.
 - Utiliza el URN del endpoint de un bucket de S3 como destino.
 - Opcionalmente, añade el elemento `<StorageClass>` y especifica una de las siguientes opciones:
 - `STANDARD`: la clase de almacenamiento predeterminada. Si no especificas una clase de almacenamiento al subir un objeto, se usa la clase de almacenamiento `STANDARD`.
 - `STANDARD_IA`: (estándar - acceso poco frecuente.) Usa esta clase de almacenamiento para datos a los que accedas con menos frecuencia, pero que sigan requiriendo un acceso rápido cuando los necesites.
 - `REDUCED_REDUNDANCY`: Utiliza esta clase de almacenamiento para datos no críticos y reproducibles que pueden almacenarse con menos redundancia que la clase de almacenamiento `STANDARD`.
 - Si especificas 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. Selecciona **View buckets** desde el panel, o selecciona **STORAGE (S3) > Buckets**.

3. Selecciona el nombre del depósito de origen.

Aparece la página de detalles del bucket.

4. Selecciona **Servicios de plataforma > Replicación**.
5. Marca la casilla **Habilitar replicación**.
6. Pega el XML de la configuración de replicación en el cuadro de texto y selecciona **Guardar cambios**.



Un administrador de StorageGRID debe habilitar los servicios de la plataforma para cada cuenta de inquilino mediante Grid Manager o Grid Management API. Ponte en contacto con tu administrador de StorageGRID si se produce un error al guardar el archivo de configuración XML.

7. Comprueba que la replicación esté configurada correctamente:
 - a. Añade un objeto al depósito de origen que cumpla los requisitos de replicación especificados en la configuración de replicación.

En el ejemplo mostrado anteriormente, se replican los objetos que coinciden con el prefijo "2020".

- b. Comprueba que el objeto se haya replicado en el depósito de destino.

Para los objetos pequeños, la replicación ocurre rápidamente.

Información relacionada

["Crear un endpoint de servicios de plataforma"](#)

Configura las notificaciones de eventos en StorageGRID

Habilitas las notificaciones para un bucket creando un XML de configuración de notificaciones y usando el Tenant Manager para aplicar el XML a un bucket.

Antes de empezar

- Los servicios de la plataforma fueron habilitados para tu cuenta de inquilino por un administrador de StorageGRID.
- Ya has creado un bucket que servirá como fuente de notificaciones.
- El punto final que pretendes utilizar como destino para las notificaciones de eventos ya existe y tienes su URN.
- Pertenece a un grupo de usuarios que tiene el ["Gestiona todos los buckets o permiso de acceso a raíz"](#). Estos permisos anulan la configuración de permisos de las políticas de grupo o de bucket al configurar el bucket mediante Tenant Manager.

Acerca de esta tarea

Configuras las notificaciones de eventos asociando un archivo XML de configuración de notificaciones a un bucket de origen. El archivo XML de configuración de notificaciones sigue las convenciones de S3 para configurar notificaciones de buckets, con el tema de Amazon SNS, el tema de Kafka o el endpoint del webhook de destino especificado como el URN de un endpoint.

Para obtener información general sobre las notificaciones de eventos y cómo configurarlas, consulta ["Documentación de Amazon"](#). Para obtener información sobre cómo StorageGRID implementa la API de configuración de notificaciones de buckets de S3, consulta ["Instrucciones para implementar aplicaciones cliente de S3"](#).

Ten en cuenta los siguientes requisitos y características a la hora de configurar las notificaciones de eventos para un bucket:

- Al crear y aplicar un archivo XML de configuración de notificaciones válido, este debe utilizar el URN de un endpoint de notificaciones de eventos para cada destino.
- Aunque es posible configurar las notificaciones de eventos en un bucket con S3 Object Lock activado, los metadatos de S3 Object Lock (incluidos Retain Until Date y el estado de Legal Hold) de los objetos no se incluirán en los mensajes de notificación.
- Después de que configures las notificaciones de eventos, cada vez que ocurra un evento especificado para un objeto en el bucket de origen, se genera una notificación y se envía al tema de Amazon SNS, al tema de Kafka o al endpoint de webhook que uses como destino.
- Si activas las notificaciones de eventos para un bucket que contiene objetos, solo se enviarán notificaciones sobre las acciones que se realicen después de guardar la configuración de notificaciones.

Pasos

1. Activa las notificaciones para tu depósito de origen:

- Utiliza un editor de texto para crear el archivo XML de configuración de notificaciones necesario para habilitar las notificaciones de eventos, como se especifica en la API de notificaciones de S3.
- Al configurar el XML, usa el URN de un endpoint 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 Tenant Manager, selecciona **STORAGE (S3) > Buckets**.

3. Selecciona el nombre del depósito de origen.

Aparece la página de detalles del bucket.

4. Selecciona **Platform services > Event notifications**.

5. Marca la casilla **Activar notificaciones de eventos**.

6. Pega el XML de configuración de notificaciones en el cuadro de texto y selecciona **Guardar cambios**.



Un administrador de StorageGRID debe habilitar los servicios de la plataforma para cada cuenta de inquilino mediante Grid Manager o Grid Management API. Ponte en contacto con tu administrador de StorageGRID si se produce un error al guardar el archivo de configuración XML.

7. Comprueba que las notificaciones de eventos estén configuradas correctamente:

- a. Realiza una acción sobre un objeto en el bucket de origen que cumpla 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 prefijo `images/`.

- b. Comprueba que se haya entregado una notificación al tema de Amazon SNS, al tema de Kafka o al endpoint del webhook de destino.

Por ejemplo, si el tema de destino está alojado en Amazon SNS, podrías configurar el servicio para que te 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 se recibe la notificación en el tema de destino, has configurado correctamente tu bucket de origen para las notificaciones de StorageGRID.

Información relacionada

- ["Entiende las notificaciones de los buckets"](#)
- ["Usa la API de REST de S3"](#)

- ["Crear un endpoint de servicios de plataforma"](#)

Configura el servicio de integración de búsqueda en StorageGRID

Habilitas la integración de búsqueda para un bucket creando un XML de integración de búsqueda y usando el Tenant Manager para aplicar el XML al bucket.

Antes de empezar

- Los servicios de la plataforma fueron habilitados para tu cuenta de inquilino por un administrador de StorageGRID.
- Ya has creado un bucket de S3 cuyo contenido quieres indexar.
- El punto final que pretendes utilizar como destino para el servicio de integración de búsquedas ya existe y tienes su URN.
- Pertenece a un grupo de usuarios que tiene el ["Gestiona todos los buckets o permiso de acceso a raíz"](#). Estos permisos anulan la configuración de permisos de las políticas de grupo o de bucket al configurar el bucket mediante Tenant Manager.

Acerca de esta tarea

Después de que configuras el servicio de integración de búsqueda para un bucket de origen, crear un objeto o actualizar los metadatos o las etiquetas de un objeto hace que los metadatos del objeto se envíen al endpoint de destino.

Si habilitas el servicio de integración de búsqueda para un bucket que ya contiene objetos, las notificaciones de metadatos no se envían automáticamente para los objetos existentes. Actualiza estos objetos existentes para asegurarte de que sus metadatos se agreguen al índice de búsqueda de destino.

Pasos

1. Habilita la integración de búsqueda para un bucket:

- Utiliza un editor de texto para crear el archivo XML de notificación de metadatos necesario para habilitar la integración de búsqueda.
- Al configurar el XML, utiliza el URN de un punto final de integración de búsqueda como destino.

Los objetos se pueden filtrar según el prefijo de su nombre. Por ejemplo, se pueden enviar los metadatos de los objetos con el prefijo `images` a un destino, y los metadatos de los objetos con el prefijo `videos` a otro. Las configuraciones que contengan prefijos que se solapen no son válidas y se rechazan al enviarlas. Por ejemplo, no se permite una configuración que incluya una regla para objetos con el prefijo `test` y una segunda regla para objetos con el prefijo `test2`.

Si es necesario, consulta la [Ejemplos para la configuración XML de metadatos](#).

```

<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>/Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Elementos en el archivo XML de configuración de la notificación de metadatos:

Nombre	Descripción	Requerido
MetadataNotificationConfiguration	Etiqueta de contenedor para las reglas que se utilizan para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o varios elementos «Rule».	Sí
Regla	Etiqueta de contenedor para una regla que identifica los objetos cuyos metadatos deben añadirse a un índice específico. Se rechazan las reglas cuyos prefijos se solapan. Incluido en el elemento MetadataNotificationConfiguration.	Sí
ID	Identificador único de la regla. Incluido en el elemento Rule.	No
Estado	El estado puede ser «Activado» o «Desactivado». No se realiza ninguna acción para las reglas que están desactivadas. Incluido en el elemento Rule.	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 coincidan todos los objetos, especifica un prefijo vacío. Incluido en el elemento Rule.	Sí
Destino	Etiqueta de contenedor para el destino de una regla. Incluido en el elemento Rule.	Sí

Nombre	Descripción	Requerido
Urna	URN del destino al que se envían los metadatos del objeto. Debe ser el URN de un endpoint de StorageGRID con las siguientes propiedades: • es debe ser el tercer elemento. • El URN debe terminar con el índice y el tipo en los que se almacenan los metadatos, en el formato <code>domain-name/myindex/mytype</code>. Los puntos finales se configuran mediante el Tenant Manager o la Tenant Management API. Tienen el siguiente formato: • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> El endpoint debe configurarse antes de enviar el archivo XML de configuración o la configuración fallará con un error 404. El URN se incluye en el elemento Destination.	Sí

2. En el Gestor de inquilinos, selecciona **STORAGE (S3) > Buckets**.

3. Selecciona el nombre del depósito de origen.

Aparece la página de detalles del bucket.

4. Selecciona **Platform services > Search integration**

5. Marca la casilla **Habilitar integración de búsqueda**.

6. Pega la configuración de la notificación de metadatos en el cuadro de texto y selecciona **Guardar cambios**.



Un administrador de StorageGRID debe habilitar los servicios de la plataforma para cada cuenta de inquilino mediante Grid Manager o Management API. Ponte en contacto con tu administrador de StorageGRID si se produce un error al guardar el archivo XML de configuración.

7. Comprueba que el servicio de integración de búsqueda esté configurado correctamente:

- Añade un objeto al depósito de origen que cumpla los requisitos para activar una notificación de metadatos según lo especificado en el archivo XML de configuración.

En el ejemplo mostrado anteriormente, todos los objetos añadidos al bucket activan una notificación de metadatos.

- Comprueba que se haya añadido al índice de búsqueda especificado en el endpoint un documento JSON que contenga los metadatos y las etiquetas del objeto.

Después de que termines

Si es necesario, puedes desactivar la integración de búsqueda para un bucket utilizando cualquiera de los

siguientes métodos:

- Selecciona **STORAGE (S3) > Buckets** y desmarca la casilla **Enable search integration**.
- Si utilizas la API de S3 directamente, usa una solicitud de notificación de metadatos de DELETE Bucket. Consulta las instrucciones para implementar aplicaciones cliente de S3.

Ejemplo: configuración de notificaciones 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 la notificación de metadatos con dos reglas

En este ejemplo, los metadatos de los objetos que coinciden con el prefijo `/images` se envían a un destino, mientras que los metadatos de los objetos que coinciden con el prefijo `/videos` se envían a un segundo destino.

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Formato de notificación de metadatos

Al habilitar el servicio de integración de búsqueda para un bucket, se genera un documento JSON y se envía al endpoint de destino cada vez que se añaden, actualizan o eliminan metadatos o etiquetas de un objeto.

Este ejemplo muestra un ejemplo del JSON que se podría generar cuando se crea un objeto con la clave SGWS/Tagging.txt en un bucket llamado test. El bucket test no está versionado, así que la etiqueta versionId 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 bucket, el nombre del objeto y el ID de versión, si lo hay.

Información del bucket y del objeto

`bucket`: nombre del depósito

`key`: nombre de la clave del objeto

`versionID`: versión del objeto, para objetos en depósitos con control de versiones

`region`: región del bucket, 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 de usuario para el objeto, como pares clave-valor

`key:value`

Etiquetas

`tags`: Todas las etiquetas de objeto definidas para el objeto, en forma de pares clave-valor

`key:value`

Cómo consultar los resultados en Elasticsearch

Para las etiquetas y los metadatos de usuario, StorageGRID pasa las fechas y los números a Elasticsearch como cadenas o como notificaciones de eventos de S3. Para configurar Elasticsearch para que interprete estas cadenas como fechas o números, sigue las instrucciones de Elasticsearch para la asignación dinámica de campos y para la asignación de formatos de fecha. Habilita las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Una vez indexado un documento, no puedes editar los tipos de campo del documento en el índice.

Usa la API de REST de S3

Versiones compatibles y actualizaciones de la API de REST de StorageGRID S3

StorageGRID es compatible con la API de Simple Storage Service (S3), que se implementa como un conjunto de servicios web de Representational State Transfer (REST).

La compatibilidad con la API de REST de S3 te permite conectar aplicaciones orientadas a servicios desarrolladas para los servicios web de S3 con el almacenamiento de objetos local que utiliza el sistema StorageGRID. Solo es necesario realizar cambios mínimos en el uso actual que hace la aplicación cliente de las llamadas a la API de REST de S3.

Versiones compatibles

StorageGRID es compatible con las siguientes versiones específicas de STS, S3 y HTTP:

Artículo	Versión
Especificación de la API STS AssumeRole	"Documentación de Amazon Web Services (AWS): referencia de la API de Amazon Assumerole" Para obtener más información sobre AssumeRole, consulta "Configura AssumeRole".
Especificación de la API de S3	"Documentación de AWS: referencia de la API de Amazon Simple Storage Service"
HTTP	1,1 Para obtener más información sobre HTTP, consulta HTTP/1.1 (RFCs 7230-35). "IETF RFC 2616: Protocolo de transferencia de hipertexto (HTTP/1.1)" Nota: StorageGRID no admite el pipelining de HTTP/1.1.

Actualizaciones en la compatibilidad con la API de REST de S3

Versión	Comentarios
12,0	- Se ha añadido compatibilidad con el intercambio de recursos entre orígenes (CORS) para una interfaz de gestión, lo que permite que otro dominio acceda a los datos de StorageGRID mediante las API de gestión. "Más información". - Se ha añadido compatibilidad con STS AssumeRole y la política de sesión. Consulta "un ejemplo de política de sesión". Puedes configurar AssumeRole en grupos de inquilinos.

Versión	Comentarios
11,9	• Se ha añadido compatibilidad con valores de suma de comprobación SHA-256 precalculados para las siguientes solicitudes y encabezados compatibles. Puedes utilizar esta función para verificar la integridad de los objetos subidos: ◦ CompleteMultipartUpload: x-amz-checksum-sha256 ◦ CreateMultipartUpload: x-amz-checksum-algorithm ◦ GetObject: x-amz-checksum-mode ◦ HeadObject: x-amz-checksum-mode ◦ ListParts ◦ PutObject: x-amz-checksum-sha256 ◦ UploadPart: x-amz-checksum-sha256 • Se añadió la posibilidad de que el administrador del grid controle la configuración de retención y Compliance a nivel de tenant. Estas configuraciones afectan los ajustes de S3 Object Lock. ◦ Modo de retención predeterminado del bucket y modo de retención de objetos: Governance o Compliance, si el administrador de la grid lo permite. ◦ Período de retención predeterminado del bucket y fecha de retención del objeto: debe ser menor o igual a lo que permite el período de retención máximo establecido por el administrador de grid. • Mejor compatibilidad con la codificación de contenido aws-chunked y los valores de streaming x-amz-content-sha256. Limitaciones: ◦ Si está presente, chunk-signature es opcional y no se valida ◦ Si está presente, x-amz-trailer el contenido se ignora
11,8	Actualicé los nombres de las operaciones de S3 para que coincidan con los nombres usados en "Documentación de Amazon Web Services (AWS): Referencia de la API de Amazon Simple Storage Service".
11,7	• Añadido "Referencia rápida: Solicitudes compatibles de la API de S3". • Se añadió compatibilidad para usar el modo GOVERNANCE con S3 Object Lock. • Se ha añadido compatibilidad con el encabezado de respuesta específico de StorageGRID x-ntap-sg-cgr-replication-status para las solicitudes GET Object y HEAD Object. Este encabezado proporciona el estado de replicación de un objeto para la replicación entre grids. • Las solicitudes de SelectObjectContent ahora admiten objetos Parquet.

Versión	Comentarios
11,6	• Se añadió compatibilidad para usar el parámetro de solicitud <code>partNumber</code> en las solicitudes GET Object y HEAD Object. • Se añadió compatibilidad con un modo de retención predeterminado y un periodo de retención predeterminado a nivel de bucket para S3 Object Lock. • Se ha añadido compatibilidad con la clave de condición de política <code>s3:object-lock-remaining-retention-days</code> para establecer el intervalo de períodos de retención permitidos para tus objetos. • Se ha modificado el tamaño máximo <i>recomendado</i> para una única operación PUT Object a 5 GiB (5,368,709,120 bytes). Si tienes objetos que superan los 5 GiB, usa la carga multiparte en su lugar.
11,5	• Se añadió compatibilidad para gestionar el cifrado de los buckets. • Se añadió compatibilidad con S3 Object Lock y se dejaron de usar las solicitudes de Compliance heredadas. • Se añadió compatibilidad para usar DELETE Multiple Objects en buckets con control de versiones. • Ahora se admite correctamente el encabezado de solicitud <code>Content-MD5</code>.
11,4	• Se añadió compatibilidad para DELETE Bucket tagging, GET Bucket tagging y PUT Bucket tagging. No se admiten las etiquetas de asignación de costes. • Para los buckets creados en StorageGRID 11.4, ya no es necesario restringir los nombres de las claves de los objetos para cumplir con las prácticas recomendadas de rendimiento. • Se añadió compatibilidad con las notificaciones de bucket en el tipo de evento <code>s3:ObjectRestore:Post</code>. • Ya se aplican los límites de tamaño de AWS para las partes de cargas multipartes. Cada parte en una carga multiparte debe estar entre 5 MiB y 5 GiB. La última parte puede ser menor de 5 MiB. • Se añadió compatibilidad con TLS 1.3
11,3	• Se ha añadido compatibilidad con el cifrado del lado del servidor de los datos de objetos mediante claves proporcionadas por el cliente (SSE-C). • Se añadió compatibilidad para las operaciones de ciclo de vida de bucket DELETE, GET y PUT (solo acción de expiración) y para el encabezado de respuesta <code>x-amz-expiration</code>. • Se actualizaron PUT Object, PUT Object - Copy y Multipart Upload para describir el impacto de las reglas de ILM que usan la colocación sincrónica al momento de la ingesta. • Los algoritmos de cifrado TLS 1.1 ya no son compatibles.

Versión	Comentarios
11,2	Se añadió compatibilidad con POST Object restore para usar con Cloud Storage Pools. Se añadió compatibilidad con el uso de la sintaxis de AWS para ARN, claves de condición de políticas y variables de políticas en las políticas de grupo y de bucket. Las políticas de grupo y de bucket existentes que usan la sintaxis de StorageGRID seguirán siendo compatibles. Nota: El uso de ARN/URN en otros archivos JSON/XML de configuración, incluidos los utilizados en funciones personalizadas de StorageGRID, no ha cambiado.
11,1	Se ha añadido compatibilidad con el intercambio de recursos entre orígenes (CORS), HTTP para las conexiones de clientes S3 a los nodos de la grid y la configuración de cumplimiento en los buckets.
11,0	Se ha añadido compatibilidad con la configuración de los servicios de la plataforma (CloudMirror replication, notificaciones e integración de búsqueda con Elasticsearch) para los buckets. También se ha añadido compatibilidad con las restricciones de ubicación de las etiquetas de objetos para los buckets, así como con la consistencia Available.
10,4	Se añadió compatibilidad con los cambios en el escaneo de ILM relacionados con el versionado, las actualizaciones de la página de nombres de dominio de los endpoints, las condiciones y variables en las políticas, los ejemplos de políticas y el permiso PutOverwriteObject.
10,3	Se añadió compatibilidad con el versionado.
10,2	Se añadió compatibilidad con las políticas de acceso a grupos y buckets, y con la copia multiparte (Upload Part - Copy).
10,1	Se añadió compatibilidad con la carga de archivos en varias partes, las solicitudes de tipo virtual hosted-style y la autenticación v4.
10,0	Compatibilidad inicial con la API de REST de S3 por parte del sistema StorageGRID. La versión de la <i>Simple Storage Service API Reference</i> compatible actualmente es 2006-03-01.

Solicitudes de API de S3 compatibles en StorageGRID

Esta página resume cómo StorageGRID es compatible con las API de Amazon S3.

Esta página incluye únicamente las operaciones de S3 compatibles con StorageGRID.



Para consultar la documentación de AWS sobre cada operación, selecciona el enlace que aparece en el título.

Parámetros de consulta y encabezados de solicitud habituales en las URI

Salvo que se indique lo contrario, se admiten los siguientes parámetros de consulta URI habituales:

- `versionId` (tal y como se requiere para las operaciones con objetos)

Salvo que se indique lo contrario, se admiten los siguientes encabezados de solicitud habituales:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Información relacionada

- ["Detalles de la implementación de la API de REST de S3"](#)
- ["Referencia de la API de Amazon Simple Storage Service: encabezados comunes de las solicitudes"](#)

"AbortMultipartUpload"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud, además de este parámetro de consulta de URI adicional:

- `uploadId`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones para cargas en varias partes"](#)

"CompleteMultipartUpload"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud, además de este parámetro de consulta de URI adicional:

- `uploadId`
- `x-amz-checksum-sha256`

Etiquetas XML del cuerpo de la solicitud

StorageGRID admite las siguientes etiquetas XML del cuerpo de la solicitud:

- ChecksumSHA256
- CompleteMultipartUpload
- ETag
- Part
- PartNumber

Documentación de StorageGRID

"CompleteMultipartUpload"

"CopyObject"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de estas cabeceras 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

"CopyObject"

"CreateBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de estas cabeceras adicionales:

- x-amz-bucket-object-lock-enabled

Cuerpo de la solicitud

StorageGRID es compatible con todos los parámetros del cuerpo de la solicitud definidos por la API de REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en cubos"

"CreateMultipartUpload"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de estas cabeceras 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

["CreateMultipartUpload"](#)

"DeleteBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Documentación de StorageGRID

["Operaciones en cubos"](#)

"DeleteBucketCors"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"DeleteBucketEncryption"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"DeleteBucketLifecycle"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

- ["Operaciones en cubos"](#)
- ["Crear configuración del ciclo de vida de S3"](#)

"DeleteBucketPolicy"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"DeleteBucketReplication"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"DeleteBucketTagging"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"DeleteObject"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de esta cabecera de solicitud adicional:

- `x-amz-bypass-governance-retention`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones con objetos"](#)

"DeleteObjects"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de esta cabecera de solicitud adicional:

- `x-amz-bypass-governance-retention`

Cuerpo de la solicitud

StorageGRID es compatible con todos los parámetros del cuerpo de la solicitud definidos por la API de REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones con objetos"

"DeleteObjectTagging"

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones con objetos"

"GetBucketAcl"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en cubos"

"GetBucketCors"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en cubos"

"GetBucketEncryption"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Operaciones en cubos"

"GetBucketLifecycleConfiguration"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

- ["Operaciones en cubos"](#)
- ["Crear configuración del ciclo de vida de S3"](#)

"GetBucketLocation"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"GetBucketNotificationConfiguration"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"GetBucketPolicy"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"GetBucketReplication"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"GetBucketTagging"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"GetBucketVersioning"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"GetObject"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de estos parámetros de consulta de 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

["GetObject"](#)

["GetObjectAcl"](#)**Parámetros de consulta URI y encabezados de solicitud**

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones con objetos"](#)

["GetObjectLegalHold"](#)**Parámetros de consulta URI y encabezados de solicitud**

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#)

["GetObjectLockConfiguration"](#)**Parámetros de consulta URI y encabezados de solicitud**

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#)

["GetObjectRetention"](#)**Parámetros de consulta URI y encabezados de solicitud**

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

"Utiliza la API de REST de S3 para configurar S3 Object Lock"

"GetObjectTagging"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones con objetos"](#)

"HeadBucket"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"HeadObject"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de estas cabeceras 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

["HeadObject"](#)

"ListBuckets"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

[Operaciones en el servicio](#) > [ListBuckets](#)

"ListMultipartUploads"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de los siguientes parámetros adicionales:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["ListMultipartUploads"](#)

"ListObjects"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de los siguientes parámetros adicionales:

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"ListObjectsV2"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de los siguientes parámetros adicionales:

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"ListObjectVersions"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de los siguientes parámetros adicionales:

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["Operaciones en cubos"](#)

"ListParts"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de los siguientes parámetros adicionales:

- max-parts

- part-number-marker
- uploadId

Cuerpo de la solicitud

Ninguno

Documentación de StorageGRID

["ListMultipartUploads"](#)

"PutBucketCors"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

StorageGRID es compatible con todos los parámetros del cuerpo de la solicitud definidos por la API de REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

["Operaciones en cubos"](#)

"PutBucketEncryption"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Etiquetas XML del cuerpo de la solicitud

StorageGRID admite las siguientes etiquetas XML del cuerpo de la solicitud:

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

Documentación de StorageGRID

["Operaciones en cubos"](#)

"PutBucketLifecycleConfiguration"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Etiquetas XML del cuerpo de la solicitud

StorageGRID admite las siguientes etiquetas XML del cuerpo de la solicitud:

- And
- Days
- Expiration

- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

Documentación de StorageGRID

- ["Operaciones en cubos"](#)
- ["Crear configuración del ciclo de vida de S3"](#)

"PutBucketNotificationConfiguration"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Etiquetas XML del cuerpo de la solicitud

StorageGRID admite las siguientes etiquetas XML del cuerpo de la solicitud:

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

Documentación de StorageGRID

"Operaciones en cubos"

"PutBucketPolicy"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Para obtener detalles sobre los campos del cuerpo JSON admitidos, consulta ["Usa políticas de acceso a buckets y de grupo"](#).

"PutBucketReplication"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [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 cubos"

"PutBucketTagging"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

StorageGRID es compatible con todos los parámetros del cuerpo de la solicitud definidos por la API de REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

"Operaciones en cubos"

"PutBucketVersioning"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [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 cubos"

"PutObject"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de estas cabeceras 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

"PutObject"

"PutObjectLegalHold"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

StorageGRID es compatible con todos los parámetros del cuerpo de la solicitud definidos por la API de REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#)

"PutObjectLockConfiguration"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

StorageGRID es compatible con todos los parámetros del cuerpo de la solicitud definidos por la API de REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#)

"PutObjectRetention"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos [parámetros y encabezados comunes](#) para esta solicitud, además de este encabezado adicional:

- `x-amz-bypass-governance-retention`

Cuerpo de la solicitud

StorageGRID es compatible con todos los parámetros del cuerpo de la solicitud definidos por la API de REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#)

"PutObjectTagging"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

StorageGRID es compatible con todos los parámetros del cuerpo de la solicitud definidos por la API de REST de Amazon S3 en el momento de la implementación.

Documentación de StorageGRID

["Operaciones con objetos"](#)

"RestoreObject"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Para obtener más información sobre los campos del cuerpo compatibles, consulta ["RestoreObject"](#).

"SelectObjectContent"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todas las [parámetros y encabezados comunes](#) para esta solicitud.

Cuerpo de la solicitud

Para obtener más información sobre los campos del cuerpo compatibles, consulta lo siguiente:

- ["Usa S3 Select"](#)
- ["SelectObjectContent"](#)

"UploadPart"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de estos parámetros de consulta de 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 parte

Documentación de StorageGRID

"UploadPart"

"UploadPartCopy"

Parámetros de consulta URI y encabezados de solicitud

StorageGRID admite todos los [parámetros y encabezados comunes](#) para esta solicitud, además de estos parámetros de consulta de 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

["UploadPartCopy"](#)

Prueba la configuración de la API de REST de StorageGRID S3

Puedes utilizar la interfaz de línea de comandos de Amazon Web Services (AWS CLI) para probar tu conexión con el sistema y verificar que puedes leer y escribir objetos.

Antes de empezar

- Has descargado e instalado la AWS CLI desde ["aws.amazon.com/cli"](https://aws.amazon.com/cli/).
- Opcionalmente, tienes ["creaste un endpoint de balanceador de carga"](#). De lo contrario, sabes la dirección IP del nodo de almacenamiento al que quieres conectarte y el número de puerto que debes usar. Consulta ["Direcciones IP y puertos para las conexiones de los clientes"](#).
- Tienes ["creaste una cuenta de usuario de S3"](#).
- Has iniciado sesión en el tenant y ["creaste una clave de acceso"](#).

Para obtener más información sobre estos pasos, consulta ["Configura las conexiones de los clientes"](#).

Pasos

1. Configura los ajustes de la CLI de AWS para utilizar la cuenta que creaste en el sistema StorageGRID:
 - a. Accede al modo de configuración: `aws configure`
 - b. Introduce el ID de la clave de acceso de la cuenta que creaste.
 - c. Introduce la clave de acceso secreta de la cuenta que has creado.
 - d. Introduce la región predeterminada que se va a utilizar. Por ejemplo, `us-east-1`.
 - e. Introduce el formato de salida predeterminado que deseas utilizar o pulsa **Intro** para seleccionar JSON.
2. Crea un bucket.

Este ejemplo asume que configuraste un endpoint 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 bucket se crea correctamente, se devuelve la ubicación del bucket, como se muestra en el siguiente ejemplo:

```
"Location": "/testbucket"
```

3. Sube 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 sube correctamente, se devuelve un Etag, que es un hash de los datos del objeto.

4. Enumera el contenido del bucket para comprobar que el objeto se subió.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. Elimina el objeto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Elimina el bucket.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Cómo implementa StorageGRID la API de REST de S3

Cómo la API de REST de StorageGRID S3 resuelve las solicitudes de clientes en conflicto

Las solicitudes contradictorias de los clientes, como por ejemplo que dos clientes escriban en la misma clave, se resuelven según el principio de "prevalece la más reciente".

El momento para la evaluación de "latest-wins" se basa en cuando el sistema StorageGRID completa una solicitud determinada, y no en cuando los clientes S3 inician una operación.

Cómo la API de REST de StorageGRID S3 equilibra la disponibilidad y la coherencia

La consistencia garantiza un equilibrio entre la disponibilidad de los objetos y la coherencia de dichos objetos en los distintos nodos de almacenamiento y emplazamientos. Puedes cambiar la consistencia según lo que necesite tu aplicación.

De forma predeterminada, StorageGRID garantiza la consistencia de lectura tras escritura para los objetos recién creados. Cualquier GET que siga a un PUT completado con éxito podrá leer los datos recién escritos. Las sobrescrituras de objetos existentes, las actualizaciones de metadatos y las eliminaciones son eventualmente consistentes.

Si deseas realizar operaciones con objetos con un nivel de consistencia diferente, puedes:

- Especifica una consistencia para [cada bucket](#).
- Especifica una consistencia para [cada operación de la API](#).
- Cambia la coherencia predeterminada en toda la cuadrícula realizando una de las siguientes tareas:
 - En el Grid Manager, ve a **Configuración > Sistema > Ajustes de almacenamiento > Consistencia predeterminada del bucket**.
 - .



Un cambio en la coherencia de toda la red solo se aplica a los buckets creados después de que se modificara la configuración. Para conocer los detalles de un cambio, consulta el registro de auditoría ubicado en `/var/local/log` (busca **consistencyLevel**).

Valores de consistencia

La consistencia influye en cómo se distribuyen entre los nodos los metadatos que utiliza StorageGRID para realizar el seguimiento de los objetos. La consistencia influye en la disponibilidad de los objetos para las solicitudes de los clientes.

Puedes establecer la consistencia de un bucket o de una operación de la API en uno de los siguientes valores:

- **Todos:** Todos los nodos reciben los metadatos del objeto de forma inmediata o la solicitud fallará.
- **Strong-global:** garantiza la consistencia de lectura después de escritura para todas las solicitudes de los clientes en todos los sitios. Cuando configuras la semántica de Quorum, se aplican los siguientes comportamientos:
 - Permite la tolerancia a fallos del sitio para las solicitudes de los clientes cuando los grids tienen tres o más sitios. Los grids de dos sitios no tendrán tolerancia a fallos del sitio.
 - Las siguientes operaciones de S3 no se podrán realizar si uno de los sitios está inactivo:
 - DeleteBucketEncryption
 - PutBucketBranch
 - PutBucketEncryption
 - PutBucketVersioning
 - PutObjectLegalHold
 - PutObjectLockConfiguration

- PutObjectRetention

Si lo necesitas, puedes ["Configura la semántica de quórum de StorageGRID para una consistencia global fuerte"](#).

- **Sitio fuerte:** Los metadatos de los objetos se distribuyen inmediatamente a los demás nodos del sitio. Garantiza la consistencia de lectura tras escritura para todas las solicitudes de los clientes dentro de un sitio.
- **Read-after-new-write:** proporciona coherencia de lectura tras escritura para objetos nuevos y coherencia eventual para actualizaciones de objetos. Ofrece garantías de alta disponibilidad y protección de datos. Recomendado para la mayoría de los casos.
- **Disponible:** Proporciona consistencia eventual tanto para los objetos nuevos como para las actualizaciones de objetos. Para los buckets de S3, utilízalo solo cuando sea necesario (por ejemplo, para un bucket que contenga valores de registro que rara vez se leen, o para operaciones HEAD o GET sobre claves que no existen). No es compatible con los buckets de S3 FabricPool.

Utiliza la consistencia "Read-after-new-write" y "Available"

Cuando una operación HEAD o GET utiliza la consistencia "Read-after-new-write", StorageGRID realiza la búsqueda en varios pasos, como sigue:

- En primer lugar, busca el objeto utilizando un nivel de consistencia bajo.
- Si esa búsqueda falla, repite la búsqueda con el siguiente valor de consistencia hasta alcanzar una consistencia equivalente al comportamiento de strong-global.

Si una operación HEAD o GET utiliza la consistencia "Read-after-new-write" pero el objeto no existe, la búsqueda del objeto siempre alcanzará una consistencia equivalente al comportamiento de strong-global. Porque esta consistencia requiere que haya varias copias de los metadatos del objeto disponibles en cada sitio, puedes recibir un alto número de errores 500 Internal Server si dos o más Storage Nodes en el mismo sitio no están disponibles.

A menos que necesites garantías de consistencia similares a las de Amazon S3, puedes evitar estos errores en las operaciones HEAD y GET configurando la consistencia en "Available". Cuando una operación HEAD o GET utiliza la consistencia "Available", StorageGRID solo proporciona consistencia eventual. No vuelve a intentar una operación fallida con un nivel de consistencia cada vez mayor, por lo que no requiere que haya disponibles varias copias de los metadatos del objeto.

Especifica la consistencia para la operación de la API

Para configurar la consistencia de una operación concreta de la API, los valores de consistencia deben ser compatibles con la operación y debes 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
```



Debes utilizar la misma coherencia tanto para las operaciones PutObject y GetObject.

Especifica la consistencia del bucket

Para configurar la consistencia de un bucket, puedes usar la solicitud de StorageGRID ["Consistencia de PUT Bucket"](#). O puedes ["cambiar la consistencia de un bucket"](#) desde Tenant Manager.

Al configurar la consistencia de un bucket, ten en cuenta lo siguiente:

- La configuración de la consistencia de un bucket determina qué consistencia se utiliza para las operaciones de S3 realizadas sobre los objetos en el bucket o sobre la configuración del bucket. No afecta las operaciones sobre el bucket en sí.
- La consistencia de una operación individual de la API prevalece sobre la consistencia del bucket.
- En general, los buckets deben utilizar la consistencia predeterminada, "Read-after-new-write". Si las solicitudes no funcionan correctamente, cambia el comportamiento del cliente de la aplicación si es posible. O configura el cliente para que especifique la consistencia en cada solicitud de API. Establece la consistencia a nivel de bucket solo como último recurso.

Cómo interactúan la consistencia y las reglas de ILM para afectar la protección de datos

Tanto la consistencia que elijas como la regla de ILM influyen en la forma en que se protegen los objetos. Estos ajustes pueden interactuar.

Por ejemplo, la consistencia utilizada al almacenar un objeto afecta la ubicación inicial de los metadatos del objeto, mientras que el comportamiento de ingesta seleccionado para la regla de ILM afecta la ubicación inicial de las copias del objeto. Porque 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 proporcionar una mejor protección inicial de los datos y respuestas del sistema más predecibles.

Los siguientes ["opciones de ingesta"](#) están disponibles para las reglas de ILM:

Confirmación doble

StorageGRID crea inmediatamente copias provisionales del objeto y devuelve un mensaje de éxito al cliente. Las copias especificadas en la regla ILM se realizan cuando es posible.

Estricto

Todas las copias especificadas en la regla ILM deben realizarse antes de que se devuelva un resultado satisfactorio al cliente.

Equilibrado

StorageGRID intenta crear todas las copias especificadas en la regla de ILM en el momento de la ingesta; si esto no es posible, se crean copias provisionales y se devuelve éxito al cliente. Las copias especificadas en la regla de ILM se crean cuando es posible.

Ejemplo de cómo pueden interactuar la consistencia y la regla ILM

Supongamos que tienes una red de tres sitios con la siguiente regla de ILM y la siguiente consistencia:

- **Regla de ILM:** crea tres copias de objeto, una en el sitio local y otra en cada sitio remoto. Usa el comportamiento de ingesta Strict.
- **Consistencia:** Global fuerte (los metadatos de los objetos se distribuyen inmediatamente a varios sitios).

Cuando un cliente almacena un objeto en la grid, StorageGRID crea las tres copias del objeto y distribuye los metadatos a varios sitios antes de indicar al cliente que la operación se ha realizado con éxito.

El objeto queda totalmente protegido contra la pérdida en el momento en que se recibe el mensaje de ingesta correcta. Por ejemplo, si el sitio local se pierde poco después de la ingesta, siguen existiendo copias tanto de los datos del objeto como de los metadatos del objeto en los sitios remotos. El objeto se puede recuperar íntegramente desde los demás sitios.

Si, por el contrario, usaste la misma regla de ILM y la consistencia de sitio fuerte, el cliente podría recibir un mensaje de éxito después de que los datos del objeto se replican en los sitios remotos, 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. El objeto no se puede recuperar.

La interrelación entre la coherencia y las reglas de ILM puede ser compleja. Ponte en contacto con NetApp si necesitas ayuda.

Cómo StorageGRID utiliza el versionado de objetos

Puedes configurar el estado de versionado de un bucket si quieres conservar varias versiones de cada objeto. Habilitar el versionado para un bucket puede ayudarte a protegerte contra el borrado accidental de objetos y te permite recuperar y restaurar versiones anteriores de un objeto.

El sistema StorageGRID implementa el control de versiones, que admite la mayoría de las funciones, aunque con algunas limitaciones. StorageGRID admite hasta 10 000 versiones de cada objeto.

El control de versiones de los 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 de los buckets de S3. Debes habilitar explícitamente el control de versiones para cada bucket. Cuando se habilita el control de versiones para un bucket, a cada objeto añadido al bucket se le asigna un identificador de versión, que es generado por el sistema StorageGRID.

No se admite el uso de MFA (autenticación multifactor) Delete.



La gestión de versiones solo se puede habilitar en los buckets creados con StorageGRID versión 10.3 o posterior.

ILM y versionado

Las políticas de ILM se aplican a cada versión de un objeto. Un proceso de escaneo de ILM examina continuamente todos los objetos y los reevalúa según la política de ILM vigente. Cualquier cambio que realices en las políticas de ILM se aplica a todos los objetos incorporados anteriormente. Esto incluye las versiones incorporadas anteriormente si el versionado está habilitado. El escaneo de ILM aplica los nuevos cambios de ILM a los objetos incorporados anteriormente.

En el caso de los objetos de S3 en buckets con la función de control de versiones habilitada, la compatibilidad con el control de versiones te permite crear reglas de ILM que usan «Tiempo no actual» como tiempo de referencia (selecciona **Sí** en la pregunta «¿Aplicar esta regla solo a las versiones más antiguas del objeto?» en "[Paso 1 del asistente para crear una regla de ILM](#)"). Cuando se actualiza un objeto, sus versiones anteriores pasan a ser no actuales. Usar un filtro de «Tiempo no actual» te permite crear políticas que reducen el impacto en el almacenamiento de las versiones anteriores de los objetos.



Cuando subes una nueva versión de un objeto usando una operación de carga multiparte, la hora 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 podría ser horas o días antes que la hora de la versión actual.

Información relacionada

- ["Cómo se eliminan los objetos versionados de S3"](#)
- ["Normas y políticas de ILM para objetos versionados en S3 \(Ejemplo 4\)"](#).

Usa la API de REST de S3 para configurar StorageGRID S3 Object Lock

Si la configuración global de S3 Object Lock está habilitada para tu sistema StorageGRID, puedes crear buckets con S3 Object Lock habilitado. Puedes especificar la retención predeterminada para cada bucket o los ajustes de retención para cada versión de objeto.

Cómo activar S3 Object Lock en un bucket

Si la configuración global de S3 Object Lock está activada para tu sistema StorageGRID, puedes activar S3 Object Lock opcionalmente al crear cada bucket.

S3 Object Lock es una configuración permanente que solo puedes habilitar cuando creas un bucket. No puedes añadir ni deshabilitar S3 Object Lock después de crear un bucket.

Para habilitar S3 Object Lock en un bucket, utiliza cualquiera de estos métodos:

- Crea el bucket con el Tenant Manager. Consulta ["Crear un bucket de S3"](#).
- Crea el bucket mediante una solicitud CreateBucket con la cabecera de solicitud `x-amz-bucket-object-lock-enabled`. Consulta ["Operaciones en cubos"](#).

S3 Object Lock requiere el control de versiones del bucket, que se activa automáticamente al crear el bucket. No puedes suspender el control de versiones del bucket. Consulta ["Control de versiones de objetos"](#).

Configuración predeterminada de retención para un bucket

Cuando se habilita S3 Object Lock para un bucket, puedes habilitar opcionalmente la retención predeterminada para el bucket y especificar un modo de retención predeterminado y un periodo de retención predeterminado.

Modo de retención predeterminado

- En modo COMPLIANCE:
 - El objeto no se puede eliminar hasta que se alcance su fecha de retención.
 - La fecha límite de retención del objeto se puede ampliar, pero no se puede reducir.
 - La fecha de retención del objeto no se puede eliminar hasta que se alcance dicha fecha.
- En el modo GOVERNANCE:
 - Los usuarios con el permiso `s3:BypassGovernanceRetention` pueden usar el encabezado de solicitud `x-amz-bypass-governance-retention: true` para omitir la configuración de retención.
 - Estos usuarios pueden eliminar una versión de un objeto antes de que se alcance su `retain-until-date`.

- Estos usuarios pueden aumentar, disminuir o eliminar la fecha de retención de un objeto.

Periodo de retención predeterminado

Cada bucket puede tener un periodo de retención predeterminado especificado en años o días.

Cómo configurar el periodo de retención predeterminado de un bucket

Para configurar el periodo de retención predeterminado de un bucket, utiliza cualquiera de estos métodos:

- Administra la configuración de los buckets desde el Tenant Manager. Consulta ["Crear un depósito de S3"](#) y ["Actualizar la retención predeterminada de S3 Object Lock"](#).
- Envía una solicitud PutObjectLockConfiguration para el bucket para especificar el modo predeterminado y el número predeterminado de días o años.

PutObjectLockConfiguration

La solicitud PutObjectLockConfiguration te permite establecer y modificar el modo de retención predeterminado y el periodo de retención predeterminado para un bucket que tenga activado S3 Object Lock. También puedes eliminar los ajustes de retención predeterminados configurados anteriormente.

Cuando se incorporan nuevas versiones de objetos al bucket, 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 periodo de retención predeterminado se usa para calcular la `retain-until-date` si `x-amz-object-lock-retain-until-date` no está especificado.

Si se modifica el periodo de retención predeterminado después de la incorporación de una versión de un objeto, la fecha de retención de dicha versión sigue siendo la misma y no se vuelve a calcular usando el nuevo periodo de retención predeterminado.

Debes tener el permiso `s3:PutBucketObjectLockConfiguration` o ser account root para completar esta operación.

El encabezado de solicitud `Content-MD5` debe especificarse en la solicitud PUT.

Ejemplo de solicitud

Este ejemplo habilita S3 Object Lock para un bucket y establece el modo de retención predeterminado en COMPLIANCE y el periodo 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 el periodo de retención predeterminado de un bucket

Para comprobar si S3 Object Lock está habilitado en un bucket y para ver el modo de retención predeterminado y el periodo de retención, utiliza cualquiera de estos métodos:

- Consulta el bucket en Tenant Manager. Consulta ["Ver depósitos de S3"](#).
- Envía una solicitud `GetObjectLockConfiguration`.

GetObjectLockConfiguration

La solicitud `GetObjectLockConfiguration` te permite determinar si S3 Object Lock está habilitado para un bucket y, si lo está, ver si hay un modo de retención predeterminado y un periodo de retención configurados para el bucket.

Cuando se incorporan nuevas versiones de objetos al depósito, se aplica el modo de retención predeterminado si `x-amz-object-lock-mode` no se especifica. El periodo de retención predeterminado se utiliza para calcular la fecha de retención si `x-amz-object-lock-retain-until-date` no se especifica.

Debes tener el permiso `s3:GetBucketObjectLockConfiguration` o ser root de la cuenta 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 de un objeto

Un bucket con S3 Object Lock habilitado puede contener una combinación de objetos con y sin configuraciones de retención de S3 Object Lock.

La configuración de retención a nivel de objeto se especifica mediante la API de REST de S3. La configuración de retención de un objeto prevalece sobre cualquier configuración de retención predeterminada del bucket.

Puedes especificar los siguientes ajustes para cada objeto:

- **Modo de retención:** COMPLIANCE o GOVERNANCE.
- **Fecha límite de conservación:** Fecha que especifica durante cuánto tiempo StorageGRID debe conservar la versión del objeto.

- En el modo COMPLIANCE, si la retain-until-date está en el futuro, el objeto se puede recuperar, pero no se puede modificar ni eliminar. La retain-until-date se puede aumentar, pero esta fecha no se puede reducir ni eliminar.
- En el modo GOVERNANCE, los usuarios con permisos especiales pueden omitir la configuración de retain-until-date. Pueden eliminar una versión de objeto antes de que haya transcurrido su periodo de retención. También pueden aumentar, reducir o incluso eliminar la retain-until-date.
- **Retención legal:** Al aplicar una retención legal a una versión de un objeto, dicho objeto queda bloqueado de inmediato. Por ejemplo, podrías necesitar aplicar una retención legal a un objeto relacionado con una investigación o una disputa legal. Una retención legal no tiene fecha de caducidad, pero permanece vigente hasta que se elimine de forma explícita.

La configuración de la retención legal de un objeto es independiente del modo de retención y de la fecha de retención. Si una versión de un objeto está sujeta a una retención legal, nadie puede eliminar esa versión.

Para especificar la configuración de S3 Object Lock al añadir una versión de objeto a un bucket, envía una solicitud "PutObject", "CopyObject" o "CreateMultipartUpload".

Puedes utilizar lo siguiente:

- x-amz-object-lock-mode, que puede ser «COMPLIANCE» o «GOVERNANCE» (distingue mayúsculas de minúsculas).



Si especificas x-amz-object-lock-mode, también debes especificar x-amz-object-lock-retain-until-date.

- x-amz-object-lock-retain-until-date
 - El valor de «retener 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 en milisegundos). No se permiten otros formatos ISO 8601.
 - La fecha límite de conservación debe estar en el futuro.
- x-amz-object-lock-legal-hold

Si la retención legal está activada (distingue mayúsculas de minúsculas), el objeto queda sujeto a una retención legal. Si la retención legal está desactivada, no se aplica ninguna retención legal. Cualquier otro valor da lugar a un error 400 Bad Request (InvalidArgument).

Si utilizas alguno de estos encabezados de solicitud, ten en cuenta estas restricciones:

- El encabezado de solicitud Content-MD5 es obligatorio si cualquier encabezado de solicitud x-amz-object-lock-* está presente en la solicitud PutObject. Content-MD5 no es obligatorio para CopyObject ni para CreateMultipartUpload.
- Si el bucket no tiene habilitado S3 Object Lock y un encabezado de solicitud x-amz-object-lock-* está presente, se devuelve un error 400 Bad Request (InvalidRequest).
- La solicitud PutObject admite el uso de x-amz-storage-class: REDUCED_REDUNDANCY para adaptarse al comportamiento de AWS. Sin embargo, cuando se ingiere un objeto en un bucket con S3 Object Lock habilitado, StorageGRID siempre realizará una ingesta con doble confirmación.
- Una respuesta posterior de tipo GET o de versión HeadObject incluirá los encabezados x-amz-object-lock-mode, x-amz-object-lock-retain-until-date y x-amz-object-lock-legal-hold, si

están configurados y si quien envía la solicitud tiene los permisos correctos de `s3:Get*`.

Puedes utilizar la clave de condición de política `s3:object-lock-remaining-retention-days` para limitar los períodos de retención mínimos y máximos permitidos para tus objetos.

Cómo actualizar la configuración de retención de un objeto

Si necesitas actualizar la retención legal o la configuración de retención de una versión de objeto existente, puedes realizar las siguientes operaciones sobre los subrecursos del objeto:

- `PutObjectLegalHold`

Si el nuevo valor de la retención legal está activado (ON), el objeto queda sujeto a una retención legal. Si el valor de la retención legal está desactivado (OFF), se levanta la retención legal.

- `PutObjectRetention`
 - El valor del modo puede ser COMPLIANCE o GOVERNANCE (distingue mayúsculas de minúsculas).
 - El valor de «retener 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 en milisegundos). No se permiten otros formatos ISO 8601.
 - Si una versión de un objeto ya tiene una fecha de retención, solo puedes ampliarla. El nuevo valor debe estar en el futuro.

Cómo usar el modo GOVERNANCE

Los usuarios que tengan el permiso `s3:BypassGovernanceRetention` pueden omitir la configuración de retención activa de un objeto que use el modo GOVERNANCE. Cualquier operación DELETE o `PutObjectRetention` debe incluir el encabezado de solicitud `x-amz-bypass-governance-retention:true`. Estos usuarios pueden realizar estas operaciones adicionales:

- Realiza operaciones `DeleteObject` o `DeleteObjects` para eliminar una versión de objeto antes de que transcurra su periodo de retención.

Los objetos sujetos a una retención legal no se pueden eliminar. La retención legal debe estar desactivada.

- Realiza operaciones de `PutObjectRetention` que cambien el modo de una versión de objeto de GOVERNANCE a COMPLIANCE antes de que haya transcurrido el periodo de retención del objeto.

Nunca está permitido cambiar el modo de COMPLIANCE a GOVERNANCE.

- Realiza operaciones `PutObjectRetention` para aumentar, reducir o eliminar el periodo de retención de una versión de un objeto.

Información relacionada

- ["Gestiona objetos con S3 Object Lock"](#)
- ["Utiliza S3 Object Lock para conservar los objetos"](#)
- ["Guía del usuario de Amazon Simple Storage Service: bloqueo de objetos"](#)

Conoce la configuración del ciclo de vida de S3 para StorageGRID

Puedes crear una configuración de ciclo de vida de S3 para controlar cuándo se eliminan

determinados objetos del sistema StorageGRID.

El sencillo ejemplo de esta sección ilustra cómo una configuración del ciclo de vida de S3 puede controlar cuándo se eliminan (caducan) determinados objetos de buckets específicos de S3. El ejemplo de esta sección tiene únicamente fines ilustrativos. Para obtener información detallada sobre cómo crear configuraciones del ciclo de vida de S3, consulta ["Guía del usuario de Amazon Simple Storage Service: gestión del ciclo de vida de los objetos"](#). Ten en cuenta que StorageGRID solo admite acciones de caducidad; no admite acciones de transición.

Qué es la configuración del ciclo de vida

Una configuración de ciclo de vida es un conjunto de reglas que se aplican a los objetos en buckets específicos de S3. Cada regla especifica qué objetos se ven afectados y cuándo esos objetos caducarán (en una fecha específica o después de cierto número de días).

StorageGRID admite hasta 1,000 reglas de ciclo de vida en una configuración de ciclo de vida. Cada regla puede incluir los siguientes elementos XML:

- Caducidad: elimina un objeto cuando se alcanza una fecha determinada o cuando se alcanza un número determinado de días, a partir del momento en que se incorporó el objeto.
- NoncurrentVersionExpiration: elimina un objeto cuando se alcanza un número determinado de días, a partir del momento en que el objeto dejó de estar vigente.
- Filtro (prefijo, etiqueta)
- Estado
- ID

Cada objeto sigue la configuración de retención de un ciclo de vida de bucket S3 o de una política de ILM. Cuando se configura un ciclo de vida de bucket S3, las acciones de expiración del ciclo de vida reemplazan la política de ILM para los objetos que coinciden con el filtro del ciclo de vida del bucket. Los objetos que no coinciden con el filtro del ciclo de vida del bucket usan la configuración de retención de la política de ILM. Si un objeto coincide con un filtro de ciclo de vida del bucket y no se especifican explícitamente acciones de expiración, no se usan los ajustes de retención de la política de ILM y se da a entender que las versiones del objeto se retienen para siempre. Consulta ["Ejemplo de prioridades para el ciclo de vida de un bucket de S3 y la política de ILM"](#).

Como resultado, es posible que un objeto se elimine de la grid aunque las instrucciones de ubicación de una regla de ILM sigan aplicándose al objeto. O, un objeto podría mantenerse en la grid incluso después de que hayan expirado todas las instrucciones de ubicación de ILM para ese objeto. Para más detalles, consulta ["Cómo funciona ILM a lo largo de la vida de un objeto"](#).



La configuración del ciclo de vida de los buckets se puede utilizar con buckets que tengan habilitado S3 Object Lock, pero la configuración del ciclo de vida de los buckets no es compatible con los buckets Compliant heredados.

StorageGRID admite el uso de las siguientes operaciones con buckets para gestionar las configuraciones de ciclo de vida:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Crear configuración del ciclo de vida

Como primer paso para crear una configuración de ciclo de vida, creas un archivo JSON que incluye una o más reglas. Por ejemplo, este archivo JSON incluye tres reglas, como sigue:

1. La regla 1 solo se aplica a los objetos que coincidan con el prefijo `category1/` y que tengan un valor de `key2 tag2`. El parámetro `Expiration` especifica que los objetos que coincidan con el filtro caducarán a medianoche del 22 de agosto de 2020.
2. La regla 2 solo se aplica a los objetos que coincidan con el prefijo `category2/`. El parámetro `Expiration` especifica que los objetos que coincidan con el filtro caducarán 100 días después de su incorporación.



Las reglas que especifican un número de días se refieren a la fecha en que se incorporó el objeto. Si la fecha actual supera la fecha de incorporación más el número de días, es posible que algunos objetos se eliminen del bucket tan pronto como se aplique la configuración del ciclo de vida.

3. La regla 3 se aplica únicamente a los objetos que coincidan con el prefijo `category3/`. El parámetro `Expiration` especifica que cualquier versión no actual de los objetos coincidentes expirará 50 días después de que dejen de estar actual.

```

{
  "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 bucket

Después de crear el archivo de configuración del ciclo de vida, lo aplicas a un bucket enviando una solicitud `PutBucketLifecycleConfiguration`.

Esta solicitud aplica la configuración del ciclo de vida del archivo de ejemplo a los objetos de un bucket llamado `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Para comprobar que la configuración del ciclo de vida se ha aplicado correctamente al bucket, envía una solicitud `GetBucketLifecycleConfiguration`. Por ejemplo:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

Una respuesta correcta muestra la configuración del ciclo de vida que acabas de aplicar.

Comprueba que la expiración del ciclo de vida del bucket se aplique al objeto

Puedes determinar si una regla de expiración en la configuración del ciclo de vida se aplica a un objeto específico al enviar una solicitud `PutObject`, `HeadObject` o `GetObject`. Si se aplica una regla, la respuesta incluye un parámetro `Expiration` que indica cuándo expira el objeto y qué regla de expiración se aplicó.



Porque el ciclo de vida del bucket tiene prioridad sobre el ILM, la `expiry-date` que se muestra es la fecha real en la que se eliminará el objeto. Para más detalles, consulta ["Cómo se determina la retención de objetos"](#).

Por ejemplo, esta solicitud `PutObject` se envió el 22 de junio de 2020 y almacena un objeto en el `testbucket` depósito.

```
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 (01 oct 2020) y que coincide con la Regla 2 de la configuración del ciclo de vida.

```
{
  "Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-id=\"rule2\"",
  "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Por ejemplo, se utilizó esta solicitud HeadObject para obtener metadatos para el mismo objeto en el bucket 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 buckets con control de versiones habilitado, el encabezado de respuesta `x-amz-expiration` solo se aplica a las versiones actuales de los objetos.

Recomendaciones para implementar la API de REST de S3 con StorageGRID

Debes seguir estas recomendaciones al implementar la API de REST de S3 para su uso con StorageGRID.

Recomendaciones para HEADs a objetos inexistentes

Si tu aplicación comprueba habitualmente si existe un objeto en una ruta en la que no esperas que exista realmente, debes utilizar la consistencia "Available" ["coherencia"](#). Por ejemplo, debes utilizar la consistencia "Available" si tu aplicación realiza una operación HEAD en una ubicación antes de realizar una operación PUT en ella.

De lo contrario, si la operación HEAD no encuentra el objeto, podrías recibir un gran número de errores 500 Internal Server si dos o más Storage Nodes en el mismo sitio no están disponibles o si un sitio remoto no es accesible.

Puedes configurar la consistencia «Disponible» para cada bucket mediante la solicitud ["Consistencia de PUT Bucket"](#), o puedes especificar la consistencia en el encabezado de la solicitud para una operación individual de la API.

Recomendaciones para las claves de los objetos

Sigue estas recomendaciones para los nombres de clave de los objetos, según cuándo se creó el bucket por primera vez.

Buckets creados en StorageGRID 11.4 o versiones anteriores

- No utilices valores aleatorios como los cuatro primeros caracteres de las claves de los objetos. Esto contrasta con la recomendación anterior de AWS sobre los prefijos de claves. En su lugar, utiliza prefijos no aleatorios y no únicos, como `image`.
- Si sigues la antigua recomendación de AWS de utilizar caracteres aleatorios y únicos en los prefijos de las claves, añade un nombre de directorio como prefijo a las claves de los objetos. 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 versiones posteriores

No es obligatorio restringir los nombres de las claves de los objetos para cumplir con las mejores prácticas de rendimiento. En la mayoría de los casos, puedes usar valores aleatorios para los cuatro primeros caracteres de los nombres de las claves de los objetos.



Una excepción a esto es una carga de trabajo de S3 que elimina continuamente todos los objetos tras un breve periodo de tiempo. Para minimizar el impacto en el rendimiento en este caso de uso, varía la parte inicial del nombre de la clave cada varios miles de objetos con algo como la fecha. Por ejemplo, supongamos que un cliente de S3 suele escribir 2,000 objetos por segundo y que la política de ILM o del ciclo de vida del bucket elimina todos los objetos al cabo de tres días. Para minimizar el impacto en el rendimiento, podrías nombrar las claves usando un patrón como este: `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

Recomendaciones para las «lecturas de rango»

Si la "[Opción global para comprimir objetos almacenados](#)" está habilitada, las aplicaciones cliente de S3 deben evitar realizar operaciones `GetObject` que especifiquen que se devuelva un rango de bytes. Estas operaciones de "lectura de rango" son ineficientes porque StorageGRID debe descomprimir 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 los rangos se leen de objetos comprimidos, las solicitudes de los clientes pueden agotar el tiempo de espera.



Si necesitas comprimir objetos y tu aplicación cliente debe utilizar lecturas por rango, aumenta el tiempo de espera de lectura de la aplicación.

Compatibilidad con la API de REST de Amazon S3

Operaciones compatibles de la API de REST de S3 y limitaciones en StorageGRID

El sistema StorageGRID implementa la API de Simple Storage Service (API versión 2006-03-01) con soporte para la mayoría de las operaciones y con algunas limitaciones. Necesitas entender los detalles de la implementación cuando integras aplicaciones cliente de la API de REST de S3.

El sistema StorageGRID admite tanto solicitudes de tipo virtual hosted como solicitudes de tipo path.

Manejo de fechas

La implementación de la API de REST de S3 en StorageGRID 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 puede especificarse en formato de hora media de Greenwich (GMT) o en formato de hora universal coordinada (UTC) sin desfase horario (+0000 debe especificarse). Si incluyes el encabezado `x-amz-date` en tu solicitud, este reemplaza cualquier valor especificado en el encabezado `Date` de la solicitud. Cuando usas AWS Signature Version 4, el encabezado `x-amz-date` debe estar presente en la solicitud firmada porque el encabezado de fecha no es compatible.

Encabezados de solicitud habituales

El sistema StorageGRID admite los encabezados de solicitud habituales definidos por "[Referencia de la API de Amazon Simple Storage Service: encabezados comunes de las solicitudes](#)", con una excepción.

Encabezado de la solicitud	Implementación
Autorización	Compatibilidad total con AWS Signature Version 2 Compatibilidad con AWS Signature Version 4, con las siguientes excepciones: • Cuando proporcionas el valor real de la suma de comprobación de la carga útil en <code>x-amz-content-sha256</code>, el valor se acepta sin validación, como si el valor <code>UNSIGNED-PAYLOAD</code> se hubiera proporcionado para el encabezado. Cuando proporcionas un valor de encabezado <code>x-amz-content-sha256</code> que implica <code>aws-chunked streaming</code> (por ejemplo, <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>), las firmas de los fragmentos no se verifican con respecto a los datos de los fragmentos.

Encabezados de respuesta habituales

El sistema StorageGRID admite todos los encabezados de respuesta habituales definidos en la *Simple Storage Service API Reference*, con una excepción.

Encabezado de respuesta	Implementación
<code>x-amz-id-2</code>	No se utiliza

Cómo StorageGRID S3 REST API autentica las solicitudes

El sistema StorageGRID admite tanto el acceso autenticado como el acceso anónimo a los objetos mediante la API de S3.

La API de S3 admite Signature version 2 y Signature version 4 para autenticar las solicitudes de la API de S3.

Las solicitudes autenticadas deben firmarse utilizando tu ID de clave de acceso y tu clave de acceso secreta.

El sistema StorageGRID admite dos métodos de autenticación: el encabezado HTTP `Authorization` y el

uso de parámetros de consulta.

Utiliza el encabezado de autorización HTTP

El encabezado HTTP `Authorization` se utiliza en todas las operaciones de la API de S3 excepto en las solicitudes anónimas donde lo permite la política del bucket. El encabezado `Authorization` contiene toda la información de firma necesaria para autenticar una solicitud.

Usa parámetros de consulta

Puedes utilizar parámetros de consulta para añadir información de autenticación a una URL. Esto se conoce como la prefirma de la URL, que puede usarse para conceder acceso temporal a recursos específicos. Los usuarios que tengan la URL prefirmada no necesitan conocer la clave de acceso secreta para acceder al recurso, lo que te permite proporcionar acceso restringido a terceros a un recurso.

Operaciones de servicio compatibles en StorageGRID

El sistema StorageGRID admite las siguientes operaciones en el servicio.

Operación	Implementación
ListBuckets (anteriormente denominado GET Service)	Implementado con todo el comportamiento de la API de REST de Amazon S3. Sujeto a cambios sin previo aviso.
Obtener uso del almacenamiento	La solicitud de StorageGRID " Obtener uso del almacenamiento " te indica la cantidad total de almacenamiento que utiliza una cuenta y la de cada bucket asociado a dicha cuenta. Esta es una operación en el servicio con la ruta <code>/</code> y un parámetro de consulta personalizado (<code>?x-ntap-sg-usage</code> añadido).
OPCIONES /	Las aplicaciones cliente pueden enviar <code>OPTIONS</code> / solicitudes al puerto S3 de un nodo de almacenamiento, sin proporcionar credenciales de autenticación de S3, para determinar si el nodo de almacenamiento está disponible. Puedes usar esta solicitud para supervisar o para permitir que los equilibradores de carga externos identifiquen cuándo un nodo de almacenamiento está inactivo.

Operaciones de bucket S3 y detalles de implementación en StorageGRID

El sistema StorageGRID admite un máximo de 5,000 buckets por cada cuenta de inquilino de S3.

Cada grid puede tener un máximo de 100,000 buckets.

Para poder alojar 5,000 buckets, cada Storage Node en la grid debe contar con un mínimo de 64 GB de RAM.

Las restricciones relativas a los nombres de los buckets se ajustan a las de la región estándar de EE. UU. de AWS, pero deberías restringirlos aún más para que se ajusten a las convenciones de nomenclatura de DNS y así admitir solicitudes de S3 de tipo virtual hosted-style.

Para obtener más información, consulta lo siguiente:

- ["Guía del usuario de Amazon Simple Storage Service: cuotas, restricciones y limitaciones de los buckets"](#)
- ["Configura los nombres de dominio de los endpoints S3"](#)

Las operaciones ListObjects (GET Bucket) y ListObjectVersions (GET Bucket object versions) son compatibles con StorageGRID ["valores de consistencia"](#).

Puedes comprobar si las actualizaciones del tiempo de acceso están activadas o desactivadas para cada depósito. Consulta ["Obtener el tiempo de último acceso al Bucket"](#).

La siguiente tabla describe cómo StorageGRID implementa las operaciones de los buckets de la API de REST de S3. Para realizar cualquiera de estas operaciones, es necesario facilitar las credenciales de acceso correspondientes a la cuenta.

Operación	Implementación
CreateBucket	Crea un nuevo depósito. Al crear el depósito, te conviertes en el propietario del depósito. • Los nombres de los buckets deben cumplir las siguientes reglas: ◦ Debe ser único en cada sistema StorageGRID (no solo dentro de la cuenta del inquilino). ◦ Debe ser compatible con DNS. ◦ Debe contener al menos 3 y no más de 63 caracteres. ◦ Puede consistir en 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 usar letras minúsculas, números y guiones. ◦ No debe parecer una dirección IP con formato de texto. ◦ No deberías usar puntos en las solicitudes de estilo virtual hosted. Los puntos causarán problemas con la verificación del certificado comodín del servidor. • De forma predeterminada, los buckets se crean en la región <code>us-east-1</code>; sin embargo, puedes usar el elemento <code>LocationConstraint</code> en el cuerpo de la solicitud para especificar una región diferente. Cuando uses el elemento <code>LocationConstraint</code>, debes especificar el nombre exacto de una región que haya sido definida usando Grid Manager o la Grid Management API. Contacta a tu administrador del sistema si no sabes el nombre de la región que deberías usar. Nota: Se producirá un error si tu solicitud <code>CreateBucket</code> utiliza una región que no se haya definido en StorageGRID. • Puedes incluir el encabezado de solicitud <code>x-amz-bucket-object-lock-enabled</code> para crear un bucket con S3 Object Lock habilitado. Consulta "Utiliza la API de REST de S3 para configurar S3 Object Lock". Debes activar S3 Object Lock al crear el bucket. No puedes añadir ni desactivar S3 Object Lock después de crear el bucket. S3 Object Lock requiere el control de versiones del bucket, que se activa automáticamente al crear el bucket.
DeleteBucket	Elimina el bucket.
DeleteBucketCors	Elimina la configuración de CORS del depósito.
DeleteBucketEncryption	Elimina el cifrado predeterminado del depósito. Los objetos cifrados existentes siguen estando cifrados, pero los nuevos objetos que se añadan al depósito no están cifrados.
DeleteBucketLifecycle	Elimina la configuración del ciclo de vida del depósito. Consulta "Crear configuración del ciclo de vida de S3" .

Operación	Implementación
DeleteBucketPolicy	Elimina la política asociada al bucket.
DeleteBucketReplication	Elimina la configuración de replicación asociada al bucket.
DeleteBucketTagging	Utiliza el subrecurso <code>tagging</code> para eliminar todas las etiquetas de un bucket. Precaución: Si se ha configurado una etiqueta de política ILM no predeterminada para este bucket, habrá una etiqueta de bucket <code>NTAP-SG-ILM-BUCKET-TAG</code> con un valor asignado. No envíes una solicitud <code>DeleteBucketTagging</code> si hay una etiqueta de bucket <code>NTAP-SG-ILM-BUCKET-TAG</code>. En su lugar, envía una solicitud <code>PutBucketTagging</code> con solo la etiqueta <code>NTAP-SG-ILM-BUCKET-TAG</code> y su valor asignado para eliminar todas las demás etiquetas del bucket. No modifiques ni elimines la etiqueta de bucket <code>NTAP-SG-ILM-BUCKET-TAG</code>.
GetBucketAcl	Devuelve una respuesta positiva y el ID, DisplayName y Permission del propietario del bucket, lo que indica que el propietario tiene acceso completo al bucket.
GetBucketCors	Devuelve la configuración de <code>cors</code> del bucket.
GetBucketEncryption	Devuelve la configuración de cifrado predeterminada del bucket.
GetBucketLifecycleConfiguration (anteriormente denominado GET Bucket lifecycle)	Devuelve la configuración del ciclo de vida del depósito. Consulta "Crear configuración del ciclo de vida de S3" .
GetBucketLocation	Devuelve la región que se estableció usando el elemento <code>LocationConstraint</code> en la solicitud <code>CreateBucket</code> . Si la región del bucket es <code>us-east-1</code> , se devuelve una cadena vacía para la región.
GetBucketNotificationConfiguration (anteriormente denominada GET Bucket notification)	Devuelve la configuración de notificaciones asociada al bucket.
GetBucketPolicy	Devuelve la política asociada al bucket.
GetBucketReplication	Devuelve la configuración de replicación asociada al bucket.

Operación	Implementación
GetBucketTagging	Utiliza el subrecurso <code>tagging</code> para devolver todas las etiquetas de un bucket. Precaución: Si se ha configurado una etiqueta de política ILM no predeterminada para este bucket, habrá una etiqueta de bucket <code>NTAP-SG-ILM-BUCKET-TAG</code> con un valor asignado. No modifiques ni elimines esta etiqueta.
GetBucketVersioning	Esta implementación utiliza el subrecurso <code>versioning</code> para devolver el estado de control de versiones de un bucket. • <i>blank</i>: El control de versiones nunca se ha activado (el bucket está en "Unversioned") • Activado: el control de versiones está activado • Suspendido: la gestión de versiones estaba activada anteriormente y ahora está suspendida
GetObjectLockConfiguration	Devuelve el modo de retención predeterminado del bucket y el periodo de retención predeterminado, si están configurados. Consulta "Utiliza la API de REST de S3 para configurar S3 Object Lock".
HeadBucket	Comprueba si existe un bucket y si 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 identificador único de seguimiento de la solicitud asociada.

Operación	Implementación
ListObjects y ListObjectsV2 (anteriormente llamado GET Bucket)	Devuelve algunos o todos (hasta 1,000) de los objetos en un bucket. La clase de almacenamiento de los objetos puede tener uno de estos dos valores, incluso si el objeto se ingresó con la opción de clase de almacenamiento REDUCED_REDUNDANCY: • STANDARD, lo que indica que el objeto se almacena en un grupo de almacenamiento formado por Storage Nodes. • GLACIER, lo que indica que el objeto se ha movido al bucket externo especificado por el Cloud Storage Pool. Si el bucket contiene un gran número de claves eliminadas que tienen el mismo prefijo, es posible que la respuesta incluya algunos CommonPrefixes que no contengan claves. Para las solicitudes HeadObject y ListObject, StorageGRID devuelve las marcas de tiempo LastModified con diferente precisión, mientras que AWS devuelve las marcas de tiempo con la misma precisión, como se muestra en los siguientes ejemplos: • StorageGRID HeadObject: "LastModified": "2024-09-26T16:43:24+00:00" • StorageGRID ListObject: "LastModified": "2024-09-26T16:43:24.931000+00:00" • AWS HeadObject: "LastModified": "2023-10-17T00:19:54+00:00" • AWS ListObject: "LastModified": "2023-10-17T00:19:54+00:00"
ListObjectVersions (anteriormente denominado GET Bucket Object versions)	Con acceso de lectura a un bucket, al usar esta operación con el subrecurso <code>versions</code> se muestran los metadatos de todas las versiones de los objetos en el bucket.
PutBucketCors	Establece la configuración CORS de un bucket para que este pueda atender solicitudes de origen cruzado. El intercambio de recursos entre orígenes (CORS) es un mecanismo de seguridad que permite a las aplicaciones web cliente de un dominio acceder a recursos de otro dominio. Por ejemplo, supongamos que usas un bucket de S3 llamado <code>images</code> para almacenar gráficos. Al establecer la configuración CORS para el bucket <code>images</code>, puedes permitir que las imágenes de ese bucket se muestren en el sitio web <code>http://www.example.com</code>.

Operación	Implementación
PutBucketEncryption	Establece el estado de cifrado predeterminado de un bucket 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 gestionadas por StorageGRID. Al especificar la regla de configuración del cifrado del lado del servidor, establece el parámetro <code>SSEAlgorithm</code> en <code>AES256</code> y no uses el parámetro <code>KMSMasterKeyID</code>. La configuración predeterminada de cifrado del bucket se ignora si la solicitud de carga de objetos ya especifica el cifrado (es decir, si la solicitud incluye el encabezado de solicitud <code>x-amz-server-side-encryption-*</code>).
PutBucketLifecycleConfiguration (anteriormente denominado PUT Bucket lifecycle)	Crea una nueva configuración de ciclo de vida para el bucket o reemplaza una configuración de ciclo de vida existente. StorageGRID admite hasta 1,000 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>) • <code>NoncurrentVersionExpiration</code> (<code>NewerNoncurrentVersions</code>, <code>NoncurrentDays</code>) • Filtro (prefijo, etiqueta) • Estado • ID StorageGRID no admite estas acciones: • <code>AbortIncompleteMultipartUpload</code> • Transición Consulta "Crear configuración del ciclo de vida de S3". Para entender cómo la acción de Caducidad en el ciclo de vida de un bucket interactúa con las instrucciones de ubicación de ILM, consulta "Cómo funciona ILM a lo largo de la vida de un objeto". Nota: La configuración del ciclo de vida de los buckets se puede utilizar con buckets que tengan habilitado S3 Object Lock, pero la configuración del ciclo de vida de los buckets no es compatible con los buckets Compliant heredados.

Operación	Implementación
PutBucketNotificationConfiguration (anteriormente denominada PUT Bucket notification)	Configura las notificaciones para el bucket utilizando el XML de configuración de notificaciones incluido en el cuerpo de la solicitud. Debes tener en cuenta los siguientes detalles de implementación: - StorageGRID admite como destinos los temas de Amazon Simple Notification Service (Amazon SNS), los temas de Kafka o los endpoints de webhook. No se admiten los endpoints de Simple Queue Service (SQS) ni los endpoints de AWS Lambda. - El destino de las notificaciones debe especificarse como el URN de un endpoint de StorageGRID. Los endpoints pueden crearse usando el Tenant Manager o la Tenant Management API. El endpoint debe existir para que la configuración de notificaciones se realice correctamente. Si el endpoint no existe, se devuelve un error 400 Bad Request con el código <code>InvalidArgument</code>. - No puedes 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, salvo que no incluyen algunas claves y utilizan valores específicos para otras, como se muestra en la siguiente lista: eventSource <code>sgws:s3</code> awsRegion no incluido x-amz-id-2 no incluido arn <code>urn:sgws:s3:::bucket_name</code>
PutBucketPolicy	Establece la política asociada al depósito. Véase "Usa políticas de acceso a buckets y de grupo".

Operación	Implementación
PutBucketReplication	Configura "Replicación de StorageGRID CloudMirror" para el bucket utilizando el XML de configuración de replicación proporcionado en el cuerpo de la solicitud. Para la replicación de CloudMirror, debes 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 del elemento <code>Filter</code> para las reglas y sigue las convenciones de la versión 1 para la eliminación de versiones de objetos. Para obtener más información, consulta "Guía del usuario de Amazon Simple Storage Service: configuración de la replicación". • La replicación de buckets se puede configurar en buckets con o sin control de versiones. • Puedes especificar un depósito de destino diferente en cada regla del archivo XML de configuración de la replicación. Un depósito de origen puede replicarse en más de un depósito de destino. • Los buckets de destino deben especificarse como el URN de los endpoints de StorageGRID, tal y como se indica en el Tenant Manager o en la Tenant Management API. Consulta "Configura la replicación de CloudMirror". El punto final debe existir para que la configuración de la replicación tenga éxito. Si el punto final no existe, la solicitud falla como un 400 Bad Request. El mensaje de error indica: <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</code> • No necesitas especificar un <code>Role</code> en el archivo XML de configuración. Este valor no es utilizado por StorageGRID y se ignorará si lo envías. • Si omites la clase de almacenamiento en el archivo XML de configuración, StorageGRID usa por defecto la clase de almacenamiento <code>STANDARD</code>. • Si eliminas un objeto del depósito de origen o eliminas el propio depósito de origen, el comportamiento de la replicación entre regiones es el siguiente: ◦ Si eliminas el objeto o el bucket antes de que se haya replicado, el objeto o el bucket no se replica y no recibes ninguna notificación. ◦ Si eliminas el objeto o el bucket después de que se haya replicado, StorageGRID sigue el comportamiento estándar de eliminación de Amazon S3 para V1 de la replicación entre regiones.

Operación	Implementación
PutBucketTagging	Utiliza el subrecurso <code>tagging</code> para añadir o actualizar un conjunto de etiquetas para un depósito. Al añadir etiquetas a un depósito, ten en cuenta las siguientes limitaciones: • Tanto StorageGRID como Amazon S3 admiten hasta 50 etiquetas por cada bucket. • Las etiquetas asociadas a un bucket deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener hasta 128 caracteres Unicode. • Los valores de las etiquetas pueden tener una longitud máxima de 256 caracteres Unicode. • Las claves y los valores distinguen mayúsculas de minúsculas. Precaución: Si se ha configurado una etiqueta de política ILM no predeterminada para este bucket, habrá una etiqueta de bucket <code>NTAP-SG-ILM-BUCKET-TAG</code> con un valor asignado. Asegúrate de que la etiqueta de bucket <code>NTAP-SG-ILM-BUCKET-TAG</code> se incluya con el valor asignado en todas las solicitudes <code>PutBucketTagging</code>. No modifiques ni elimines esta etiqueta. Nota: Esta operación sobrescribirá cualquier etiqueta que ya tenga el bucket. Si se omite alguna etiqueta existente del conjunto, dicha etiqueta se eliminará del bucket.
PutBucketVersioning	Utiliza el subrecurso <code>versioning</code> para configurar el estado de control de versiones de un bucket existente. Puedes configurar el estado de control de versiones con uno de los siguientes valores: • Activado: Activa el control de versiones para los objetos del depósito. Todos los objetos añadidos al depósito reciben un identificador de versión único. • Suspendido: desactiva el control de versiones para los objetos del depósito. Todos los objetos añadidos al depósito reciben el ID de versión <code>null</code>.
PutObjectLockConfiguration	Configura o elimina el modo de retención predeterminado y el periodo de retención predeterminado del bucket. Si se modifica el periodo de retención predeterminado, la fecha de retención de las versiones existentes de los objetos sigue siendo la misma y no se vuelve a calcular utilizando el nuevo periodo de retención predeterminado. Consulta "Utiliza la API de REST de S3 para configurar S3 Object Lock" para obtener información detallada.

Operaciones con objetos

Cómo StorageGRID implementa las operaciones de API de REST de S3 para objetos

Esta sección describe cómo el sistema StorageGRID implementa las operaciones de la API de REST de S3 para los objetos.

Las siguientes condiciones se aplican a todas las operaciones con objetos:

- StorageGRID "valores de consistencia" es compatible con todas las operaciones en objetos, con la excepción de las siguientes:
 - `GetObjectAcl`
 - `OPTIONS /`
 - `PutObjectLegalHold`
 - `PutObjectRetention`
 - `SelectObjectContent`
- Las solicitudes conflictivas de los clientes, como por ejemplo cuando dos clientes escriben en la misma clave, se resuelven según el principio de "la última gana". El momento en que se evalúa el principio de "la última gana" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes S3 inician una operación.
- Todos los objetos de un depósito de StorageGRID son propiedad del titular del depósito, incluidos los objetos creados por un usuario anónimo o por otra cuenta.

La siguiente tabla describe cómo StorageGRID implementa las operaciones de objetos de la API de REST de S3.

Operación	Implementación
DeleteObject	Al procesar una solicitud de DeleteObject, StorageGRID intenta eliminar inmediatamente todas las copias del objeto de todas las ubicaciones donde está almacenado. Si tiene éxito, StorageGRID devuelve una respuesta al cliente de inmediato. 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 al cliente que tuvo éxito. Restricciones • La autenticación multifactor (MFA) y el encabezado de respuesta <code>x-amz-mfa</code> no son compatibles. • Las <code>If-None</code> y <code>If-None-Match</code> cabeceras son aceptadas pero no funcionan. Control de versiones Para eliminar una versión concreta, el solicitante debe ser el propietario del bucket y usar el subrecurso <code>versionId</code>. Usar este subrecurso elimina la versión de forma permanente. Si el <code>versionId</code> corresponde a un marcador de eliminación, el encabezado de respuesta <code>x-amz-delete-marker</code> se devuelve configurado en <code>true</code>. • Si se elimina un objeto sin el <code>versionId</code> subrecurso en un bucket con el versionado activado, se genera un marcador de eliminación. El <code>versionId</code> del marcador de eliminación se devuelve usando el encabezado de respuesta <code>x-amz-version-id</code>, y el encabezado de respuesta <code>x-amz-delete-marker</code> se devuelve configurado en <code>true</code>. • Si se elimina un objeto sin el <code>versionId</code> subrecurso en un bucket con el versionado suspendido, se elimina permanentemente una versión 'null' ya existente o un marcador de eliminación 'null', y se genera un nuevo marcador de eliminación 'null'. El encabezado de respuesta <code>x-amz-delete-marker</code> se devuelve configurado en <code>true</code>. Nota: En algunos casos, puede haber varios marcadores de eliminación para un objeto. Consulta "Utiliza la API de REST de S3 para configurar S3 Object Lock" para saber cómo eliminar versiones de objetos en el modo GOVERNANCE.

Operación	Implementación
DeleteObjects (anteriormente denominada DELETE Multiple Objects)	La autenticación multifactor (MFA) y el encabezado de respuesta <code>x-amz-mfa</code> no son compatibles. Se pueden eliminar varios objetos en un mismo mensaje de solicitud. Consulta "Utiliza la API de REST de S3 para configurar S3 Object Lock" para saber cómo eliminar versiones de objetos en el modo GOVERNANCE.
DeleteObjectTagging	Utiliza el subrecurso <code>tagging</code> para eliminar todas las etiquetas de un objeto. Control de versiones Si el parámetro de consulta <code>versionId</code> no se especifica en la solicitud, la operación elimina todas las etiquetas de la versión más reciente del objeto en un bucket con versiones. Si la versión actual del objeto es un marcador de eliminación, se devuelve un estado "MethodNotAllowed" con el encabezado de respuesta <code>x-amz-delete-marker</code> configurado en <code>true</code>.
GetObject	"GetObject"
GetObjectAcl	Si se facilitan las credenciales de acceso necesarias para la cuenta, la operación devuelve una respuesta positiva y el ID, DisplayName y Permission del propietario del objeto, lo que indica que el propietario tiene acceso completo al objeto.
GetObjectLegalHold	"Utiliza la API de REST de S3 para configurar S3 Object Lock"
GetObjectRetention	"Utiliza la API de REST de S3 para configurar S3 Object Lock"
GetObjectTagging	Utiliza el subrecurso <code>tagging</code> para devolver todas las etiquetas de un objeto. Control de versiones Si el parámetro de consulta <code>versionId</code> no se especifica en la solicitud, la operación devuelve todas las etiquetas de la versión más reciente del objeto en un bucket con versiones. Si la versión actual del objeto es un marcador de eliminación, se devuelve un estado "MethodNotAllowed" con el encabezado de respuesta <code>x-amz-delete-marker</code> establecido en <code>true</code>.
HeadObject	"HeadObject"
RestoreObject	"RestoreObject"
PutObject	"PutObject"

Operación	Implementación
CopyObject (anteriormente denominado PUT Object - Copy)	"CopyObject"
PutObjectLegalHold	"Utiliza la API de REST de S3 para configurar S3 Object Lock"
PutObjectRetention	"Utiliza la API de REST de S3 para configurar S3 Object Lock"

Operación	Implementación
PutObjectTagging	Utiliza el subrecurso <code>tagging</code> para añadir un conjunto de etiquetas a un objeto ya existente. Límites de las etiquetas de objetos Puedes añadir etiquetas a los objetos nuevos al subirlos, o puedes añadirlas a objetos ya existentes. Tanto StorageGRID como Amazon S3 admiten hasta 10 etiquetas por cada objeto. Las etiquetas asociadas a un objeto deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener hasta 128 caracteres Unicode y los valores de las etiquetas pueden tener hasta 256 caracteres Unicode. Las claves y los valores distinguen mayúsculas de minúsculas. Actualizaciones de etiquetas y comportamiento de ingestión Cuando usas PutObjectTagging para actualizar las etiquetas de un objeto, StorageGRID no vuelve a ingerir el objeto. Esto significa que la opción para Ingest Behavior especificada en la regla ILM correspondiente no se usa. Cualquier cambio en la ubicación del objeto que se active por la actualización se realiza cuando el ILM es reevaluado por los procesos normales de ILM en segundo plano. Esto significa que, si la regla de ILM utiliza la opción Strict para el comportamiento de ingesta, no se lleva a cabo ninguna acción si no es posible realizar las ubicaciones de objetos requeridas (por ejemplo, porque una ubicación recién requerida no está disponible). El objeto actualizado conserva su ubicación actual hasta que sea posible la ubicación requerida. Resolución de conflictos Las solicitudes conflictivas de los clientes, como por ejemplo cuando dos clientes escriben en la misma clave, se resuelven según el principio de "la última gana". El momento en que se evalúa el principio de "la última gana" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes S3 inician una operación. Control de versiones Si el parámetro de consulta <code>versionId</code> no se especifica en la solicitud, la operación añade etiquetas a la versión más reciente del objeto en un bucket con versiones. Si la versión actual del objeto es un marcador de eliminación, se devuelve un estado "MethodNotAllowed" con el encabezado de respuesta <code>x-amz-delete-marker</code> configurado en <code>true</code>.
SelectObjectContent	"SelectObjectContent"

Operaciones compatibles de Amazon S3 Select en StorageGRID

StorageGRID admite las siguientes cláusulas de Amazon S3 Select, tipos de datos y operadores para el ["SelectObjectContent comando"](#).



Los artículos que no figuren en la lista no son compatibles.

Para consultar la sintaxis, visita ["SelectObjectContent"](#). Para obtener más información sobre S3 Select, consulta ["Documentación de AWS sobre S3 Select"](#).

Solo las cuentas de inquilino que tengan habilitada la función S3 Select pueden realizar consultas SelectObjectContent. Consulta ["Consideraciones y requisitos para usar S3 Select"](#).

Cláusulas

- Lista SELECT
- Cláusula FROM
- Cláusula WHERE
- Cláusula LIMIT

Tipos de datos

- bool
- entero
- cadena
- flotante
- decimal, numérico
- marca de tiempo

Operadores

Operadores lógicos

- Y
- NO
- O

Operadores de comparación

- <
- >
- ≤
- ≥
- =
- =
- <>
- !=
- ENTRE
- EN

Operadores de coincidencia de patrones

- ME GUSTA
- _
- %

Operadores unitarios

- ES NULO
- NO ES NULO

Operadores matemáticos

- +
- -
- *
- /
- %

StorageGRID sigue la precedencia de operadores de Amazon S3 Select.

Funciones de agregación

- AVG()
- COUNT(*)
- MAX()
- MIN()
- SUM()

Funciones condicionales

- CASO
- COALESCE
- NULLIF

Funciones de conversión

- CONVERSIÓN (para el tipo de datos admitido)

Funciones de fecha

- DATE_ADD
- DATE_DIFF
- EXTRACTO
- TO_STRING
- TO_TIMESTAMP

- UTCNOW

Funciones de cadenas

- CHAR_LENGTH, CHARACTER_LENGTH
- INFERIOR
- SUBSTRING
- TRIM
- PARTE SUPERIOR

Cómo StorageGRID utiliza el cifrado del lado del servidor

El cifrado en el servidor te permite proteger tus datos de objetos en reposo. StorageGRID cifra los datos a medida que escribe el objeto y los descifra cuando accedes al objeto.

Si deseas utilizar el cifrado del lado del servidor, puedes elegir una de las dos opciones siguientes, que son mutuamente excluyentes, en función de cómo se gestionan las claves de cifrado:

- **SSE (cifrado del lado del servidor con claves gestionadas por StorageGRID):** Cuando envías una solicitud S3 para almacenar un objeto, StorageGRID cifra el objeto con una clave única. Cuando envías una solicitud S3 para recuperar el objeto, StorageGRID usa la clave almacenada para descifrar el objeto.
- **SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente):** al realizar una solicitud de S3 para almacenar un objeto, proporcionas tu propia clave de cifrado. Al recuperar un objeto, proporcionas la misma clave de cifrado como parte de tu solicitud. Si las dos claves de cifrado coinciden, el objeto se descifra y se devuelven los datos de tu objeto.

Aunque StorageGRID gestiona todas las operaciones de cifrado y descifrado de objetos, tú debes gestionar las claves de cifrado que proporcionas.



Las claves de cifrado que facilites nunca se almacenan. Si pierdes una clave de cifrado, pierdes el objeto correspondiente.



Si un objeto está cifrado con SSE o SSE-C, se ignoran todas las configuraciones de cifrado a nivel de depósito o de grid.

Utiliza SSE

Para cifrar un objeto con una clave única gestionada por StorageGRID, usa el siguiente encabezado de solicitud:

```
x-amz-server-side-encryption
```

El encabezado de solicitud SSE es compatible con las siguientes operaciones sobre objetos:

- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"

Utiliza SSE-C

Para cifrar un objeto con una clave única que gestionas tú mismo, debes utilizar tres encabezados de solicitud:

Encabezado de la solicitud	Descripción
x-amz-server-side-encryption-customer-algorithm	Especifica el algoritmo de cifrado. El valor de la cabecera debe ser AES256.
x-amz-server-side-encryption-customer-key	Especifica la clave de cifrado que se utilizará para cifrar o descifrar el objeto. El valor de la clave debe ser de 256 bits, codificado en base64.
x-amz-server-side-encryption-customer-key-MD5	Especifica 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 ser de 128 bits codificado en base64.

Las operaciones de objeto siguientes admiten los encabezados de solicitud SSE-C:

- "GetObject"
- "HeadObject"
- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

Consideraciones para usar el cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C)

Antes de utilizar SSE-C, ten en cuenta las siguientes consideraciones:

- Debes utilizar https.



StorageGRID rechaza cualquier solicitud realizada a través de http cuando se utiliza SSE-C. Por motivos de seguridad, debes considerar que cualquier clave que envíes accidentalmente mediante http está comprometida. Descarta la clave y róta la según corresponda.

- El ETag de la respuesta no es el MD5 de los datos del objeto.
- Debes gestionar la asociación de las claves de cifrado con los objetos. StorageGRID no almacena las claves de cifrado. Eres responsable de realizar el seguimiento de la clave de cifrado que proporciones para cada objeto.
- Si tu bucket tiene habilitado el control de versiones, cada versión de objeto debería tener su propia clave de cifrado. Eres responsable de realizar el seguimiento de la clave de cifrado utilizada para cada versión de objeto.

- Dado que gestionas las claves de cifrado en el lado del cliente, también debes gestionar cualquier medida de seguridad adicional, como la rotación de claves, en el lado del cliente.



Las claves de cifrado que facilites nunca se almacenan. Si pierdes una clave de cifrado, pierdes el objeto correspondiente.

- Si se ha configurado la replicación entre grids o la replicación de CloudMirror para el bucket, no puedes ingestar 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 \(SSE-C\)"](#)

Crea una copia de un objeto en StorageGRID con la solicitud S3 CopyObject

Puedes usar la solicitud CopyObject de S3 para crear una copia de un objeto que ya está almacenado en S3. Una operación CopyObject es lo mismo que realizar GetObject seguido de PutObject.

Resolver conflictos

Las solicitudes conflictivas de los clientes, como por ejemplo cuando dos clientes escriben en la misma clave, se resuelven según el principio de "la última gana". El momento en que se evalúa el principio de "la última gana" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes S3 inician una operación.

Tamaño del objeto

El tamaño máximo *recomendado* para una sola operación de PutObject es de 5 GiB (5,368,709,120 bytes). Si tienes objetos que superan los 5 GiB, utiliza ["carga en varias partes"](#) en su lugar.

El tamaño máximo *admitido* para una sola operación de PutObject es de 5 TiB (5,497,558,138,880 bytes).



Si has actualizado desde StorageGRID 11.6 o una versión anterior, se activará la alerta «S3 PUT Object size too large» si intentas cargar un objeto que supere los 5 GiB. Si tienes 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 de AWS S3, las futuras versiones de StorageGRID no admitirán cargas de objetos mayores a 5 GiB.

Caracteres UTF-8 en los metadatos de usuario

Si una solicitud incluye valores UTF-8 (sin caracteres de escape) en el nombre de la clave o en el valor de los metadatos definidos por el usuario, el comportamiento de StorageGRID es indefinido.

StorageGRID no analiza ni interpreta los caracteres UTF-8 escapados incluidos en el nombre o el valor de los metadatos definidos por el usuario. Los caracteres UTF-8 escapados se tratan como caracteres ASCII:

- Las solicitudes se procesan correctamente si los metadatos definidos por el usuario incluyen caracteres UTF-8 escapados.
- StorageGRID no devuelve la cabecera `x-amz-missing-meta` si el valor interpretado del nombre o del valor de la clave incluye caracteres no imprimibles.

Encabezados de solicitud compatibles

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, lo que te 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 por defecto es COPY, lo que te permite copiar el objeto y todas las etiquetas.

Puedes especificar REPLACE para sobrescribir las etiquetas existentes al copiar el objeto o para actualizarlas.

- Encabezados de solicitud de S3 Object Lock:

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

Si realizas una solicitud sin estas cabeceras, se utilizará la configuración de retención predeterminada del bucket para calcular el modo de versión del objeto y la fecha de retención hasta. Consulta ["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#).

- 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 compatibles

No se admiten los siguientes encabezados de solicitud:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- If-Match

El If-Match header es aceptado pero no funciona.

- If-None-Match

El If-None-Match header es aceptado pero no funciona.

- x-amz-checksum-algorithm

Al copiar 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 intentas usar `x-amz-checksum-algorithm` en la solicitud del objeto.

- x-amz-website-redirect-location

Opciones de clase de almacenamiento

Se admite el encabezado de solicitud `x-amz-storage-class` y afecta cuántas copias de objetos crea StorageGRID si la regla de ILM correspondiente utiliza Dual commit o Balanced "[opción de ingesta](#)".

- STANDARD

(Por defecto) Especifica una operación de ingesta con doble confirmación cuando la regla de ILM utiliza la opción de doble confirmación 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 utiliza la opción de confirmación doble o cuando la opción equilibrada recurre a la creación de copias provisionales.



Si estás ingiriendo un objeto en un bucket con S3 Object Lock activado, la opción `REDUCED_REDUNDANCY` se ignora. Si estás ingiriendo un objeto en un bucket Compliant heredado, la opción `REDUCED_REDUNDANCY` devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Uso de x-amz-copy-source en CopyObject

Si el bucket y la clave de origen, especificados en la cabecera `x-amz-copy-source`, son diferentes del bucket y la clave de destino, se escribe una copia de los datos del objeto de origen en el destino.

Si la fuente y el destino coinciden, y el encabezado `x-amz-metadata-directive` 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 incorporar el objeto. Esto tiene dos consecuencias importantes:

- No puedes usar `CopyObject` para cifrar un objeto existente en su lugar ni para cambiar el cifrado de un objeto existente en su lugar. Si proporcionas el encabezado `x-amz-server-side-encryption` o el encabezado `x-amz-server-side-encryption-customer-algorithm`, StorageGRID rechaza la solicitud y devuelve `XNotImplemented`.
- No se utiliza la opción de Ingest Behavior especificada en la regla ILM correspondiente. Cualquier cambio en la ubicación de los objetos que se derive de la actualización se realiza cuando ILM se vuelve a evaluar mediante los procesos normales de ILM en segundo plano.

Esto significa que, si la regla de ILM utiliza la opción `Strict` para el comportamiento de ingesta, no se lleva a cabo ninguna acción si no es posible realizar las ubicaciones de objetos requeridas (por ejemplo, porque una ubicación recién 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 utilizas ["usar el cifrado del lado del servidor"](#), los encabezados de solicitud que proporcionas dependen de si el objeto de origen está cifrado y de si planeas cifrar el objeto de destino.

- Si el objeto de origen está cifrado con una clave proporcionada por el cliente (SSE-C), debes 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`: indica AES256.
 - `x-amz-copy-source-server-side-encryption-customer-key`: especifica la clave de cifrado que proporcionaste cuando creaste el objeto de origen.
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Indica el resumen MD5 que proporcionaste cuando creaste el objeto de origen.
- Si deseas cifrar el objeto de destino (la copia) con una clave única que tú mismo proporcionas y gestionas, incluye los siguientes tres encabezados:
 - `x-amz-server-side-encryption-customer-algorithm`: Indica AES256.
 - `x-amz-server-side-encryption-customer-key`: Especifica una nueva clave de cifrado para el objeto de destino.
 - `x-amz-server-side-encryption-customer-key-MD5`: Indica el resumen MD5 de la nueva clave de cifrado.



Las claves de cifrado que facilites nunca se almacenan. Si pierdes una clave de cifrado, pierdes el objeto correspondiente. Antes de usar claves proporcionadas por el cliente para proteger los datos de los objetos, revisa las consideraciones para ["utilizando el cifrado del lado del servidor"](#).

- Si deseas cifrar el objeto de destino (la copia) con una clave única gestionada por StorageGRID (SSE), incluye este encabezado en la solicitud `CopyObject`:
 - `x-amz-server-side-encryption`



El `server-side-encryption` valor del objeto no se puede actualizar. En su lugar, haz una copia con un nuevo `server-side-encryption` valor utilizando `x-amz-metadata-directive: REPLACE`.

Control de versiones

Si el bucket de origen está versionado, puedes usar el encabezado `x-amz-copy-source` para copiar la última versión de un objeto. Para copiar una versión específica de un objeto, debes especificar explícitamente la versión que quieres copiar usando el subrecurso `versionId`. Si el bucket de destino está versionado, la versión generada se devuelve en el encabezado de respuesta `x-amz-version-id`. Si el versionado está suspendido para el bucket de destino, entonces `x-amz-version-id` devuelve un valor "null".

Recupera un objeto de un bucket en StorageGRID con la solicitud `GetObject`

Puedes usar la solicitud S3 `GetObject` para recuperar un objeto de un bucket S3.

`GetObject` y objetos multiparte

Puedes usar el parámetro de solicitud `partNumber` para recuperar una parte específica de un objeto multiparte o segmentado. El elemento de respuesta `x-amz-mp-parts-count` indica cuántas partes tiene el objeto.

Puedes establecer `partNumber` en 1 tanto para objetos segmentados/multipartes como para objetos no segmentados/no multipartes; sin embargo, el elemento de respuesta `x-amz-mp-parts-count` solo se devuelve para objetos segmentados o multipartes.

Caracteres UTF-8 en los metadatos de usuario

StorageGRID no analiza ni interpreta los caracteres UTF-8 escapados en los metadatos definidos por el usuario. Las solicitudes GET para un objeto con caracteres UTF-8 escapados en los metadatos definidos por el usuario no devuelven el `x-amz-missing-meta` encabezado si el nombre o el 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` header no es compatible con `x-amz-checksum-mode` para `GetObject`. 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 admitido

El siguiente encabezado de solicitud no es compatible y devuelve `XNotImplemented`:

- `x-amz-website-redirect-location`

Control de versiones

Si no se especifica un `versionId` subrecurso, la operación recupera la versión más reciente del objeto en un bucket versionado. Si la versión actual del objeto es un marcador de eliminación, se devuelve el estado "Not Found" con el encabezado de respuesta `x-amz-delete-marker` configurado en `true`.

Encabezados de solicitud para el cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)

Utiliza los tres encabezados si el objeto está cifrado con una clave única que hayas proporcionado.

- `x-amz-server-side-encryption-customer-algorithm`: Indica AES256.
- `x-amz-server-side-encryption-customer-key`: Indica tu clave de cifrado para el objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: indica el resumen MD5 de la clave de cifrado del objeto.



Las claves de cifrado que facilites nunca se almacenan. Si pierdes una clave de cifrado, pierdes el objeto correspondiente. Antes de usar claves proporcionadas por el cliente para proteger los datos de los objetos, revisa las consideraciones en ["Utiliza el cifrado del lado del servidor"](#).

Comportamiento de GetObject para objetos del Cloud Storage Pool

Si un objeto se ha almacenado en un ["Grupo de almacenamiento en la nube"](#), el comportamiento de una solicitud `GetObject` depende del estado del objeto. Consulta ["HeadObject"](#) para más detalles.



Si un objeto se almacena en un Cloud Storage Pool y también existen una o más copias de dicho objeto en el grid, las solicitudes de `GetObject` intentarán recuperar los datos del grid antes de recuperarlos del Cloud Storage Pool.

Estado del objeto	Comportamiento de GetObject
Objeto incorporado a StorageGRID pero aún no evaluado por ILM, u objeto almacenado en un grupo de almacenamiento tradicional o usando erasure coding	200 OK Se recupera una copia del objeto.
Objeto en el Cloud Storage Pool pero aún no ha pasado a un estado no recuperable	200 OK Se recupera una copia del objeto.
El objeto pasó a un estado no recuperable	403 Forbidden, InvalidObjectState Utiliza una solicitud "RestoreObject" para restaurar el objeto a un estado en el que se pueda recuperar.
Objeto en proceso de restauración desde un estado no recuperable	403 Forbidden, InvalidObjectState Espera a que finalice la solicitud de <code>RestoreObject</code> .

Estado del objeto	Comportamiento de GetObject
Objeto restaurado por completo en el Cloud Storage Pool	200 OK Se recupera una copia del objeto.

Objetos multiparte o segmentados en un Cloud Storage Pool

Si has subido un objeto multiparte o si StorageGRID ha dividido un objeto de gran tamaño en segmentos, StorageGRID determina si el objeto está disponible en el Cloud Storage Pool mediante un muestreo de un subconjunto de las partes o segmentos del objeto. En algunos casos, una solicitud de GetObject puede devolver erróneamente 200 OK cuando algunas partes del objeto ya han pasado a un estado en el que no se pueden recuperar o cuando algunas partes del objeto aún no se han restaurado.

En estos casos:

- La solicitud GetObject podría devolver algunos datos, pero detenerse a mitad de la transferencia.
- Una solicitud posterior a GetObject podría devolver 403 Forbidden.

GetObject y la replicación entre grids

Si usas "federación de grid" y "replicación entre grids" está habilitado para un bucket, el cliente S3 puede verificar el estado de replicación de un objeto haciendo una solicitud GetObject. La respuesta incluye el encabezado de respuesta específico de StorageGRID `x-ntap-sg-cgr-replication-status`, que tendrá uno de los siguientes valores:

Grid	Estado de la replicación
Fuente	• FINALIZADO: La replicación se realizó con éxito. • PENDIENTE: El objeto aún no se ha replicado. • ERROR: La replicación falló debido a un error permanente. Un usuario debe solucionar el error.
Destino	RÉPLICA: El objeto fue replicado desde la cuadrícula de origen.



StorageGRID no admite el encabezado `x-amz-replication-status`.

Recupera metadatos de un objeto en StorageGRID con la solicitud S3 HeadObject

Puedes usar la solicitud S3 HeadObject para recuperar metadatos de un objeto sin devolver el propio objeto. Si el objeto está almacenado en un Cloud Storage Pool, puedes usar HeadObject para determinar el estado de transición del objeto.

HeadObject y objetos multiparte

Puedes usar el parámetro de solicitud `partNumber` para recuperar los metadatos de una parte específica de un objeto multiparte o segmentado. El elemento de respuesta `x-amz-mp-parts-count` indica cuántas partes tiene el objeto.

Puedes establecer `partNumber` en 1 tanto para objetos segmentados/multipartes como para objetos no segmentados/no multipartes; sin embargo, el elemento de respuesta `x-amz-mp-parts-count` solo se devuelve para objetos segmentados o multipartes.

Caracteres UTF-8 en los metadatos de usuario

StorageGRID no analiza ni interpreta los caracteres UTF-8 escapados en los metadatos definidos por el usuario. Las solicitudes HEAD para un objeto con caracteres UTF-8 escapados en los metadatos definidos por el usuario no devuelven el encabezado `x-amz-missing-meta` si el nombre o el valor de la clave incluye caracteres no imprimibles.

Encabezado de solicitud compatible

Se admite el siguiente encabezado de solicitud:

- `x-amz-checksum-mode`

El parámetro `partNumber` y el encabezado `Range` no son compatibles con `x-amz-checksum-mode` para `HeadObject`. Cuando los incluyes en la solicitud con `x-amz-checksum-mode` activado, StorageGRID no devuelve un valor de suma de comprobación en la respuesta.

Encabezado de solicitud no admitido

El siguiente encabezado de solicitud no es compatible y devuelve `XNotImplemented`:

- `x-amz-website-redirect-location`

Control de versiones

Si no se especifica un `versionId` subrecurso, la operación recupera la versión más reciente del objeto en un bucket versionado. Si la versión actual del objeto es un marcador de eliminación, se devuelve el estado "Not Found" con el encabezado de respuesta `x-amz-delete-marker` configurado en `true`.

Encabezados de solicitud para el cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (SSE-C)

Utiliza los tres encabezados si el objeto está cifrado con una clave única que tú proporcionaste.

- `x-amz-server-side-encryption-customer-algorithm`: Indica AES256.
- `x-amz-server-side-encryption-customer-key`: Indica tu clave de cifrado para el objeto.
- `x-amz-server-side-encryption-customer-key-MD5`: indica el resumen MD5 de la clave de cifrado del objeto.



Las claves de cifrado que facilites nunca se almacenan. Si pierdes una clave de cifrado, pierdes el objeto correspondiente. Antes de usar claves proporcionadas por el cliente para proteger los datos de los objetos, revisa las consideraciones en ["Utiliza el cifrado del lado del servidor"](#).

HeadObject respuestas 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 proporcionan información sobre el estado de un objeto a medida que se traslada a un Cloud Storage Pool, se pasa opcionalmente a un estado no recuperable y se restaura.

Estado del objeto	Respuesta a HeadObject
Objeto incorporado a StorageGRID pero aún no evaluado por ILM, u objeto almacenado en un grupo de almacenamiento tradicional o usando erasure coding	200 OK (No se devuelve ningún encabezado de respuesta especial.)
Objeto en el Cloud Storage Pool pero 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> se establece en un momento lejano en el futuro. El momento exacto de la transición no lo controla el sistema StorageGRID.
El objeto ha pasado a un estado en el que no se puede recuperar, pero también existe al menos una copia en el grid	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> se ha establecido para algún momento lejano en el futuro. Nota: Si la copia en la grid no está disponible (por ejemplo, un Storage Node está inactivo), debes enviar una solicitud "RestoreObject" para restaurar la copia desde el Cloud Storage Pool antes de poder recuperar correctamente el objeto.
El objeto pasó a un estado no recuperable y no existe ninguna copia en el grid	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 restaurado por completo en el Cloud Storage Pool	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 2018 00:00:00 GMT" El expiry-date indica cuándo el objeto del Cloud Storage Pool pasará a un estado en el que no se podrá recuperar.

Objetos multiparte o segmentados en Cloud Storage Pool

Si has subido un objeto multiparte o si StorageGRID ha dividido un objeto de gran tamaño en segmentos, StorageGRID determina si el objeto está disponible en el Cloud Storage Pool mediante un muestreo de un subconjunto de las partes o segmentos del objeto. En algunos casos, una solicitud de HeadObject podría devolver erróneamente `x-amz-restore: ongoing-request="false"` cuando algunas partes del objeto ya han pasado a un estado no recuperable o cuando algunas partes del objeto aún no se han restaurado.

HeadObject y la replicación entre grids

Si usas ["federación de grid"](#) y ["replicación entre grids"](#) está habilitado para un bucket, el cliente S3 puede verificar el estado de replicación de un objeto haciendo una solicitud HeadObject. La respuesta incluye el encabezado de respuesta específico de StorageGRID `x-ntap-sg-cgr-replication-status`, que tendrá uno de los siguientes valores:

Grid	Estado de la replicación
Fuente	• FINALIZADO: La replicación se realizó con éxito. • PENDIENTE: El objeto aún no se ha replicado. • ERROR: La replicación falló debido a un error permanente. Un usuario debe solucionar el error.
Destino	RÉPLICA: El objeto fue replicado desde la cuadrícula de origen.



StorageGRID no admite el encabezado `x-amz-replication-status`.

Agrega un objeto a un bucket en StorageGRID con la solicitud S3 PutObject

Puedes usar la solicitud PutObject de S3 para añadir un objeto a un bucket.

Resolver conflictos

Las solicitudes conflictivas de los clientes, como por ejemplo cuando dos clientes escriben en la misma clave, se resuelven según el principio de "la última gana". El momento en que se evalúa el principio de "la última gana" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes S3 inician una operación.

Tamaño del objeto

El tamaño máximo *recomendado* para una sola operación de PutObject es de 5 GiB (5,368,709,120 bytes). Si tienes objetos que superan los 5 GiB, utiliza ["carga en varias partes"](#) en su lugar.

El tamaño máximo *admitido* para una sola operación de PutObject es de 5 TiB (5,497,558,138,880 bytes).



Si has actualizado desde StorageGRID 11.6 o una versión anterior, se activará la alerta «S3 PUT Object size too large» si intentas cargar un objeto que supere los 5 GiB. Si tienes 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 de AWS S3, las futuras versiones de StorageGRID no admitirán cargas de objetos mayores a 5 GiB.

Tamaño de los metadatos de usuario

Amazon S3 limita el tamaño de los metadatos definidos por el usuario dentro de cada cabecera 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 sumando el número de bytes en la codificación UTF-8 de cada clave y valor.

Caracteres UTF-8 en los metadatos de usuario

Si una solicitud incluye valores UTF-8 (sin caracteres de escape) en el nombre de la clave o en el valor de los metadatos definidos por el usuario, el comportamiento de StorageGRID es indefinido.

StorageGRID no analiza ni interpreta los caracteres UTF-8 escapados incluidos en el nombre o el valor de los metadatos definidos por el usuario. Los caracteres UTF-8 escapados se tratan como caracteres ASCII:

- PutObject, CopyObject, GetObject y HeadObject las solicitudes se procesan correctamente si los metadatos definidos por el usuario incluyen caracteres UTF-8 escapados.
- StorageGRID no devuelve la cabecera x-amz-missing-meta si el valor interpretado del nombre o del valor de la clave incluye caracteres no imprimibles.

Límites de las etiquetas de objetos

Puedes añadir etiquetas a los objetos nuevos al subirlos, o puedes añadirlas a objetos ya existentes. Tanto StorageGRID como Amazon S3 admiten hasta 10 etiquetas por cada objeto. Las etiquetas asociadas a un objeto deben tener claves de etiqueta únicas. Una clave de etiqueta puede tener hasta 128 caracteres Unicode y los valores de las etiquetas pueden tener hasta 256 caracteres Unicode. Las claves y los valores distinguen mayúsculas de minúsculas.

Propiedad de los objetos

En StorageGRID, todos los objetos son propiedad de la cuenta del propietario del bucket, incluidos los objetos creados por una cuenta que no sea la del propietario o por un usuario anónimo.

Encabezados de solicitud compatibles

Se admiten los siguientes encabezados de solicitud:

- Cache-Control
- Content-Disposition
- Content-Encoding

Cuando especificas `aws-chunked` para `Content-Encoding` StorageGRID no verifica los siguientes elementos:

- StorageGRID no verifica el `chunk-signature` con los datos del fragmento.
- StorageGRID no verifica el valor que proporcionas para `x-amz-decoded-content-length` con 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 la 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, utiliza este formato general:

```
x-amz-meta-name: value
```

Si deseas utilizar la opción **Hora de creación definida por el usuario** como hora de referencia para una regla de ILM, debes utilizar `creation-time` como 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 calcula en segundos desde el 1 de enero de 1970.



Una regla de ILM no puede usar una **hora de creación definida por el usuario** para la hora de referencia y la opción de ingesta `Balanced` o `Strict` al mismo tiempo. Se devuelve un error al crear la regla de ILM.

- `x-amz-tagging`

- Encabezados de solicitud de S3 Object Lock

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

Si haces una solicitud sin estas cabeceras, se usa la configuración de retención predeterminada del bucket para calcular el modo de versión del objeto y la fecha de retención hasta. Consulta ["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#).

- 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 compatibles

No se admiten los siguientes encabezados de solicitud:

- `If-Match`

El `If-Match` header es aceptado pero no funciona.

- `If-None-Match`

El `If-None-Match` header es aceptado pero no funciona.

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

La `x-amz-website-redirect-location` cabecera devuelve `XNotImplemented`.

Opciones de clase de almacenamiento

Se admite el encabezado de solicitud `x-amz-storage-class`. El valor enviado para `x-amz-storage-class` afecta cómo StorageGRID protege los datos del objeto durante la ingesta y no cuántas copias persistentes del objeto se almacenan en el sistema StorageGRID (lo cual lo determina ILM).

Si la regla de ILM que coincide con un objeto ingerido utiliza la opción de ingesta Strict, la cabecera `x-amz-storage-class` no tiene efecto.

Se pueden usar los siguientes valores para `x-amz-storage-class`:

- **STANDARD (Por defecto)**

- **Dual commit:** Si la regla ILM especifica la opción Dual commit 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 Storage Node diferente (dual commit). Cuando se evalúa el ILM, StorageGRID determina si estas copias provisionales iniciales cumplen las instrucciones de ubicación en la regla. Si no lo hacen, puede que sea necesario crear nuevas copias del objeto en ubicaciones diferentes y eliminar las copias provisionales iniciales.
- **Equilibrado:** Si la regla de ILM especifica la opción Balanced y StorageGRID no puede crear de inmediato todas las copias especificadas en la regla, StorageGRID crea dos copias provisionales en distintos Storage Nodes.

Si StorageGRID puede crear inmediatamente todas las copias de objetos especificadas en la regla de ILM (colocación sincrónica), el encabezado `x-amz-storage-class` no tiene ningún efecto.

- **REDUCED_REDUNDANCY**

- **Doble confirmación:** Si la regla de ILM especifica la opción Doble confirmación para el comportamiento de ingesta, StorageGRID crea una única copia provisional al incorporar el objeto (confirmación única).
- **Equilibrado:** Si la regla ILM especifica la opción Equilibrado, StorageGRID crea una única copia provisional solo si el sistema no puede crear inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar una colocación sincrónica, este encabezado no tiene efecto. La `REDUCED_REDUNDANCY` opción se usa mejor cuando la regla de ILM que coincide con el objeto crea una sola copia replicada. En este caso, usar `REDUCED_REDUNDANCY` elimina la creación y eliminación innecesarias de una copia adicional del objeto en cada operación de ingesta.

No se recomienda utilizar la opción `REDUCED_REDUNDANCY` en otras circunstancias.

`REDUCED_REDUNDANCY` Aumenta el riesgo de pérdida de datos de objetos durante la ingesta. Por ejemplo, podrías perder datos si la única copia se almacena inicialmente en un Storage Node que falla antes de que pueda ocurrir la evaluación de ILM.



Disponer de una única copia replicada para cualquier periodo 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 Storage Node falla o tiene un error significativo. También pierdes temporalmente el acceso al objeto durante procedimientos de mantenimiento como las actualizaciones.

Especificar `REDUCED_REDUNDANCY` solo afecta al número de copias que se crean cuando un objeto se incorpora por primera vez. No afecta al número de copias del objeto que se crean cuando el objeto es evaluado por las políticas de ILM activas, ni da lugar a que los datos se almacenen con niveles de redundancia más bajos en el sistema StorageGRID.



Si estás ingiriendo un objeto en un bucket con S3 Object Lock activado, la opción `REDUCED_REDUNDANCY` se ignora. Si estás ingiriendo un objeto en un bucket Compliant heredado, la opción `REDUCED_REDUNDANCY` devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Encabezados de solicitud para el cifrado del lado del servidor

Puedes utilizar los siguientes encabezados de solicitud para cifrar un objeto mediante el cifrado del lado del servidor. Las opciones SSE y SSE-C son mutuamente excluyentes.

- **SSE:** Utiliza el siguiente encabezado si deseas cifrar el objeto con una clave única gestionada por StorageGRID.

- `x-amz-server-side-encryption`

Cuando la cabecera `x-amz-server-side-encryption` no se incluye en la solicitud `PutObject`, se omite "[Configuración de cifrado de objetos almacenados](#)" a nivel de grid de la respuesta de `PutObject`.

- **SSE-C:** Utiliza estos tres encabezados si deseas cifrar el objeto con una clave única que tú mismo proporcionas y gestionas.

- `x-amz-server-side-encryption-customer-algorithm`: Indica AES256.

- `x-amz-server-side-encryption-customer-key`: Indica tu clave de cifrado para el nuevo objeto.

- `x-amz-server-side-encryption-customer-key-MD5`: indica el resumen MD5 de la clave de cifrado del nuevo objeto.



Las claves de cifrado que facilites nunca se almacenan. Si pierdes una clave de cifrado, pierdes el objeto correspondiente. Antes de usar claves proporcionadas por el cliente para proteger los datos de los objetos, revisa las consideraciones para "[utilizando el 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 depósito o de grid.

Control de versiones

Si se ha habilitado el control de versiones para un bucket, se genera automáticamente un `versionId` único para la versión del objeto que se va a almacenar. Este `versionId` también se devuelve en la respuesta mediante el encabezado de respuesta `x-amz-version-id`.

Si se suspende el control de versiones, la versión del objeto se almacena con un `null versionId` y si ya existe una versión `null`, se sobrescribirá.

Cálculos de la firma para el encabezado «Authorization»

Al usar la cabecera `Authorization` para autenticar solicitudes, StorageGRID se diferencia de AWS de las siguientes formas:

- StorageGRID no requiere que los encabezados `host` se incluyan dentro de `CanonicalHeaders`.
- StorageGRID no requiere que se incluya `Content-Type` dentro de `CanonicalHeaders`.
- StorageGRID no requiere que `x-amz-*` las cabeceras se incluyan dentro de `CanonicalHeaders`.



Como buena práctica general, incluye siempre estos encabezados dentro de `CanonicalHeaders` para garantizar que se verifiquen; sin embargo, si los excluyes, StorageGRID no devuelve un error.

Para más detalles, consulta "[Cálculos de firma para el encabezado de autorización: transferir la carga útil en un único fragmento \(AWS Signature Version 4\)](#)".

Información relacionada

- ["Gestiona objetos con ILM"](#)
- ["Referencia de la API de Amazon Simple Storage Service: PutObject"](#)

Restaura un objeto en StorageGRID con la solicitud S3 RestoreObject

Puedes usar la solicitud S3 RestoreObject para restaurar un objeto que está almacenado en un Cloud Storage Pool.

Tipo de solicitud admitido

StorageGRID solo admite solicitudes RestoreObject para restaurar un objeto. No admite el tipo de restauración `SELECT`. Las solicitudes `Select` devuelven `XNotImplemented`.

Control de versiones

Opcionalmente, especifica `versionId` para restaurar una versión específica de un objeto en un bucket con control de versiones. Si no especificas `versionId`, se restaura la versión más reciente del objeto.

Comportamiento de RestoreObject en los objetos del Cloud Storage Pool

Si un objeto se ha almacenado en un ["Grupo de almacenamiento en la nube"](#), una solicitud de RestoreObject tiene el siguiente comportamiento, según el estado del objeto. Consulta ["HeadObject"](#) para más detalles.



Si un objeto se almacena en un Cloud Storage Pool y también existen una o más copias del objeto en el grid, no es necesario restaurar el objeto mediante una solicitud RestoreObject. En su lugar, la copia local se puede recuperar directamente usando una solicitud GetObject.

Estado del objeto	Comportamiento de RestoreObject
Objeto incorporado a StorageGRID pero aún no evaluado por ILM, o el objeto no está en un Cloud Storage Pool	403 Forbidden, InvalidObjectState
Objeto en el Cloud Storage Pool pero aún no ha pasado a un estado no recuperable	200 OK No se realizan cambios. Nota: antes de que un objeto haya realizado la transición a un estado no recuperable, no puedes cambiar su <code>expiry-date</code> .

Estado del objeto	Comportamiento de RestoreObject
El objeto pasó a un estado no recuperable	202 Accepted Restaura una copia recuperable del objeto en el Cloud Storage Pool durante el número de días especificado en el cuerpo de la solicitud. Al finalizar este periodo, el objeto vuelve a un estado no recuperable. Opcionalmente, usa el elemento de solicitud <code>Tier</code> para determinar cuánto tiempo tardará en finalizar el trabajo de restauración (<code>Expedited</code>, <code>Standard</code> o <code>Bulk</code>). Si no especificas <code>Tier</code>, se usa el tier <code>Standard</code>. Importante: si un objeto se ha transferido a S3 Glacier Deep Archive o el Cloud Storage Pool utiliza el almacenamiento de Azure Blob, no puedes restaurarlo mediante el nivel <code>Expedited</code>. Se devuelve el siguiente error 403 <code>Forbidden, InvalidTier: Retrieval option is not supported by this storage class</code>.
Objeto en proceso de restauración desde un estado no recuperable	409 Conflict, RestoreAlreadyInProgress
Objeto restaurado por completo en el Cloud Storage Pool	200 OK Nota: Si un objeto se ha restaurado a un estado recuperable, puedes cambiar su <code>expiry-date</code> volviendo a enviar la solicitud <code>RestoreObject</code> con un nuevo valor para <code>Days</code>. La fecha de restauración se actualiza en función de la hora de la solicitud.

Filtra datos de objetos en StorageGRID con la solicitud S3 SelectObjectContent

Puedes utilizar la solicitud `SelectObjectContent` de S3 para filtrar el contenido de un objeto de S3 basándote en una instrucción SQL sencilla.

Para obtener más información, consulta ["Referencia de la API de Amazon Simple Storage Service: SelectObjectContent"](#).

Antes de empezar

- La cuenta del inquilino tiene el permiso S3 Select.
- Tienes permiso de `s3:GetObject` para el objeto que quieres consultar.
- El objeto que deseas consultar debe tener uno de los siguientes formatos:
 - **CSV.** Se puede usar tal cual o comprimir 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 en formato Parquet. Debes especificar el formato de salida como CSV o JSON.
 - El tamaño máximo de un grupo de filas sin comprimir es de 512 MB.

- Debes utilizar los tipos de datos especificados en el esquema del objeto.
- No puedes usar los tipos lógicos INTERVAL, JSON, LIST, TIME ni UUID.
- Tu expresión SQL tiene una longitud máxima de 256 KB.
- Cualquier registro de la entrada o de los resultados tiene una longitud máxima de 1 MiB.

Ejemplo de sintaxis de solicitud CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <CSV>
      <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
      <Comments>#</Comments>
      <FieldDelimiter>\t</FieldDelimiter>
      <FileHeaderInfo>USE</FileHeaderInfo>
      <QuoteCharacter>'</QuoteCharacter>
      <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
      <RecordDelimiter>\n</RecordDelimiter>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

Ejemplo de sintaxis de solicitud de Parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <PARQUET>
    </PARQUET>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

Ejemplo de consulta SQL

Esta consulta obtiene el nombre del estado, la población en 2010, la población estimada en 2015 y el porcentaje de variación a partir 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 que se va a consultar, SUB-EST2020_ALL.csv, tienen este aspecto:


```
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`, tienen este aspecto:

```
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, tienen este aspecto:

```
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 en varias partes

Operaciones de carga multiparte compatibles en StorageGRID

Esta sección describe cómo StorageGRID admite las operaciones de subida de archivos en varias partes.

Las siguientes condiciones y notas se aplican a todas las operaciones de carga de varias partes:

- No debes superar 1,000 cargas multiparte simultáneas en un solo bucket porque los resultados de las consultas ListMultipartUploads para ese bucket podrían devolver resultados incompletos.
- StorageGRID aplica los límites de tamaño de AWS para las partes multiparte. Los clientes de S3 deben seguir estas directrices:
 - Cada parte de una subida en varias partes debe tener un tamaño comprendido entre 5 MiB (5,242,880 bytes) y 5 GiB (5,368,709,120 bytes).
 - La última parte puede tener un tamaño inferior a 5 MiB (5,242,880 bytes).
 - En general, el tamaño de las partes debe ser lo más grande posible. Por ejemplo, utiliza partes de 5 GiB para un objeto de 100 GiB. Dado que cada parte se considera un objeto único, usar partes de gran tamaño reduce la sobrecarga de metadatos de StorageGRID.
 - Para objetos de menos de 5 GiB, considera usar la carga no multiparte en su lugar.
- El ILM se evalúa para cada parte de un objeto multiparte a medida que se importa y para el objeto en su conjunto cuando finaliza la carga multiparte, si la regla de ILM utiliza Balanced o Strict ["opción de ingesta"](#). Debes tener en cuenta cómo esto afecta la ubicación del objeto y de sus partes:
 - Si el ILM cambia mientras se está realizando una subida multiparte a S3, es posible que algunas partes del objeto no cumplan los requisitos actuales del ILM cuando finalice la subida multiparte. Cualquier parte que no se haya colocado correctamente se pone en cola para una reevaluación del

ILM y se traslada posteriormente a la ubicación correcta.

- Al evaluar la ILM para una parte, StorageGRID aplica filtros en función del tamaño de la parte, no del tamaño del objeto. Esto significa que las partes de un objeto pueden almacenarse en ubicaciones que no cumplan los requisitos de ILM para el objeto en su conjunto. 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 el momento de la ingesta. Sin embargo, cuando se evalúa la ILM para el objeto en su conjunto, todas las partes del objeto se trasladan a DC1.
- Todas las operaciones de carga en varias partes son compatibles con StorageGRID ["valores de consistencia"](#).
- Cuando se ingiere un objeto usando la carga en varias partes, la ["umbral de segmentación de objetos \(1 GiB\)"](#) no se aplica.
- Si lo necesitas, puedes usar ["cifrado del lado del servidor"](#) con cargas multiparte. Para usar SSE (cifrado del lado del servidor con claves gestionadas por StorageGRID), incluyes el encabezado de solicitud `x-amz-server-side-encryption` solo en la solicitud `CreateMultipartUpload`. Para usar SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente), especificas los mismos tres encabezados de solicitud de claves de cifrado en la solicitud `CreateMultipartUpload` y en cada solicitud `UploadPart` posterior.
- Un objeto subido en varias partes se incluye en un ["bucket de rama"](#) si la importación se inició antes de la marca de tiempo `Before` del bucket base, independientemente de cuándo finalice la subida.

Operación	Implementación
<code>AbortMultipartUpload</code>	Implementado con todo el comportamiento de la API de REST de Amazon S3. Sujeto a cambios sin previo aviso.
<code>CompleteMultipartUpload</code>	Ver "CompleteMultipartUpload"
<code>CreateMultipartUpload</code> (anteriormente denominado <code>Initiate Multipart Upload</code>)	Ver "CreateMultipartUpload"
<code>ListMultipartUploads</code>	Ver "ListMultipartUploads"
<code>ListParts</code>	Implementado con todo el comportamiento de la API de REST de Amazon S3. Sujeto a cambios sin previo aviso.
<code>UploadPart</code>	Ver "UploadPart"
<code>UploadPartCopy</code>	Ver "UploadPartCopy"

Cómo la API de REST de StorageGRID S3 completa las cargas multiparte

La operación `CompleteMultipartUpload` completa la carga en varias partes de un objeto reuniendo las partes cargadas anteriormente.



StorageGRID admite valores no consecutivos en orden ascendente para el parámetro de solicitud `partNumber` con `CompleteMultipartUpload`. El parámetro puede comenzar con cualquier valor.

Resolver conflictos

Las solicitudes conflictivas de los clientes, como por ejemplo cuando dos clientes escriben en la misma clave, se resuelven según el principio de "la última gana". El momento en que se evalúa el principio de "la última gana" se basa en cuándo el sistema StorageGRID completa una solicitud determinada, y no en cuándo los clientes S3 inician una operación.

Encabezados de solicitud compatibles

Se admiten los siguientes encabezados de solicitud:

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

El `x-amz-storage-class` encabezado afecta cuántas copias de objetos crea StorageGRID si la regla ILM correspondiente especifica el ["Opción de doble confirmación o de ingesta equilibrada"](#).

- `STANDARD`

(Por defecto) Especifica una operación de ingesta con doble confirmación cuando la regla de ILM utiliza la opción de doble confirmación 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 utiliza la opción de confirmación doble o cuando la opción equilibrada recurre a la creación de copias provisionales.



Si estás ingiriendo un objeto en un bucket con S3 Object Lock activado, la opción `REDUCED_REDUNDANCY` se ignora. Si estás ingiriendo un objeto en un bucket Compliant heredado, la opción `REDUCED_REDUNDANCY` devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.



Si una carga en varias partes no se completa en un plazo de 15 días, la operación se marca como inactiva y todos los datos asociados se eliminan del sistema.



El `ETag` valor devuelto no es una suma MD5 de los datos, sino que sigue la implementación de la API de Amazon S3 del `ETag` valor para objetos multiparte.

Encabezados de solicitud no compatibles

No se admiten los siguientes encabezados de solicitud:

- `If-Match`

El `If-Match` header es aceptado pero no funciona.

- If-None-Match

El If-None-Match header es aceptado pero no funciona.

- x-amz-sdk-checksum-algorithm
- x-amz-trailer

Control de versiones

Esta operación finaliza una carga en varias partes. Si el control de versiones está habilitado para un bucket, la versión del objeto se crea después de completar la carga en varias partes.

Si se ha habilitado el control de versiones para un bucket, se genera automáticamente un `versionId` único para la versión del objeto que se va a almacenar. Este `versionId` también se devuelve en la respuesta mediante el encabezado de respuesta `x-amz-version-id`.

Si se suspende el control de versiones, la versión del objeto se almacena con un `null versionId` y si ya existe una versión `null`, se sobrescribirá.



Cuando el control de versiones está habilitado para un bucket, al completar una subida multiparte siempre se crea una nueva versión, incluso si hay subidas multiparte simultáneas que se completan en la misma clave de objeto. Cuando el control de versiones no está habilitado para un bucket, es posible iniciar una subida multiparte y luego que otra subida multiparte se inicie y complete primero en la misma clave de objeto. En los buckets sin control de versiones, la subida multiparte que se complete al final tiene prioridad.

Error en la replicación, la notificación o la notificación de metadatos

Si el bucket en el que se realiza la carga multiparte está configurado para un servicio de plataforma, la carga multiparte se realiza con éxito incluso si falla la acción de replicación o notificación asociada.

Un inquilino puede provocar el fallo en la replicación o la notificación al actualizar los metadatos o las etiquetas del objeto. Un inquilino puede volver a enviar los valores existentes para evitar hacer cambios no deseados.

Consulta ["Soluciona problemas de los servicios de la plataforma"](#).

Cabeceras y opciones de solicitud S3 CreateMultipartUpload en StorageGRID

La operación `CreateMultipartUpload` (anteriormente denominada `Initiate Multipart Upload`) inicia una carga multiparte para un objeto y devuelve un ID de carga.

Se admite el encabezado de solicitud `x-amz-storage-class`. El valor enviado para `x-amz-storage-class` afecta cómo StorageGRID protege los datos del objeto durante la ingesta y no cuántas copias persistentes del objeto se almacenan en el sistema StorageGRID (lo cual lo determina ILM).

Si la regla de ILM que coincide con un objeto importado utiliza Strict ["opción de ingesta"](#), el `x-amz-storage-class` header no tiene ningún efecto.

Se pueden usar los siguientes valores para `x-amz-storage-class`:

- STANDARD (Por defecto)

- **Dual commit:** Si la regla ILM especifica la opción de ingesta Dual commit, tan pronto como se ingiere un objeto, se crea una segunda copia de ese objeto y se distribuye a un Storage Node diferente (dual commit). Cuando se evalúa la ILM, StorageGRID determina si estas copias provisionales iniciales cumplen las instrucciones de ubicación en la regla. Si no lo hacen, podría ser necesario crear nuevas copias del objeto en ubicaciones diferentes y eliminar las copias provisionales iniciales.
- **Equilibrado:** Si la regla de ILM especifica la opción Balanced y StorageGRID no puede crear de inmediato todas las copias especificadas en la regla, StorageGRID crea dos copias provisionales en distintos Storage Nodes.

Si StorageGRID puede crear inmediatamente todas las copias de objetos especificadas en la regla de ILM (colocación sincrónica), el encabezado `x-amz-storage-class` no tiene ningún efecto.

- `REDUCED_REDUNDANCY`

- **Confirmación doble:** Si la regla de ILM especifica la opción de confirmación doble, StorageGRID crea una única copia provisional en el momento de la ingesta del objeto (confirmación única).
- **Equilibrado:** Si la regla ILM especifica la opción Equilibrado, StorageGRID crea una única copia provisional solo si el sistema no puede crear inmediatamente todas las copias especificadas en la regla. Si StorageGRID puede realizar una colocación sincrónica, este encabezado no tiene efecto. La `REDUCED_REDUNDANCY` opción se usa mejor cuando la regla de ILM que coincide con el objeto crea una sola copia replicada. En este caso, usar `REDUCED_REDUNDANCY` elimina la creación y eliminación innecesarias de una copia adicional del objeto en cada operación de ingesta.

No se recomienda utilizar la opción `REDUCED_REDUNDANCY` en otras circunstancias.

`REDUCED_REDUNDANCY` Aumenta el riesgo de pérdida de datos de objetos durante la ingesta. Por ejemplo, podrías perder datos si la única copia se almacena inicialmente en un Storage Node que falla antes de que pueda ocurrir la evaluación de ILM.



Disponer de una única copia replicada para cualquier periodo 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 Storage Node falla o tiene un error significativo. También pierdes temporalmente el acceso al objeto durante procedimientos de mantenimiento como las actualizaciones.

Especificar `REDUCED_REDUNDANCY` solo afecta al número de copias que se crean cuando un objeto se incorpora por primera vez. No afecta al número de copias del objeto que se crean cuando el objeto es evaluado por las políticas de ILM activas, ni da lugar a que los datos se almacenen con niveles de redundancia más bajos en el sistema StorageGRID.



Si estás ingiriendo un objeto en un bucket con S3 Object Lock activado, la opción `REDUCED_REDUNDANCY` se ignora. Si estás ingiriendo un objeto en un bucket Compliant heredado, la opción `REDUCED_REDUNDANCY` devuelve un error. StorageGRID siempre realizará una ingesta con doble confirmación para garantizar que se cumplan los requisitos de cumplimiento.

Encabezados de solicitud compatibles

Se admiten los siguientes encabezados de solicitud:

- `Content-Type`
- `x-amz-checksum-algorithm`

Actualmente, solo se admite el valor SHA256 de `x-amz-checksum-algorithm`.

- `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, utiliza este formato general:

```
x-amz-meta-_name_: `value`
```

Si deseas utilizar la opción **Hora de creación definida por el usuario** como hora de referencia para una regla de ILM, debes utilizar `creation-time` como 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 calcula en segundos desde el 1 de enero de 1970.



No está permitido añadir `creation-time` como metadatos definidos por el usuario si estás añadiendo un objeto a un bucket que tiene habilitado el Compliance heredado. Se devolverá un error.

- Encabezados de solicitud de S3 Object Lock:

- `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 usan los ajustes de retención predeterminados del bucket para calcular la fecha de retención de la versión del objeto.

["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#)

- 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 gestiona StorageGRID los caracteres UTF-8, consulta ["PutObject"](#).

Encabezados de solicitud para el cifrado del lado del servidor

Puedes utilizar los siguientes encabezados de solicitud para cifrar un objeto multiparte mediante cifrado del

lado del servidor. Las opciones SSE y SSE-C son mutuamente excluyentes.

- **SSE:** Usa el siguiente encabezado en la solicitud CreateMultipartUpload si quieres cifrar el objeto con una clave única gestionada por StorageGRID. No especifiques este encabezado en ninguna de las solicitudes UploadPart.

- `x-amz-server-side-encryption`

- **SSE-C:** Utiliza estos tres encabezados en la solicitud CreateMultipartUpload (y en cada solicitud posterior UploadPart) si quieres cifrar el objeto con una clave única que tú mismo proporcionas y gestionas.

- `x-amz-server-side-encryption-customer-algorithm`: Indica AES256.

- `x-amz-server-side-encryption-customer-key`: Indica tu clave de cifrado para el nuevo objeto.

- `x-amz-server-side-encryption-customer-key-MD5`: indica el resumen MD5 de la clave de cifrado del nuevo objeto.



Las claves de cifrado que facilites nunca se almacenan. Si pierdes una clave de cifrado, pierdes el objeto correspondiente. Antes de usar claves proporcionadas por el cliente para proteger los datos de los objetos, revisa las consideraciones para ["utilizando el cifrado del lado del servidor"](#).

Encabezados de solicitud no compatibles

No se admite el siguiente encabezado de solicitud:

- `x-amz-website-redirect-location`

La `x-amz-website-redirect-location` cabecera devuelve XNotImplemented.

Control de versiones

La carga en varias partes consta de operaciones independientes para iniciar la carga, mostrar la lista de cargas, cargar las partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si aplica) cuando se realiza la operación CompleteMultipartUpload.

S3 ListMultipartUploads operación y parámetros compatibles en StorageGRID

La operación ListMultipartUploads muestra las subidas multiparte en curso de un bucket.

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 en varias partes consta de operaciones independientes para iniciar la carga, mostrar la lista de cargas, cargar las partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si aplica) cuando se realiza la operación CompleteMultipartUpload.

Cabeceras de solicitud admitidas y no admitidas para operaciones S3 UploadPart en StorageGRID

La operación UploadPart carga una parte en una carga multiparte de un objeto.

Encabezados de solicitud compatibles

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 has especificado el cifrado SSE-C para la solicitud CreateMultipartUpload, también debes incluir los siguientes encabezados de solicitud en cada solicitud UploadPart:

- x-amz-server-side-encryption-customer-algorithm: Indica AES256.
- x-amz-server-side-encryption-customer-key: Indica la misma clave de cifrado que proporcionaste en la solicitud CreateMultipartUpload.
- x-amz-server-side-encryption-customer-key-MD5: Indica el mismo resumen MD5 que proporcionaste en la solicitud CreateMultipartUpload.



Las claves de cifrado que facilites nunca se almacenan. Si pierdes una clave de cifrado, pierdes el objeto correspondiente. Antes de usar claves proporcionadas por el cliente para proteger los datos de los objetos, revisa las consideraciones en ["Utiliza el cifrado del lado del servidor"](#).

Si especificaste una suma de comprobación SHA-256 durante la solicitud CreateMultipartUpload, también debes incluir el siguiente encabezado de solicitud en cada solicitud UploadPart:

- x-amz-checksum-sha256: Indica la suma de comprobación SHA-256 para esta parte.

Encabezados de solicitud no compatibles

No se admiten los siguientes encabezados de solicitud:

- x-amz-sdk-checksum-algorithm
- x-amz-trailer

Control de versiones

La carga en varias partes consta de operaciones independientes para iniciar la carga, mostrar la lista de cargas, cargar las partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si aplica) cuando se realiza la operación CompleteMultipartUpload.

Carga una parte de un objeto en StorageGRID con la operación S3 UploadPartCopy

La operación UploadPartCopy carga una parte de un objeto copiando datos de un objeto ya existente como fuente de datos.

La operación UploadPartCopy se implementa con todo el comportamiento de la API de 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 has especificado el cifrado SSE-C para la solicitud CreateMultipartUpload, también debes incluir los siguientes encabezados de solicitud en cada solicitud UploadPartCopy:

- `x-amz-server-side-encryption-customer-algorithm`: Indica AES256.
- `x-amz-server-side-encryption-customer-key`: Indica la misma clave de cifrado que proporcionaste en la solicitud CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Indica el mismo resumen MD5 que proporcionaste en la solicitud CreateMultipartUpload.

Si el objeto de origen está cifrado con una clave proporcionada por el cliente (SSE-C), debes 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`: indica AES256.
- `x-amz-copy-source-server-side-encryption-customer-key`: especifica la clave de cifrado que proporcionaste cuando creaste el objeto de origen.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Indica el resumen MD5 que proporcionaste cuando creaste el objeto de origen.



Las claves de cifrado que facilites nunca se almacenan. Si pierdes una clave de cifrado, pierdes el objeto correspondiente. Antes de usar claves proporcionadas por el cliente para proteger los datos de los objetos, revisa las consideraciones en ["Utiliza el cifrado del lado del servidor"](#).

Control de versiones

La carga en varias partes consta de operaciones independientes para iniciar la carga, mostrar la lista de cargas, cargar las partes, ensamblar las partes cargadas y completar la carga. Los objetos se crean (y se versionan si aplica) cuando se realiza la operación CompleteMultipartUpload.

Respuestas de error de StorageGRID S3 API de REST

El sistema StorageGRID admite todas las respuestas de error estándar de la API de REST de S3 que sean aplicables. Además, la implementación de StorageGRID añade varias respuestas personalizadas.

Códigos de error compatibles con la API de S3

Nombre	Estado HTTP
AccessDenied	403 Prohibido
BadDigest	400 Solicitud incorrecta
BucketAlreadyExists	409 Conflicto
BucketNotEmpty	409 Conflicto
IncompleteBody	400 Solicitud incorrecta
InternalError	Error 500 interno del servidor
InvalidAccessKeyId	403 Prohibido
InvalidArgument	400 Solicitud incorrecta
InvalidBucketName	400 Solicitud incorrecta
InvalidBucketState	409 Conflicto
InvalidDigest	400 Solicitud incorrecta
InvalidEncryptionAlgorithmError	400 Solicitud incorrecta
InvalidPart	400 Solicitud incorrecta
InvalidPartOrder	400 Solicitud incorrecta
InvalidRange	416 Rango solicitado no satisfactorio
InvalidRequest	400 Solicitud incorrecta
InvalidStorageClass	400 Solicitud incorrecta
InvalidTag	400 Solicitud incorrecta

Nombre	Estado HTTP
URI no válido	400 Solicitud incorrecta
KeyTooLong	400 Solicitud incorrecta
XML con errores de formato	400 Solicitud incorrecta
MetadataTooLarge	400 Solicitud incorrecta
MethodNotAllowed	405 Método no permitido
MissingContentLength	411 Longitud requerida
MissingRequestBodyError	400 Solicitud incorrecta
MissingSecurityHeader	400 Solicitud incorrecta
NoSuchBucket	404 No encontrado
NoSuchKey	404 No encontrado
NoSuchUpload	404 No encontrado
NotImplemented	501 No implementado
NoSuchBucketPolicy	404 No encontrado
ObjectLockConfigurationNotFoundError	404 No encontrado
PreconditionFailed	412 Condición previa no cumplida
RequestTimeTooSkewed	403 Prohibido
ServiceUnavailable	503 Servicio no disponible
SignatureDoesNotMatch	403 Prohibido
TooManyBuckets	400 Solicitud incorrecta
UserKeyMustBeSpecified	400 Solicitud incorrecta

Códigos de error personalizados de StorageGRID

Nombre	Descripción	Estado HTTP
XBucketLifecycleNotAllowed	No se permite la configuración del ciclo de vida de un bucket Compliant heredado	400 Solicitud incorrecta
XBucketPolicyParseException	No se pudo analizar el JSON de la política del bucket recibido.	400 Solicitud incorrecta
XComplianceConflict	Operación denegada debido a la configuración heredada de Compliance.	403 Prohibido
XComplianceReducedRedundancyForbidden	No se permite la redundancia reducida en el bucket Compliant heredado.	400 Solicitud incorrecta
XMaxBucketPolicyLengthExceeded	Tu política supera la longitud máxima permitida para una bucket policy.	400 Solicitud incorrecta
XMissingInternalRequestHeader	Falta un encabezado en una solicitud interna.	400 Solicitud incorrecta
XNoSuchBucketCompliance	El bucket especificado no tiene habilitado el Compliance heredado.	404 No encontrado
XNoAcceptable	La solicitud contiene uno o varios encabezados «Accept» que no se pudieron satisfacer.	406 No aceptable
XNotImplemented	La solicitud que has enviado implica una funcionalidad que no está implementada.	501 No implementado

Operaciones personalizadas de StorageGRID

Operaciones personalizadas de bucket admitidas en StorageGRID

El sistema StorageGRID admite operaciones personalizadas que se añaden a la API de REST de S3.

La siguiente tabla muestra las operaciones personalizadas que admite StorageGRID.

Operación	Descripción
"Obtener la consistencia del Bucket"	Devuelve el nivel de consistencia que se aplica a un bucket concreto.
"Consistencia de PUT Bucket"	Establece la consistencia que se aplica a un bucket concreto.
"Obtener el tiempo de último acceso al Bucket"	Indica si las actualizaciones del tiempo de acceso más reciente están habilitadas o deshabilitadas para un bucket concreto.

Operación	Descripción
"PUT Bucket tiempo de acceso más reciente"	Te permite activar o desactivar las actualizaciones del tiempo de acceso más reciente para un bucket concreto.
"ELIMINAR configuración de notificaciones de metadatos del bucket"	Elimina el archivo XML de configuración de notificaciones de metadatos asociado a un bucket en particular.
"Obtener configuración de notificaciones de metadatos del bucket"	Devuelve el XML de configuración de notificaciones de metadatos asociado a un bucket concreto.
"PUT Bucket configuración de notificación de metadatos"	Configura el servicio de notificación de metadatos para un bucket.
"Obtener uso del almacenamiento"	Te dice la cantidad total de almacenamiento en uso por una cuenta y para cada bucket asociado con la cuenta.
"Obsoleto: CreateBucket con la configuración de cumplimiento"	Obsoleto y sin soporte: ya no puedes crear nuevos buckets con Compliance activado.
"Obsoleto: GET Bucket compliance"	Obsoleto pero compatible: Devuelve la configuración de cumplimiento vigente actualmente para un bucket Compliant heredado ya existente.
"Obsoleto: PUT Bucket compliance"	Obsoleto, pero compatible: te permite modificar la configuración de cumplimiento para un depósito Compliant heredado ya existente.

Recupera el nivel de consistencia del bucket en StorageGRID con la solicitud GET Bucket consistency

La solicitud de consistencia de GET Bucket te permite determinar la consistencia que se aplica a un bucket concreto.

La consistencia predeterminada está configurada para garantizar la lectura posterior a la escritura para los objetos recién creados.

Debes tener el permiso s3:GetBucketConsistency o ser el usuario raíz de la cuenta para completar esta operación.

Ejemplo de solicitud

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Respuesta

En el XML de respuesta, <Consistency> devolverá uno de los siguientes valores:

Coherencia	Descripción
all	Todos los nodos reciben los datos de inmediato o la solicitud fallará.
strong-global	Garantiza la consistencia de lectura tras escritura para todas las solicitudes de los clientes en todos los sitios.
sitio fuerte	Garantiza la consistencia de lectura tras escritura para todas las solicitudes de los clientes dentro de un sitio.
lectura tras una nueva escritura	(Predeterminado) Proporciona consistencia de lectura después de escritura para los objetos nuevos y consistencia eventual para las 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 los objetos nuevos como para las actualizaciones de objetos. Para los buckets de S3, úsalo 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 es compatible con los buckets de 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

["Coherencia"](#)

Especifica los niveles de consistencia en StorageGRID con la solicitud de consistencia PUT Bucket

La solicitud de consistencia de PUT Bucket te permite especificar la consistencia que se aplicará a las operaciones realizadas en un bucket.

La consistencia predeterminada está configurada para garantizar la lectura posterior a la escritura para los objetos recién creados.

Antes de empezar

Debes tener el permiso `s3:PutBucketConsistency`, o ser la raíz de la cuenta, para completar esta operación.

Solicitud

El `x-ntap-sg-consistency` parámetro debe contener uno de los siguientes valores:

Coherencia	Descripción
all	Todos los nodos reciben los datos de inmediato o la solicitud fallará.
strong-global	Garantiza la consistencia de lectura tras escritura para todas las solicitudes de los clientes en todos los sitios.
sitio fuerte	Garantiza la consistencia de lectura tras escritura para todas las solicitudes de los clientes dentro de un sitio.
lectura tras una nueva escritura	(Predeterminado) Proporciona consistencia de lectura después de escritura para los objetos nuevos y consistencia eventual para las 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 los objetos nuevos como para las actualizaciones de objetos. Para los buckets de S3, úsalo 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 es compatible con los buckets de S3 FabricPool.

Nota: En general, deberías usar la consistencia "Read-after-new-write". Si las solicitudes no funcionan correctamente, cambia el comportamiento del cliente de la aplicación si es posible. O configura el cliente para que especifique la consistencia en cada solicitud de API. Establece la consistencia a nivel de bucket solo 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

["Coherencia"](#)

Recupera el estado del tiempo de último acceso al bucket en StorageGRID con la solicitud GET Bucket last access time

La solicitud de tiempo de acceso último de GET Bucket te permite determinar si las actualizaciones del tiempo de acceso último están activadas o desactivadas para cada bucket.

Debes tener el permiso s3:GetBucketLastAccessTime o ser el usuario raíz 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 tiempo de acceso más reciente están habilitadas para el bucket.

```
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>
```

Activar y desactivar las actualizaciones del tiempo de último acceso en StorageGRID con la solicitud PUT Bucket last access time

La solicitud PUT Bucket last access time te permite activar o desactivar las actualizaciones del tiempo de acceso para buckets individuales. Desactivar las actualizaciones del tiempo de acceso mejora el rendimiento y es la configuración predeterminada para todos los buckets creados con la versión 10.3.0 o posterior.

Debes tener el permiso s3:PutBucketLastAccessTime para un bucket, o ser el root de la cuenta, para completar esta operación.



A partir de la versión 10.3 de StorageGRID, las actualizaciones del último tiempo de acceso están desactivadas de forma predeterminada para todos los buckets nuevos. Si tienes buckets creados con una versión anterior de StorageGRID y quieres que coincidan con el nuevo comportamiento predeterminado, debes desactivar explícitamente las actualizaciones del último tiempo de acceso para cada uno de esos buckets anteriores. Puedes activar o desactivar las actualizaciones del último tiempo de acceso mediante la solicitud PUT Bucket last access time o desde la página de detalles de un bucket en el Tenant Manager. Consulta ["Activar o desactivar las actualizaciones del último tiempo de acceso"](#).

Si las actualizaciones del tiempo de acceso más reciente están desactivadas para un bucket, se aplica el siguiente comportamiento a las operaciones en el bucket:

- GetObject, GetObjectAcl, GetObjectTagging y HeadObject no actualizan el tiempo de acceso. El objeto no se añade a las colas para la evaluación del ciclo de vida de la información (ILM).
- Las solicitudes CopyObject y PutObjectTagging que actualizan solo los metadatos también actualizan el tiempo de acceso. El objeto se añade a las colas para la evaluación de ILM.
- Si las actualizaciones del tiempo de último acceso están desactivadas para el bucket de origen, las solicitudes CopyObject no actualizan el tiempo de último acceso para el bucket de origen. El objeto que se copió no se añade a las colas para la evaluación de ILM del bucket de origen. Sin embargo, para el destino, las solicitudes CopyObject siempre actualizan el tiempo de último acceso. La copia del objeto se añade a las colas para la evaluación de ILM.
- Las solicitudes de CompleteMultipartUpload actualizan el último tiempo de acceso. El objeto completado se añade a las colas para la evaluación de ILM.

Ejemplos de solicitudes

Este ejemplo habilita el tiempo de último acceso para un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Este ejemplo desactiva el tiempo de acceso más reciente de un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Desactiva el servicio de integración de búsqueda con la solicitud de configuración de notificación de metadatos DELETE Bucket en StorageGRID

La solicitud de configuración de notificaciones de metadatos de DELETE Bucket te permite desactivar el servicio de integración de búsqueda para buckets concretos eliminando el archivo XML de configuración.

Debes tener el permiso `s3:DeleteBucketMetadataNotification` para un bucket, o ser account root, para completar esta operación.

Ejemplo de solicitud

Este ejemplo muestra cómo desactivar el servicio de integración de búsqueda para un bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Configura la integración de búsqueda en StorageGRID con la solicitud GET Bucket metadata notification configuration

La solicitud de configuración de notificaciones de metadatos de GET Bucket te permite recuperar el XML de configuración que se utiliza para configurar la integración de búsqueda para buckets individuales.

Debes tener el permiso `s3:GetBucketMetadataNotification` o ser el usuario raíz de la cuenta para completar esta operación.

Ejemplo de solicitud

Esta solicitud recupera la configuración de notificaciones de metadatos del bucket llamado `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 notificaciones de metadatos del bucket. La configuración de notificaciones de metadatos te permite determinar cómo se configura el bucket para la integración con la búsqueda. Es decir, te permite determinar qué objetos se indexan y a qué endpoints se envían los metadatos de dichos objetos.

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>

```

Cada configuración de notificación de metadatos incluye una o varias reglas. Cada regla especifica los objetos a los que se aplica y el destino donde StorageGRID debe enviar los metadatos de los objetos. Los destinos deben especificarse usando el URN de un endpoint de StorageGRID.

Nombre	Descripción	Requerido
MetadataNotificationConfiguration	Etiqueta de contenedor para las reglas que se utilizan para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o varios elementos «Rule».	Sí
Regla	Etiqueta de contenedor para una regla que identifica los objetos cuyos metadatos deben añadirse a un índice específico. Se rechazan las reglas cuyos prefijos se solapan. Incluido en el elemento MetadataNotificationConfiguration.	Sí
ID	Identificador único de la regla. Incluido en el elemento Rule.	No
Estado	El estado puede ser «Activado» o «Desactivado». No se realiza ninguna acción para las reglas que están desactivadas. Incluido en el elemento Rule.	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 coincidan todos los objetos, especifica un prefijo vacío. Incluido en el elemento Rule.	Sí
Destino	Etiqueta de contenedor para el destino de una regla. Incluido en el elemento Rule.	Sí
Urna	URN del destino al que se envían los metadatos del objeto. Debe ser el URN de un endpoint de StorageGRID con las siguientes propiedades: • <code>es</code> debe ser el tercer elemento. • El URN debe terminar con el índice y el tipo en los que se almacenan los metadatos, en el formato <code>domain-name/myindex/mytype</code>. Los puntos finales se configuran mediante el Tenant Manager o la Tenant Management API. Tienen el siguiente formato: • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> El endpoint debe configurarse antes de enviar el archivo XML de configuración o la configuración fallará con un error 404. Urn se incluye en el elemento Destination.	Sí

Ejemplo de respuesta

El código XML incluido entre las etiquetas

`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` muestra cómo se configura la integración con un endpoint de integración de búsqueda para el bucket. En este ejemplo, los metadatos de los objetos se envían a un índice de Elasticsearch llamado `current` y a un tipo llamado `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

["Utiliza una cuenta de inquilino"](#)

Habilita el servicio de integración de búsqueda en StorageGRID con la solicitud de configuración de notificación de metadatos PUT Bucket

La solicitud de configuración de notificaciones de metadatos de PUT Bucket te permite habilitar el servicio de integración de búsqueda para buckets concretos. El archivo XML de configuración de notificaciones de metadatos que facilitas en el cuerpo de la solicitud especifica los objetos cuyos metadatos se envían al índice de búsqueda de destino.

Debes tener el permiso `s3:PutBucketMetadataNotification` para un bucket, o ser account root, para completar esta operación.

Solicitud

La solicitud debe incluir la configuración de notificación de metadatos en el cuerpo de la solicitud. Cada configuración de notificación de metadatos incluye una o más reglas. Cada regla especifica los objetos a los que se aplica y el destino al que StorageGRID debe enviar los metadatos de los objetos.

Los objetos se pueden filtrar según el prefijo del nombre del objeto. Por ejemplo, podrías enviar los metadatos de los objetos con el prefijo `/images` a un destino y los objetos con el prefijo `/videos` a otro.

Las configuraciones que contengan prefijos que se solapen no son válidas y se rechazan al enviarlas. Por ejemplo, una configuración que incluyera una regla para objetos con el prefijo `test` y una segunda regla para objetos con el prefijo `test2` no estaría permitida.

Debes especificar los destinos mediante el URN de un endpoint de StorageGRID. El endpoint debe existir

cuando se envíe la configuración de notificación de metadatos o, de lo contrario, la solicitud fallará como 400 Bad Request. El mensaje de error indica: Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: *URN*.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

La tabla describe los elementos en el archivo XML de configuración de notificación de metadatos.

Nombre	Descripción	Requerido
MetadataNotificationConfi guration	Etiqueta de contenedor para las reglas que se utilizan para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o varios elementos «Rule».	Sí
Regla	Etiqueta de contenedor para una regla que identifica los objetos cuyos metadatos deben añadirse a un índice específico. Se rechazan las reglas cuyos prefijos se solapan. Incluido en el elemento MetadataNotificationConfiguration.	Sí
ID	Identificador único de la regla. Incluido en el elemento Rule.	No

Nombre	Descripción	Requerido
Estado	El estado puede ser «Activado» o «Desactivado». No se realiza ninguna acción para las reglas que están desactivadas. Incluido en el elemento Rule.	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 coincidan todos los objetos, especifica un prefijo vacío. Incluido en el elemento Rule.	Sí
Destino	Etiqueta de contenedor para el destino de una regla. Incluido en el elemento Rule.	Sí
Urna	URN del destino al que se envían los metadatos del objeto. Debe ser el URN de un endpoint de StorageGRID con las siguientes propiedades: • <code>es</code> debe ser el tercer elemento. • El URN debe terminar con el índice y el tipo en los que se almacenan los metadatos, en el formato <code>domain-name/myindex/mytype</code>. Los puntos finales se configuran mediante el Tenant Manager o la Tenant Management API. Tienen el siguiente formato: • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> El endpoint debe configurarse antes de enviar el archivo XML de configuración o la configuración fallará con un error 404. Urn se incluye en el elemento Destination.	Sí

Ejemplos de solicitudes

Este ejemplo muestra cómo habilitar la integración de búsqueda para un bucket. En este ejemplo, los metadatos de objeto de todos los objetos se envían al mismo destino.


```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:sgws:es::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

En este ejemplo, los metadatos de los objetos que coinciden con el prefijo `/images` se envían a un destino, mientras que los metadatos de los objetos que coinciden con el prefijo `/videos` se envían 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

Al habilitar el servicio de integración de búsqueda para un bucket, se genera un documento JSON y se envía al endpoint de destino cada vez que se añaden, actualizan o eliminan metadatos o etiquetas de un objeto.

Este ejemplo muestra un ejemplo del JSON que se podría generar cuando se crea un objeto con la clave SGWS/Tagging.txt en un bucket llamado test. El bucket test no está versionado, así que la etiqueta versionId 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 notificaciones de metadatos

La tabla recoge todos los campos que se incluyen en el documento JSON que se envía al endpoint de destino cuando se habilita la integración de búsqueda.

El nombre del documento incluye el nombre del bucket, el nombre del objeto y el ID de versión, si lo hay.

Tipo	Nombre del artículo	Descripción
Información del bucket y del objeto	bucket	Nombre del bucket
Información del bucket y del objeto	clave	Nombre de clave de objeto
Información del bucket y del objeto	ID de versión	Versión del objeto, para objetos en buckets con control de versiones
Información del bucket y del objeto	región	Región del bucket, por ejemplo us-east-1
Metadatos del sistema	tamaño	Tamaño del objeto (en bytes) tal y como lo ve un cliente HTTP
Metadatos del sistema	md5	Hash del objeto
Metadatos del usuario	metadatos <i>key:value</i>	Todos los metadatos de usuario del objeto, en forma de pares clave-valor

Tipo	Nombre del artículo	Descripción
Etiquetas	etiquetas <i>key:value</i>	Todas las etiquetas definidas para el objeto, en forma de pares clave-valor



Para las etiquetas y los metadatos de usuario, StorageGRID pasa las fechas y los números a Elasticsearch como cadenas o como notificaciones de eventos de S3. Para configurar Elasticsearch para que interprete estas cadenas como fechas o números, sigue las instrucciones de Elasticsearch para el mapeo dinámico de campos y para el mapeo de formatos de fecha. Debes habilitar los mapeos dinámicos de campos en el índice antes de configurar el servicio de integración de búsqueda. Una vez indexado un documento, no puedes editar los tipos de campo del documento en el índice.

Información relacionada

["Utiliza una cuenta de inquilino"](#)

Recupera el uso de almacenamiento de cuentas y buckets en StorageGRID con la solicitud GET Storage Usage

La solicitud GET Storage Usage te indica la cantidad total de almacenamiento que utiliza una cuenta y la de cada bucket asociado a la cuenta.

La cantidad de almacenamiento utilizada por una cuenta y sus buckets se puede obtener mediante una solicitud modificada de ListBuckets con el parámetro de consulta `x-ntap-sg-usage`. El uso de almacenamiento de los buckets se registra por separado de las solicitudes PUT y DELETE procesadas por el sistema. Puede producirse cierto retraso antes de que los valores de uso coincidan con los valores esperados en función del procesamiento de las solicitudes, especialmente si el sistema está sometido a una carga elevada.

De forma predeterminada, StorageGRID intenta recuperar la información de uso mediante consistencia global fuerte. Si no es posible lograr la consistencia global fuerte, StorageGRID intenta recuperar la información de uso con consistencia fuerte a nivel de sitio.

Debes tener el permiso `s3:ListAllMyBuckets` o ser root de la cuenta para completar esta operación.

Ejemplo de solicitud

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Ejemplo de respuesta

Este ejemplo muestra una cuenta que tiene cuatro objetos y 12 bytes de datos en dos buckets. Cada bucket 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 los valores de `ObjectCount` y `DataBytes` en la respuesta. Los marcadores de eliminación no se añaden al total de `ObjectCount`.

Información relacionada

["Coherencia"](#)

Solicitudes de bucket obsoletas para legacy Compliance

Solicitudes obsoletas de bucket para la antigua StorageGRID Compliance

Es posible que tengas que utilizar la API de REST de StorageGRID S3 para gestionar los buckets que se crearon mediante la función de cumplimiento normativo heredada.

Función de cumplimiento obsoleta

La función Compliance de StorageGRID que estaba disponible en versiones anteriores de StorageGRID está obsoleta y ha sido reemplazada por S3 Object Lock.

Si anteriormente habías activado la configuración global de Compliance, la configuración global de S3 Object Lock estará activada en StorageGRID 11.6. Ya no puedes crear nuevos buckets con Compliance activado; sin embargo, si lo necesitas, puedes usar la API de REST de StorageGRID S3 para gestionar cualquier bucket heredado existente con Compliance.

- ["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#)
- ["Gestiona objetos con ILM"](#)
- ["NetApp base de conocimientos: cómo gestionar los buckets Compliant heredados en StorageGRID 11.5"](#)

Solicitudes de cumplimiento obsoletas:

- ["Obsoleto - modificaciones de la solicitud PUT Bucket para cumplimiento"](#)

El elemento XML «SGCompliance» ha quedado obsoleto. Anteriormente, podías incluir este elemento personalizado de StorageGRID en el cuerpo opcional de la solicitud XML de las peticiones PUT de bucket para crear un bucket conforme.

- ["Obsoleto - GET Bucket compliance"](#)

La solicitud GET Bucket compliance ha quedado obsoleta. Sin embargo, puedes seguir usando esta solicitud para determinar la configuración de cumplimiento que está vigente actualmente para un bucket Compliant heredado existente.

- ["Obsoleto - PUT Bucket compliance"](#)

La solicitud PUT Bucket compliance ha quedado obsoleta. Sin embargo, puedes seguir usando esta solicitud para modificar la configuración de cumplimiento de un bucket Compliant heredado ya existente. Por ejemplo, puedes poner un bucket existente en retención legal o aumentar su periodo de retención.

Elemento SGCompliance obsoleto en StorageGRID

El elemento XML «SGCompliance» ha quedado obsoleto. Antes, podías incluir este elemento personalizado de StorageGRID en el cuerpo opcional de la solicitud XML de las peticiones CreateBucket para crear un bucket Compliant.



La función StorageGRID Compliance, que estaba disponible en versiones anteriores de StorageGRID, ha quedado obsoleta y ha sido sustituida por S3 Object Lock. Consulta lo siguiente para más detalles:

- ["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#)
- ["NetApp base de conocimientos: cómo gestionar los buckets Compliant heredados en StorageGRID 11.5"](#)

Ya no puedes crear nuevos buckets con Compliance activado. El siguiente mensaje de error aparece si intentas usar las modificaciones de la solicitud CreateBucket para compliance y crear un nuevo bucket Compliant:

```
The Compliance feature is deprecated.  
Contact your StorageGRID administrator if you need to create new Compliant  
buckets.
```

Solicitud obsoleta de GET Bucket compliance en StorageGRID

La solicitud GET Bucket compliance ha quedado obsoleta. Sin embargo, puedes seguir usando esta solicitud para determinar la configuración de cumplimiento que está vigente actualmente para un bucket Compliant heredado existente.



La función StorageGRID Compliance, que estaba disponible en versiones anteriores de StorageGRID, ha quedado obsoleta y ha sido sustituida por S3 Object Lock. Consulta lo siguiente para más detalles:

- ["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#)
- ["NetApp base de conocimientos: cómo gestionar los buckets Compliant heredados en StorageGRID 11.5"](#)

Debes tener el permiso s3:GetBucketCompliance o ser root de la cuenta para completar esta operación.

Ejemplo de solicitud

Esta solicitud de ejemplo te permite determinar la configuración de cumplimiento normativo del bucket llamado 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 la configuración de cumplimiento vigente para el bucket. Esta respuesta de ejemplo muestra la configuración de cumplimiento para un bucket en el que cada objeto se conservará durante un año (525,600 minutos), a partir del momento en que el objeto se ingresa en la grid. Actualmente no hay ninguna retención legal en este bucket. 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
RetentionPeriodMinutes	La duración del periodo de retención de los objetos añadidos a este bucket, en minutos. El periodo de retención comienza cuando el objeto se ingiere en el grid.
LegalHold	• Cierto: Este depósito está actualmente sujeto a una retención legal. Los objetos de este depósito no se pueden eliminar hasta que se levante la retención legal, aunque haya vencido su periodo de retención. • Falso: Este bucket no está actualmente bajo una retención legal. Los objetos en este bucket se pueden eliminar cuando expire su periodo de retención.
AutoDelete	• Cierto: Los objetos de este depósito se eliminarán automáticamente cuando expire su periodo de retención, a menos que el depósito esté sujeto a una retención legal. • Falso: Los objetos de este depósito no se eliminarán automáticamente cuando venza el periodo de retención. Debes eliminar estos objetos manualmente si necesitas eliminarlos.

Respuestas de error

Si el bucket no se creó para ser compatible, el código de estado HTTP de la respuesta es 404 Not Found, con un código de error de S3 de `XNoSuchBucketCompliance`.

Solicitud obsoleta de PUT Bucket compliance en StorageGRID

La solicitud PUT Bucket compliance ha quedado obsoleta. Sin embargo, puedes seguir usando esta solicitud para modificar la configuración de cumplimiento de un bucket Compliant heredado ya existente. Por ejemplo, puedes poner un bucket existente en retención legal o aumentar su periodo de retención.



La función StorageGRID Compliance, que estaba disponible en versiones anteriores de StorageGRID, ha quedado obsoleta y ha sido sustituida por S3 Object Lock. Consulta lo siguiente para más detalles:

- ["Utiliza la API de REST de S3 para configurar S3 Object Lock"](#)
- ["NetApp base de conocimientos: cómo gestionar los buckets Compliant heredados en StorageGRID 11.5"](#)

Debes tener el permiso `s3:PutBucketCompliance` o ser root de la cuenta para completar esta operación.

Debes especificar un valor para cada campo de la configuración de cumplimiento al enviar una solicitud PUT Bucket compliance.

Ejemplo de solicitud

Esta solicitud de ejemplo modifica la configuración de cumplimiento del bucket llamado `mybucket`. En este ejemplo, los objetos en `mybucket` ahora se conservarán durante dos años (1,051,200 minutos) en vez de un

año, empezando desde que el objeto se ingresa en el grid. No hay ninguna retención legal en este bucket. 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
RetentionPeriodMinutes	La duración del periodo de retención de los objetos añadidos a este bucket, en minutos. El periodo de retención comienza cuando el objeto se ingiere en el grid. Importante Al especificar un nuevo valor para RetentionPeriodMinutes, debes indicar un valor igual o superior al periodo de retención actual del bucket. Después de que se establezca el periodo de retención del bucket, no puedes disminuir ese valor; solo puedes aumentarlo.
LegalHold	• Cierto: Este depósito está actualmente sujeto a una retención legal. Los objetos de este depósito no se pueden eliminar hasta que se levante la retención legal, aunque haya vencido su periodo de retención. • Falso: Este bucket no está actualmente bajo una retención legal. Los objetos en este bucket se pueden eliminar cuando expire su periodo de retención.
AutoDelete	• Cierto: Los objetos de este depósito se eliminarán automáticamente cuando expire su periodo de retención, a menos que el depósito esté sujeto a una retención legal. • Falso: Los objetos de este depósito no se eliminarán automáticamente cuando venza el periodo de retención. Debes eliminar estos objetos manualmente si necesitas eliminarlos.

Coherencia en la configuración de cumplimiento

Cuando actualizas los ajustes de cumplimiento de un bucket de S3 mediante una solicitud PUT Bucket compliance, StorageGRID intenta actualizar los metadatos del bucket en toda la grid. De forma predeterminada, StorageGRID utiliza la consistencia **Strong-global** para garantizar que todos los data centers y todos los Storage Nodes que contienen metadatos del bucket tengan consistencia de lectura tras escritura para los ajustes de cumplimiento modificados.

Si StorageGRID no puede alcanzar la consistencia **global fuerte** porque un centro de datos o varios nodos de almacenamiento de un mismo centro no están disponibles, el código de estado HTTP de la respuesta es 503 `Service Unavailable`.

Si recibes esta respuesta, debes ponerte en contacto con el administrador de la grid para asegurarte de que los servicios de almacenamiento necesarios estén disponibles lo antes posible. Si el administrador de la grid no puede poner a disposición suficientes Storage Nodes en cada sitio, es posible que soporte técnico te indique que vuelvas a intentar la solicitud fallida forzando la consistencia **Strong-site**.



Nunca impongas la consistencia **Strong-site** para el cumplimiento de PUT bucket, a menos que soporte técnico te lo haya indicado y comprendas las posibles consecuencias de usar este nivel.

Cuando la consistencia se reduce a **Strong-site**, StorageGRID garantiza que los ajustes de cumplimiento actualizados tendrán consistencia de lectura después de escritura solo para las solicitudes de los clientes dentro de un sitio. Esto significa que el sistema StorageGRID podría tener temporalmente múltiples ajustes inconsistentes para este bucket hasta que todos los sitios y nodos de almacenamiento estén disponibles. Las configuraciones inconsistentes pueden dar lugar a un comportamiento inesperado e indeseado. Por ejemplo, si pones un bucket bajo retención legal y fuerzas una consistencia inferior, la configuración de cumplimiento anterior del bucket (es decir, retención legal desactivada) podría seguir vigente en algunos centros de datos. Como resultado, los objetos que crees que están bajo 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**, vuelve a enviar la solicitud de cumplimiento de PUT Bucket e incluye el encabezado de solicitud HTTP `Consistency-Control`, como se indica a continuación:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Respuestas de error

- Si el bucket no se creó para cumplir con los requisitos, el código de estado HTTP de la respuesta es 404 `Not Found`.
- Si `RetentionPeriodMinutes` en la solicitud es menor que el periodo de retención actual del bucket, el código de estado HTTP es 400 `Bad Request`.

Información relacionada

["Obsoleto: modificaciones de la solicitud PUT Bucket para cumplimiento"](#)

Gestiona las políticas de acceso

Cómo StorageGRID usa las políticas de AWS para controlar el acceso a los buckets y objetos de S3

StorageGRID utiliza el lenguaje de políticas de Amazon Web Services (AWS) para permitir a los usuarios de S3 controlar el acceso a los buckets y a los objetos dentro de esos buckets. El sistema StorageGRID implementa un subconjunto del lenguaje de políticas de la API de REST de S3. Las políticas de acceso para la API de S3 se escriben en JSON.

Resumen de la política de acceso

StorageGRID admite tres tipos de políticas de acceso:

- **Políticas de bucket**, que se gestionan mediante las operaciones de la API de S3 GetBucketPolicy, PutBucketPolicy y DeleteBucketPolicy, o bien a través de Tenant Manager o la API de gestión de inquilinos. Las políticas de bucket se asocian a los buckets, por lo que se configuran para controlar el acceso de los usuarios de la cuenta del propietario del bucket o de otras cuentas al bucket y a los objetos que contiene. Una política de bucket se aplica únicamente a un bucket y, posiblemente, a varios grupos.
- **Políticas de grupo**, que se configuran mediante Tenant Manager o Tenant Management API. Las políticas de grupo se asocian a un grupo de la cuenta, por lo que se configuran para permitir que ese grupo acceda a recursos específicos que pertenecen a esa cuenta. Una política de grupo se aplica únicamente a un grupo y posiblemente a varios buckets.
- **Políticas de sesión**, que se incluyen como parte de hacer una solicitud AssumeRole. Las políticas de sesión solo se aplican a la sesión en cuestión y definen con mayor detalle los permisos que tiene el usuario, además de los concedidos por la política de grupo y la política de bucket.



No hay ninguna diferencia de prioridad entre las políticas de grupo, de bucket y de sesión.

Las políticas de bucket y de grupo de StorageGRID siguen una sintaxis específica definida por Amazon. Dentro de cada política hay un arreglo de instrucciones de política, y cada instrucción contiene los siguientes elementos:

- Identificador de declaración (Sid) (opcional)
- Efecto
- Principal/NotPrincipal
- Recurso/NotResource
- Acción/NotAction
- Condición (opcional)

Las declaraciones de políticas se elaboran siguiendo esta estructura para especificar los permisos: conceder <Effect> para permitir o denegar a <Principal> realizar <Action> en <Resource> cuando <Condition> aplica.

Cada elemento de la política se utiliza para una función específica:

Elemento	Descripción
Sid	El elemento Sid es opcional. El Sid solo tiene como finalidad servir de descripción para el usuario. El sistema StorageGRID lo almacena, pero no lo interpreta.
Efecto	Utiliza el elemento Effect para establecer si las operaciones especificadas están permitidas o denegadas. Debes identificar las operaciones que permites (o deniegas) en los buckets u objetos usando las palabras clave admitidas del elemento Action.

Elemento	Descripción
Principal/NotPrincipal	Puedes permitir que usuarios, grupos y cuentas accedan a recursos específicos y realicen acciones específicas. Si la solicitud no incluye ninguna firma S3, se permite el acceso anónimo especificando el carácter comodín (*) como principal. Por defecto, solo la cuenta raíz tiene acceso a los recursos que pertenecen a la cuenta. Solo es necesario especificar el elemento «Principal» en una política de bucket. En el caso de las políticas de grupo, el grupo al que está asociada la política es el elemento «Principal» implícito.
Recurso/NotResource	El elemento «Resource» identifica los buckets y los objetos. Puedes conceder o denegar permisos a los buckets y objetos utilizando el nombre de recurso de Amazon (ARN) para identificar el recurso.
Acción/NotAction	Los elementos «Acción» y «Efecto» son los dos componentes de los permisos. Cuando un grupo solicita un recurso, se le concede o se le deniega el acceso al recurso. El acceso queda denegado a menos que tú asignes permisos de forma específica, pero puedes usar la denegación explícita para anular un permiso concedido por otra política.
Estado	El elemento «Condition» es opcional. Las condiciones te permiten crear expresiones para determinar cuándo debe aplicarse una política.

En el elemento Action, puedes utilizar el carácter comodín (*) para especificar todas las operaciones o un subconjunto de operaciones. Por ejemplo, esta Action coincide con permisos como s3:GetObject, s3:PutObject y s3:DeleteObject.

```
s3:*Object
```

En el elemento «Resource», puedes 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 configurar el acceso anónimo, lo que otorga permiso a todo el mundo. Por ejemplo, si estableces el comodín (*) como el valor de Principal.

```
"Principal": "*"

```

```
"Principal":{"AWS":["*"]}

```

En el siguiente ejemplo, la declaración utiliza los elementos «Effect», «Principal», «Action» y «Resource». Este ejemplo muestra una declaración completa de política de bucket que utiliza el efecto «Allow» para otorgar a los Principals, el admin group `federated-group/admin` y el finance group `federated-group/finance`, permisos para realizar la Action `s3:ListBucket` en el bucket llamado `mybucket` y la Action `s3:GetObject` en todos los objetos dentro de ese bucket.

```
{
  "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 bucket tiene un límite de tamaño de 20,480 bytes, y la política de grupo tiene un límite de tamaño de 5,120 bytes.

Coherencia en las políticas

De forma predeterminada, cualquier actualización que realices en las políticas de grupo es de consistencia eventual. Cuando una política de grupo alcanza la consistencia, los cambios pueden tardar hasta 15 minutos adicionales en surtir efecto debido al almacenamiento en caché de las políticas. De forma predeterminada, cualquier actualización que realices en las políticas de bucket es de consistencia fuerte.

Si es necesario, puedes modificar las garantías de consistencia para las actualizaciones de la política de un bucket. Por ejemplo, es posible que desees que un cambio en la política de un bucket esté disponible durante un fallo energético en el sitio.

En este caso, puedes establecer el encabezado `Consistency-Control` en la solicitud `PutBucketPolicy`, o puedes usar la solicitud `PUT Bucket consistency`. Cuando una política de bucket se vuelve coherente, los cambios pueden tardar 8 segundos adicionales en surtir efecto, debido al almacenamiento en caché de la política.



Si ajustas la consistencia a un valor diferente para solucionar una situación temporal, asegúrate de volver a establecer la configuración a nivel de bucket en su valor original cuando hayas terminado. De lo contrario, todas las futuras solicitudes al bucket usarán la configuración modificada.

¿Qué es la política de sesión?

Una política de sesión es una política de acceso que restringe temporalmente los permisos disponibles durante una sesión concreta, como cuando un usuario asume un grupo. Una política de sesión solo puede permitir un subconjunto de permisos y no puede conceder permisos adicionales. El propio grupo puede tener permisos más amplios.

Usa ARN en las declaraciones de política

En las declaraciones de política, el ARN se usa en los elementos Principal y Resource.

- Utiliza esta sintaxis para especificar el ARN del recurso de S3:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Utiliza 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:

- Puedes utilizar el asterisco (*) como comodín para que coincida con cero o más caracteres dentro de la clave del objeto.
- Los caracteres internacionales, que pueden especificarse en la clave del objeto, deben codificarse utilizando JSON UTF-8 o usando las 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 codificarse con charset=UTF-8.

Especifica recursos en una política

En las declaraciones de política, puedes usar el elemento Resource para especificar el bucket u objeto para el que se permiten o deniegan permisos.

- Cada declaración de política requiere un elemento Resource. En una política, los recursos se indican mediante el elemento Resource, o alternativamente, NotResource para exclusión.
- Especificas los recursos con un ARN de recurso de S3. Por ejemplo:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- También puedes 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 bucket que aún no exista cuando se crea una política de grupo.

Especifica entidades en una política

Utiliza el elemento Principal para identificar la cuenta de usuario, grupo o inquilino a la que la declaración de política permite o deniega el acceso al recurso.

- Cada declaración de política en una política de bucket 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 mediante el elemento «Principal» o, alternativamente, «NotPrincipal» en caso de 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 cuenta root y todos los usuarios de la cuenta:

```
"Principal": { "AWS": "27233906934684427525" }
```

- Puedes especificar únicamente la raíz de la cuenta:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Puedes indicar un usuario federado concreto ("Alex"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
user/Alex" }
```

- Puedes especificar un grupo federado concreto ("Managers"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
group/Managers" }
```

- Puedes especificar un principal anónimo:

```
"Principal": ""
```

- Para evitar ambigüedades, puedes 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 se elimina el nombre de usuario `Alex`. Si un nuevo Alex se incorpora a la organización y se le asigna el mismo `Alex` nombre de usuario, es posible que el nuevo usuario herede involuntariamente los permisos concedidos al usuario original.

- El valor principal puede especificar un nombre de grupo o de usuario que aún no exista en el momento de crear una política de bucket.

Especifica permisos en una política

En una política, el elemento «Action» se utiliza para conceder o denegar permisos sobre un recurso. Existe un conjunto de permisos que se pueden especificar en una política, los cuales se indican mediante el elemento «Action» o, alternativamente, «NotAction» para la exclusión. Cada uno de estos elementos se corresponde con operaciones específicas de la API de REST de S3.

En la tabla se enumeran los permisos que se aplican a los buckets y los permisos que se aplican a los objetos.



Amazon S3 ahora utiliza el permiso `s3:PutReplicationConfiguration` tanto para las acciones `PutBucketReplication` y `DeleteBucketReplication`. StorageGRID utiliza permisos separados para cada acción, lo que coincide con la especificación original de Amazon S3.



Se lleva a cabo una eliminación cuando se utiliza un `put` para sobrescribir un valor existente.

Permisos que se aplican a los buckets

Permisos	Operaciones de la API de REST de S3	Personalizado para StorageGRID
<code>s3:CreateBucket</code>	<code>CreateBucket</code>	Sí. Nota: Utiliza solo en la política de grupo.
<code>s3>DeleteBucket</code>	<code>DeleteBucket</code>	
<code>s3>DeleteBucketMetadataNotification</code>	ELIMINAR configuración de notificaciones de metadatos del bucket	Sí
<code>s3>DeleteBucketPolicy</code>	<code>DeleteBucketPolicy</code>	

Permisos	Operaciones de la API de REST de S3	Personalizado para StorageGRID
s3:DeleteReplicationConfiguration	DeleteBucketReplication	Sí, permisos distintos para PUT y DELETE
s3:GetBucketAcl	GetBucketAcl	
s3:GetBucketCompliance	GET Bucket compliance (obsoleto)	Sí
s3:GetBucketConsistency	Obtener la consistencia del Bucket	Sí
s3:GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	Obtener el tiempo de último acceso al Bucket	Sí
s3:GetBucketLocation	GetBucketLocation	
s3:GetBucketMetadataNotification	Obtener configuración de notificaciones de metadatos del bucket	Sí
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	
s3:ListAllMyBuckets	- ListBuckets - Obtener uso del almacenamiento	Sí, para GET Storage Usage. Nota: Utiliza solo en la política de grupo.

Permisos	Operaciones de la API de REST de S3	Personalizado para StorageGRID
s3:ListBucket	- ListObjects - HeadBucket - RestoreObject	
s3:ListBucketMultipartUploads	- ListMultipartUploads - RestoreObject	
s3:ListBucketVersions	Obtener versiones de bucket	
s3:PutBucketCompliance	PUT Bucket compliance (obsoleto)	Sí
s3:PutBucketConsistency	Consistencia de PUT Bucket	Sí
s3:PutBucketCORS	- DeleteBucketCors† - PutBucketCors	
s3:PutEncryptionConfiguration	- DeleteBucketEncryption - PutBucketEncryption	
s3:PutBucketLastAccessTime	PUT Bucket tiempo de acceso más reciente	Sí
s3:PutBucketMetadataNotification	PUT Bucket configuración de notificación de metadatos	Sí
s3:PutBucketNotification	PutBucketNotificationConfiguration	
s3:PutBucketObjectLockConfiguration	- CreateBucket con el encabezado de solicitud <code>x-amz-bucket-object-lock-enabled: true</code> (también requiere el permiso <code>s3:CreateBucket</code>) - PutObjectLockConfiguration	
s3:PutBucketPolicy	PutBucketPolicy	
s3:PutBucketTagging	- DeleteBucketTagging† - PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	

Permisos	Operaciones de la API de REST de S3	Personalizado para StorageGRID
s3:PutLifecycleConfiguration	- DeleteBucketLifecycle† - PutBucketLifecycleConfiguration	
s3:PutReplicationConfiguration	PutBucketReplication	Sí, permisos distintos para PUT y DELETE

Permisos que se aplican a los objetos

Permisos	Operaciones de la API de REST de S3	Personalizado para StorageGRID
s3:AbortMultipartUpload	- AbortMultipartUpload - RestoreObject	
s3:BypassGovernanceRetention	- DeleteObject - DeleteObjects - PutObjectRetention	
s3>DeleteObject	- DeleteObject - DeleteObjects - RestoreObject	
s3>DeleteObjectTagging	DeleteObjectTagging	
s3>DeleteObjectVersionTagging	DeleteObjectTagging (una versión específica del objeto)	
s3>DeleteObjectVersion	DeleteObject (una versión concreta del objeto)	
s3:GetObject	- GetObject - HeadObject - RestoreObject - SelectObjectContent	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	

Permisos	Operaciones de la API de REST de S3	Personalizado para StorageGRID
s3:GetObjectTagging	GetObjectTagging	
s3:GetObjectVersionTagging	GetObjectTagging (una versión concreta del objeto)	
s3:GetObjectVersion	GetObject (una versión concreta del objeto)	
s3:ListMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	• PutObject • CopyObject • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (una versión concreta del objeto)	
s3:PutOverwriteObject	• PutObject • CopyObject • PutObjectTagging • DeleteObjectTagging • CompleteMultipartUpload	Sí
s3:RestoreObject	RestoreObject	

Usa el permiso PutOverwriteObject

El permiso s3:PutOverwriteObject es un permiso personalizado de StorageGRID 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 las etiquetas de los 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 ya existente en la misma ruta:
 - No se pueden sobrescribir los datos del objeto, los metadatos definidos por el usuario ni las etiquetas del objeto S3.
 - Se cancelan todas las operaciones de ingesta que estén en curso y se devuelve un error.
 - Si el control de versiones de S3 está habilitado, la configuración Deny impide que las operaciones PutObjectTagging o DeleteObjectTagging modifiquen el TagSet de un objeto y sus versiones no vigentes.
 - Si no se encuentra un objeto existente, este permiso no tiene ningún efecto.
- Cuando no se dispone de este permiso, el efecto es el mismo que si Allow estuviera activado.



Si la política de S3 actual permite la sobrescritura y el permiso PutOverwriteObject está establecido en Deny, el cliente no puede sobrescribir los datos de un objeto, los metadatos definidos por el usuario ni las etiquetas del objeto. Además, si la casilla de verificación **Evitar la modificación del cliente** está seleccionada (**Configuración > Configuración de seguridad > Red y objetos**), esa configuración anula la configuración del permiso PutOverwriteObject.

Especifica las condiciones en una directiva

Las condiciones definen cuándo estará vigente una política. Las condiciones se componen de operadores y pares clave-valor.

Las condiciones usan pares clave-valor para la evaluación. Un elemento Condition puede contener varias condiciones, y cada condición puede contener varios pares clave-valor. El bloque de condiciones usa el siguiente formato:

```
Condition: {
  condition_type: {
    condition_key: condition_values
```

En el siguiente ejemplo, la condición IpAddress utiliza la clave de condición SourceIp.

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
```

Operadores de condición admitidos

Los operadores de condición se clasifican de la siguiente manera:

- Cadena

- Numérico
- Booleano
- Dirección IP
- Comprobación de valores nulos

Operadores condicionales	Descripción
StringEquals	Compara una clave con un valor de cadena basándose en la coincidencia exacta (distingue mayúsculas de minúsculas).
StringNotEquals	Compara una clave con un valor de cadena según una coincidencia negada (distingue mayúsculas de minúsculas).
StringEqualsIgnoreCase	Compara una clave con un valor de cadena basándose en la coincidencia exacta (ignora mayúsculas y minúsculas).
StringNotEqualsIgnoreCase	Compara una clave con un valor de cadena basándose en la coincidencia negada (ignora mayúsculas y minúsculas).
StringLike	Compara una clave con un valor de cadena basándose en una coincidencia exacta (distingue mayúsculas de minúsculas). Puede incluir los caracteres comodín * y ?.
StringNotLike	Compara una clave con un valor de cadena según una coincidencia negada (distingue mayúsculas de minúsculas). Puede incluir los caracteres comodín * y ?.
NumericEquals	Compara una clave con un valor numérico basándose en una coincidencia exacta.
NumericNotEquals	Compara una clave con un valor numérico basándose en una coincidencia negada.
NumericGreaterThan	Compara una clave con un valor numérico basándose en la condición "mayor que".
NumericGreaterThanEquals	Compara una clave con un valor numérico basándose en la condición "mayor o igual que".
NumericLessThan	Compara una clave con un valor numérico basándose en la condición "menor que".
NumericLessThanEquals	Compara una clave con un valor numérico basándose en "menor o igual que".
Bool	Compara una clave con un valor booleano basándose en la coincidencia "verdadero o falso".

Operadores condicionales	Descripción
IpAddress	Compara una clave con una dirección IP o un rango de direcciones IP.
NotIpAddress	Compara una clave con una dirección IP o un rango de direcciones IP basándose en la coincidencia negada.
Nulo	Comprueba si existe una clave de condición en el contexto de la solicitud actual.
IfExists	Se añade a cualquier operador de condición, excepto a la condición Null, para comprobar la ausencia de esa clave de condición. Devuelve TRUE si la clave de condición no está presente.

Claves de condición admitidas

Claves de condición	Acciones	Descripción
aws:SourceIp	Operadores de IP	Se comparará con la dirección IP desde la que se envió la solicitud. Se puede usar para operaciones de bucket o de objeto. Nota: Si la solicitud S3 se envió a través del servicio de Load Balancer en los nodos de Admin y los nodos de Gateway, esto se comparará con la dirección IP situada aguas arriba del servicio de Load Balancer. Nota: Si se utiliza un equilibrador de carga de terceros no transparente, se realizará la comparación con la dirección IP de ese equilibrador de carga. Cualquier encabezado X-Forwarded-For se ignorará porque no se puede verificar su validez.
aws:username	Recurso/Identidad	Se comparará con el nombre de usuario del remitente desde el que se envió la solicitud. Se puede utilizar para operaciones con buckets u objetos.
s3:delimiter	s3:ListBucket y Permisos de s3:ListBucketVersions	Se comparará con el parámetro delimitador especificado en una solicitud de ListObjects o ListObjectVersions.

Claves de condición	Acciones	Descripción
s3:ExistingObjectTag/<tag-key>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl 3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging s3:PutObjectAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Exigirá que el objeto existente tenga la clave y el valor específicos de la etiqueta.
s3:max-keys	s3:ListBucket y Permisos de s3:ListBucketVersions	Se comparará con el parámetro max-keys especificado en una solicitud ListObjects o ListObjectVersions.
s3:object-lock-mode	s3:PutObject	Se compara con el object-lock-mode expandido a partir de la cabecera de la solicitud en la solicitud PutObject, CopyObject y CreateMultipartUpload.
s3:object-lock-mode	s3:PutObjectRetention	Se compara con el object-lock-mode expandido desde el cuerpo XML en la solicitud PutObjectRetention.
s3:object-lock-remaining-retention-days	s3:PutObject	Compara con la fecha de retención especificada en el encabezado de solicitud x-amz-object-lock-retain-until-date o calculada a partir del periodo de retención predeterminado del bucket para asegurarse de que estos valores estén dentro del rango permitido para las siguientes solicitudes: • PutObject • CopyObject • CreateMultipartUpload

Claves de condición	Acciones	Descripción
s3:object-lock-remaining-retention-days	s3:PutObjectRetention	Lo compara con la fecha de retención especificada en la solicitud PutObjectRetention para asegurarse de que esté dentro del intervalo permitido.
s3:prefijo	s3:ListBucket y Permisos de s3:ListBucketVersions	Se comparará con el parámetro de prefijo especificado en una solicitud ListObjects o ListObjectVersions.
s3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Requerirá una clave y un valor de etiqueta específicos cuando la solicitud del objeto incluya el etiquetado.
s3:x-amz-server-side-encryption-customer-algorithm	s3:PutObject	Se compara con el sse-customer-algorithm o con el copy-source-sse-customer-algorithm expandido desde el encabezado de la solicitud en PutObject, CopyObject, CreateMultipartUpload, UploadPart, UploadPartCopy y CompleteMultipartUpload.

Especifica variables en una política

Puedes usar variables en las políticas para completar la información de la política cuando esté disponible. Puedes usar variables de política en el elemento `Resource` y en comparaciones de cadenas en el elemento `Condition`.

En este ejemplo, la variable `${aws:username}` forma parte del elemento «Resource»:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

En este ejemplo, la variable `${aws:username}` es parte del valor de la condición en el bloque de condiciones:

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```

Variable	Descripción
<code>\${aws:SourceIp}</code>	Utiliza la clave SourceIp como la variable proporcionada.
<code>\${aws:username}</code>	Utiliza la clave username como variable proporcionada.
<code>\${s3:prefix}</code>	Utiliza la clave de prefijo específica del servicio como 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. Usa el carácter como un carácter ? literal.
<code>\${\$}</code>	Carácter especial. Usa el carácter como un carácter \$ literal.

Crea políticas que requieran un manejo especial

A veces, una política puede conceder permisos que son peligrosos para la seguridad o para la continuidad de las operaciones, como bloquear al usuario raíz de la cuenta. La implementación de la API de REST de S3 de StorageGRID es menos restrictiva durante la validación de políticas que Amazon, pero igual de estricta durante la evaluación de políticas.

Descripción de la política	Tipo de política	Comportamiento de Amazon	Comportamiento de StorageGRID
Negarte cualquier permiso para la cuenta de root	Bucket	Válida y aplicada, pero el usuario raíz conserva el permiso para todas las operaciones de políticas de bucket de S3	Lo mismo
Negar a uno mismo cualquier permiso para el usuario/grupo	Grupo	Válido y aplicable	Lo mismo
Permitir a un grupo de cuentas extranjeras cualquier permiso	Bucket	Principal no válido	Válido, pero los permisos para todas las operaciones de políticas de buckets S3 devuelven un error 405 Method Not Allowed cuando están permitidas por una política

Descripción de la política	Tipo de política	Comportamiento de Amazon	Comportamiento de StorageGRID
Permitir que un usuario raíz o usuario de una cuenta externa tenga cualquier permiso	Bucket	Válido, pero los permisos para todas las operaciones de políticas de buckets S3 devuelven un error 405 Method Not Allowed cuando están permitidas por una política	Lo mismo
Conceder a todos permisos para todas las acciones	Bucket	Es válido, pero los permisos para todas las operaciones de políticas de buckets de S3 devuelven un error 405 Method Not Allowed para el usuario raíz y los usuarios de la cuenta externa.	Lo mismo
Denegar a todos los usuarios los permisos para todas las acciones	Bucket	Válida y aplicada, pero el usuario raíz conserva el permiso para todas las operaciones de políticas de bucket de S3	Lo mismo
Principal es un usuario o grupo que no existe	Bucket	Principal no válido	Válido
El recurso es un bucket de S3 que no existe	Grupo	Válido	Lo mismo
Principal es un grupo local	Bucket	Principal no válido	Válido
La política concede a una cuenta que no es propietaria (incluidas las cuentas anónimas) permisos para poner objetos.	Bucket	Válido. Los objetos son propiedad de la cuenta del creador y la política de bucket no se aplica. La cuenta del creador debe conceder permisos de acceso al objeto mediante ACL de objeto.	Válido. Los objetos son propiedad de la cuenta del propietario del bucket. Se aplica la política del bucket.

Protección de escritura única y lectura múltiple (WORM)

Puedes crear buckets WORM (write-once-read-many) para proteger los datos, los metadatos de objetos definidos por el usuario y el etiquetado de objetos de S3. Configura los buckets WORM para permitir la creación de objetos nuevos y evitar la sobrescritura o eliminación del contenido existente. Utiliza uno de los enfoques descritos aquí.

Para asegurarte de que las sobrescrituras siempre se rechacen, puedes:

- Desde el Grid Manager, ve a **Configuration > Security > Security settings > Network and objects**, y

selecciona la casilla **Prevent client modification**.

- Aplica las siguientes reglas y políticas de S3:
 - Añade una operación DENY de PutOverwriteObject a la política de S3.
 - Agrega una operación DENY de DeleteObject a la política de S3.
 - Añade una operación ALLOW de PutObject a la directiva de S3.



Establecer DeleteObject en DENY en una política de S3 no impide que ILM elimine objetos cuando existe una regla como "cero copias después de 30 días".



Incluso cuando aplicas todas estas reglas y políticas, no protegen contra las escrituras simultáneas (ver Situación A). Sí protegen contra las sobrescrituras secuenciales completadas (ver Situación B).

Situación A: Escrituras simultáneas (sin protección)

```
/mybucket/important.doc  
PUT#1 ---> OK  
PUT#2 -----> OK
```

Situación B: Sobrescrituras secuenciales completadas (protegidas)

```
/mybucket/important.doc  
PUT#1 -----> PUT#2 ---X (denied)
```

Información relacionada

- ["Cómo gestionan los objetos las reglas de ILM de StorageGRID"](#)
- ["Ejemplos de políticas de bucket"](#)
- ["Ejemplos de políticas de grupo"](#)
- ["Ejemplo de política de sesión"](#)
- ["Gestiona objetos con ILM"](#)
- ["Utiliza una cuenta de inquilino"](#)

Ejemplo de política de sesión de StorageGRID S3 API de REST

Utiliza el siguiente ejemplo para crear una política de sesión de StorageGRID.

Ejemplo: configurar una política de sesión que permita la recuperación de objetos

En este ejemplo, el principal de la sesión solo tiene permiso para recuperar objetos de bucket1. Todas las demás acciones están implícitamente denegadas, excepto las acciones específicas de StorageGRID, como usar el permiso ["s3:PutOverwriteObject"](#). La política de sesión puede proporcionarse como un archivo JSON al llamar a la API AssumeRole.

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket1/*"
    }
  ]
}
```

Ejemplos de políticas de bucket de la API de REST de StorageGRID S3

Utiliza los ejemplos de esta sección para crear políticas de acceso de StorageGRID para los buckets.

Las políticas de bucket especifican los permisos de acceso para el bucket al que está asociada la política. Configuras una política de bucket usando la API de S3 PutBucketPolicy a través de una de estas herramientas:

- ["Administrador de inquilinos"](#).
- AWS CLI con este comando (consulta ["Operaciones en cubos"](#)):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Ejemplo: permitir a todos acceso de solo lectura a un bucket

En este ejemplo, todos, incluidos los anónimos, pueden listar objetos en el bucket y realizar operaciones GetObject en todos los objetos del bucket. Todas las demás operaciones serán denegadas. Ten en cuenta que esta política podría no ser especialmente útil porque nadie excepto el usuario raíz de la cuenta tiene permisos para escribir en el bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ]
    }
  ]
}
```

Ejemplo: concede acceso completo a todos los usuarios de una cuenta y acceso de solo lectura a todos los usuarios de otra cuenta a un bucket

En este ejemplo, todos en una cuenta especificada tienen acceso completo a un bucket, mientras que todos en otra cuenta especificada solo pueden listar el bucket y realizar operaciones `GetObject` en los objetos del bucket que comiencen con el prefijo de clave de objeto `shared/`.



En StorageGRID, los objetos creados por una cuenta que no sea la del propietario (incluidas las cuentas anónimas) son propiedad de la cuenta del propietario del bucket. La política del 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: conceder a todos acceso de solo lectura a un bucket y acceso completo a un grupo específico

En este ejemplo, todos, incluidos los anónimos, pueden listar el bucket y realizar operaciones GetObject en todos los objetos del bucket, mientras que solo los usuarios que pertenecen al grupo Marketing en la cuenta especificada tienen 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 acceso de lectura y escritura a un bucket si el cliente se encuentra en un rango de direcciones IP

En este ejemplo, se permite a todo el mundo, incluidos los usuarios anónimos, consultar el contenido del bucket y realizar cualquier operación sobre todos los objetos del mismo, siempre que las solicitudes procedan de un rango de direcciones IP específico (de 54.240.143.0 a 54.240.143.255, excepto 54.240.143.188). El resto de operaciones serán denegadas, y todas las solicitudes fuera de ese rango de direcciones IP serán denegadas.


```

{
  "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 al bucket `examplebucket` y a sus objetos. A todos los demás usuarios, incluido `'root'`, se les deniegan explícitamente todas las operaciones. Sin embargo, ten en cuenta que a `'root'` nunca se le deniegan 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` efecto de `PutOverwriteObject` y `DeleteObject` garantiza que nadie pueda sobrescribir ni eliminar los datos del objeto, los metadatos definidos por el usuario ni las etiquetas del objeto 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/*"
    }
  ]
}

```

Ejemplos de políticas de grupo de la API de REST de StorageGRID S3

Utiliza los ejemplos de esta sección para crear políticas de acceso a StorageGRID para grupos.

Las políticas de grupo especifican los permisos de acceso para el grupo al que está asociada la política. No hay ningún **Principal** elemento en la política porque es implícito. Las políticas de grupo se configuran usando Tenant Manager o la API.

Ejemplo: configurar la política de grupo mediante Tenant Manager

Al añadir o editar un grupo en Tenant Manager, puedes seleccionar una política de grupo para determinar qué permisos de acceso a S3 tendrán los miembros de este grupo. Consulta ["Crear grupos para un inquilino de S3"](#).

- **Sin acceso a S3:** opción predeterminada. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que se les conceda acceso mediante una política de bucket. Si seleccionas esta opción, solo el usuario raíz 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 listar objetos y leer los datos de los objetos, metadatos y etiquetas. Cuando seleccionas 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 seleccionas esta opción, aparece en el cuadro de texto la cadena JSON para una política de grupo de acceso completo. No puedes editar esta cadena.
- **Mitigación del ransomware:** Esta política de ejemplo se aplica a todos los buckets de este tenant. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden eliminar de forma permanente objetos de los buckets que tengan habilitado el versionado de objetos.

Los usuarios de Tenant Manager que tengan el permiso de Manage all buckets pueden anular esta política de grupo. Limita el permiso de Manage all buckets a usuarios de confianza y usa la autenticación multifactor (MFA) donde esté disponible.

- **Personalizado:** Los usuarios del grupo reciben los permisos que especifiques en el cuadro de texto.

Ejemplo: conceder al grupo acceso completo a todos los buckets

En este ejemplo, todos los miembros del grupo tienen acceso completo a todos los buckets propiedad de la cuenta del inquilino, salvo que la política del bucket lo deniegue explícitamente.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Ejemplo: permitir el acceso de solo lectura a todos los buckets para un grupo

En este ejemplo, todos los miembros del grupo tienen acceso de solo lectura a los recursos de S3, salvo que la política del bucket lo deniegue explícitamente. Por ejemplo, los usuarios de este grupo pueden listar objetos y leer los datos, metadatos y etiquetas de los objetos.

```

{
  "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» dentro de un bucket

En este ejemplo, los miembros del grupo solo pueden listar y acceder a su carpeta específica (prefijo de clave) en el bucket indicado. Ten en cuenta que, a la hora de determinar la privacidad de estas carpetas, deben tenerse en cuenta los permisos de acceso de otras políticas de grupo y de la política del bucket.

```
{
  "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 S3 registradas en los registros de auditoría de StorageGRID

Los servicios de StorageGRID generan mensajes de auditoría que se almacenan en archivos de registro de texto. Puedes revisar los mensajes de auditoría específicos de S3 en el registro de auditoría para obtener detalles sobre las operaciones en los buckets y los objetos.

Operaciones con buckets registradas en los registros de auditoría

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- DeleteObjects
- GetBucketTagging
- HeadBucket
- ListObjects
- ListObjectVersions
- Cumplimiento de PUT Bucket
- PutBucketTagging
- PutBucketVersioning

Operaciones con objetos registradas en los registros de auditoría

- CompleteMultipartUpload
- CopyObject
- DeleteObject
- GetObject
- HeadObject
- PutObject
- RestoreObject
- SelectObject
- UploadPart (cuando una regla de ILM utiliza Balanced o Strict ingest)
- UploadPartCopy (cuando una regla de ILM utiliza la ingesta equilibrada o estricta)

Información relacionada

- ["Acceder al archivo de registro de auditoría"](#)
- ["Mensajes de auditoría de escritura del cliente"](#)
- ["Mensajes de auditoría de lectura del cliente"](#)

Usa la API de REST de Swift (fin de vida útil)

Compatibilidad con la API de REST de Swift en StorageGRID

El soporte para la API de Swift ha llegado al final de su ciclo de vida y se eliminará en una futura versión.



Hemos eliminado los detalles de Swift de esta versión del sitio de documentación. Consulta ["StorageGRID 11.8: usa la API de REST de Swift"](#).

Supervisar y solucionar problemas en un sistema StorageGRID

Supervisa el sistema StorageGRID

Supervisa un sistema StorageGRID

Supervisa tu sistema StorageGRID con regularidad para asegurarte de que funciona según lo previsto.

Antes de empezar

- Has 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 Grid Manager, selecciona el menú desplegable de usuario en la esquina superior derecha del Grid Manager y luego selecciona **User preferences**.

Acerca de esta tarea

Estas instrucciones describen cómo:

- ["Ver y gestionar el panel de control"](#)
- ["Ver la página Nodes"](#)
- ["Supervisa estos aspectos del sistema con regularidad:"](#)
 - ["Estado del sistema"](#)
 - ["Capacidad de almacenamiento"](#)
 - ["Gestión del ciclo de vida de la información"](#)
 - ["Redes y recursos del sistema"](#)
 - ["Actividad del inquilino"](#)
 - ["Operaciones de equilibrio de carga"](#)
 - ["Conexiones de grid federation"](#)
- ["Gestiona alertas"](#)
- ["Ver archivos de registro"](#)
- ["Configura la gestión de registros y el servidor syslog externo"](#)
- ["Utiliza un servidor syslog externo"](#) para recopilar información de auditoría
- ["Utiliza SNMP para la supervisión"](#)
- ["Modificar la priorización de E/S"](#) para modificar las prioridades relativas de las operaciones de E/S

Ver y gestionar el panel de control en StorageGRID

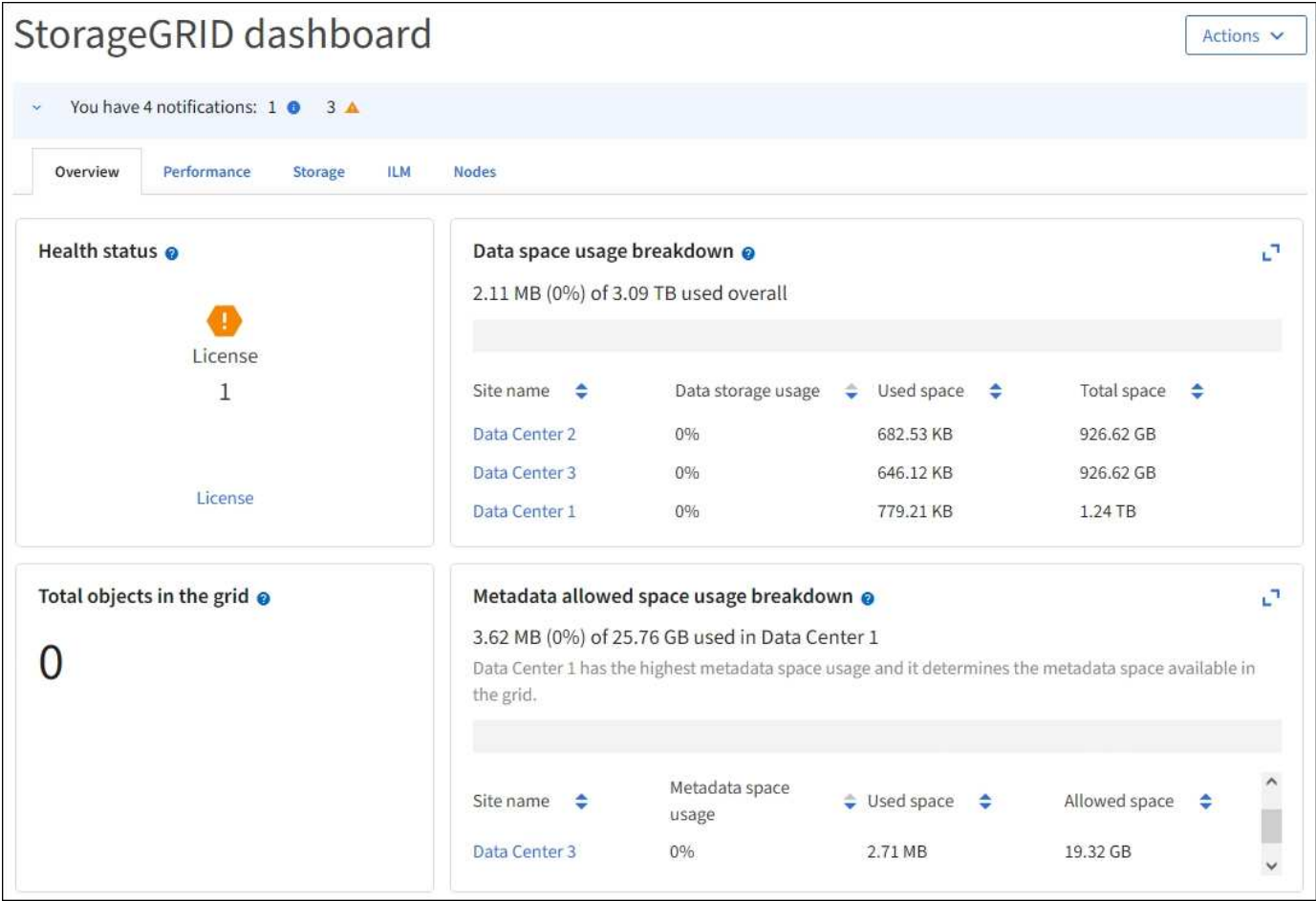
Puedes utilizar el panel de control para supervisar las actividades del sistema de un solo vistazo. Puedes crear paneles de control personalizados para supervisar tu

implementación de StorageGRID.



Para cambiar las unidades de los valores de almacenamiento que se muestran en el Grid Manager, selecciona el menú desplegable de usuario en la esquina superior derecha del Grid Manager y luego selecciona **User preferences**.

Tu panel de control puede variar en función de 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 tarjetas.

Puedes utilizar el panel de control que proporciona el sistema tal cual. Además, puedes crear paneles de control personalizados que contengan únicamente las pestañas y las fichas relevantes para supervisar tu implementación de StorageGRID.

Las pestañas del panel de control que ofrece 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 las alertas activas, el uso del espacio y el número total de objetos en la cuadrícula.
Rendimiento	Uso del espacio, almacenamiento utilizado a lo largo del tiempo, operaciones S3, duración de las solicitudes, tasa de errores.
Almacenamiento	Uso de la cuota de inquilino y uso del espacio lógico. Previsiones sobre el uso del espacio para los datos de usuario y los metadatos.
ILM	Cola de gestión del ciclo de vida de la información y tasa de evaluación.
Nodos	Uso de la CPU, los datos y la memoria por nodo. Operaciones de S3 por nodo. Distribución de nodo a sitio.

Algunas de las tarjetas se pueden maximizar para facilitar su visualización. Selecciona el icono de maximizar  en la esquina superior derecha de la tarjeta. Para cerrar una tarjeta maximizada, selecciona el icono de minimizar  o selecciona **Close**.

Gestiona paneles de control

Si tienes acceso Root (consulta "[Permisos del grupo de administradores](#)"), puedes realizar las siguientes tareas de gestión para los paneles:

- Crea un panel de control personalizado desde cero. Puedes utilizar los paneles de control personalizados para controlar qué información de StorageGRID se muestra y cómo se organiza dicha información.
- Clona un dashboard para crear dashboards personalizados.
- Establece un panel de control activo para un usuario. El panel de control activo puede ser el que proporciona el sistema o uno personalizado.
- Establece un panel de control predeterminado, que es lo que ven todos los usuarios a menos que activen su propio panel de control.
- Edita el nombre de un panel de control.
- Edita un panel para añadir o eliminar pestañas y tarjetas. Puedes tener un mínimo de 1 y un máximo de 20 pestañas.
- Eliminar un panel de control.



Si tienes cualquier otro permiso además del acceso Root, solo puedes establecer un panel activo.

Para gestionar los paneles, selecciona **Actions > Manage dashboards**.



Configura paneles de control

Para crear un nuevo panel de control clonando el panel de control activo, selecciona **Actions > Clone active dashboard**.

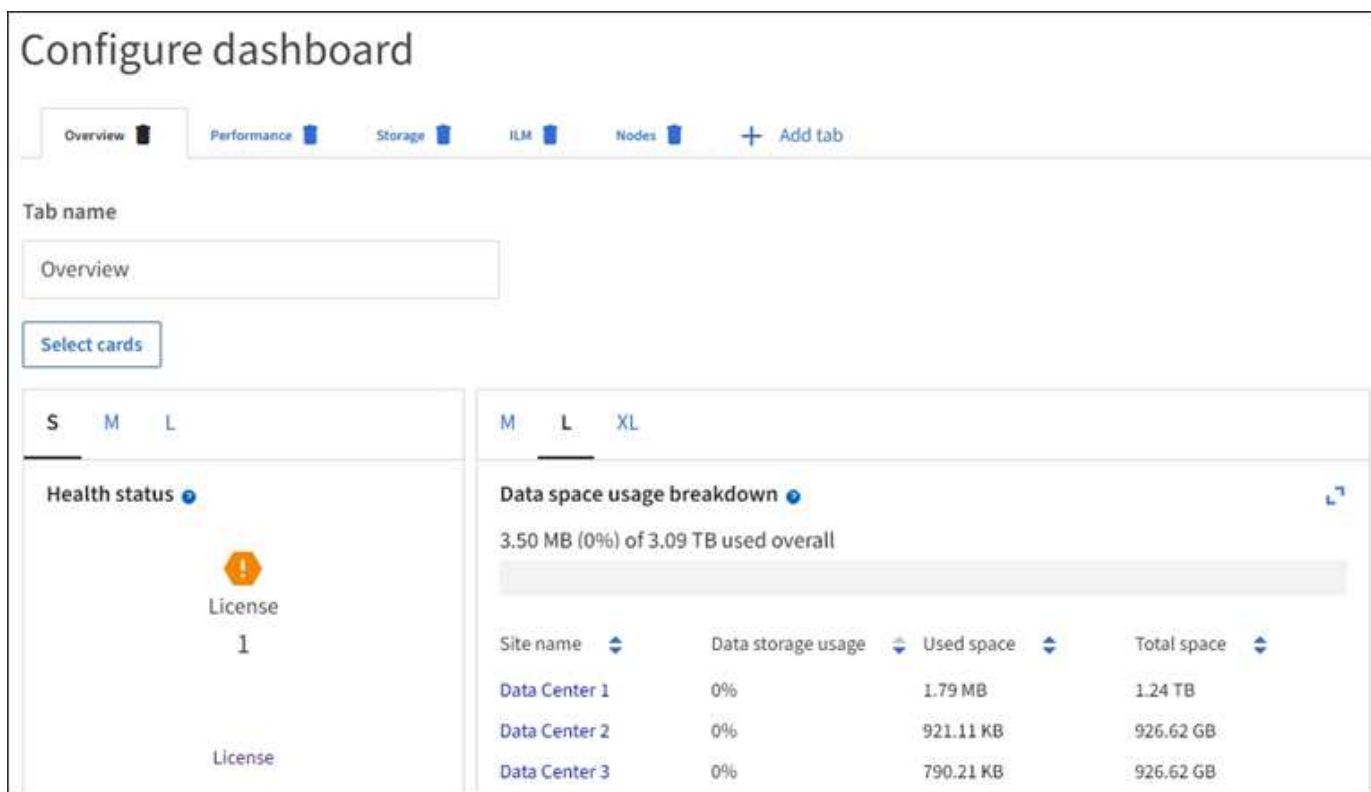
Para editar o clonar un dashboard ya existente, selecciona **Actions > Manage dashboards**.



El panel de control que proporciona el sistema no se puede editar ni eliminar.

Al configurar un panel de control, puedes:

- Agregar o quitar pestañas
- Cambiar el nombre de las pestañas y asignar nombres únicos a las nuevas pestañas
- Añade, elimina o reorganiza (arrastra) las fichas de cada pestaña
- Selecciona el tamaño de cada tarjeta eligiendo **S**, **M**, **L** o **XL** en la parte superior de la tarjeta



Ver la página Nodes

Ver la página de nodos de StorageGRID

Si necesitas información más detallada sobre tu sistema StorageGRID de la que ofrece

el panel de control, puedes usar la página Nodos para ver las métricas de toda la grid, de cada sitio en la grid y de cada nodo en un sitio.

La tabla «Nodos» muestra información resumida sobre toda la grid, cada sitio y cada nodo. Si un nodo está desconectado o tiene una alerta activa, aparece un icono junto al nombre de nodo. Si el nodo está conectado y no tiene alertas activas, no se muestra ningún icono.



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



Para cambiar las unidades de los valores de almacenamiento que se muestran en el Grid Manager, selecciona el menú desplegable de usuario en la esquina superior derecha del Grid Manager y luego selecciona **User preferences**.



Las capturas de pantalla que se muestran son ejemplos. Tus resultados pueden variar en función de tu 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 grid, aparecerá cualquiera de los siguientes iconos junto al nombre de nodo.

Icono	Descripción	Acción requerida
	Sin conexión - Desconocido Por alguna razón desconocida, un nodo se ha desconectado o los servicios de dicho nodo han dejado de funcionar de forma inesperada. Por ejemplo, es posible que un servicio del nodo se haya detenido o que el nodo haya perdido la conexión a la red debido a un corte de corriente o a una interrupción inesperada. También podría activarse la alerta Unable to communicate with node. Es posible que también haya otras alertas activas.	Requiere atención inmediata. "Selecciona cada alerta" y sigue las acciones recomendadas. Por ejemplo, es posible que tengas que reiniciar un servicio que se haya detenido o reiniciar el host para el nodo. Nota: Es posible que un nodo aparezca como «Desconocido» durante las operaciones de apagado controlado. En estos casos, puedes ignorar el estado «Desconocido».
	Sin conexión - Fuera de servicio por motivos administrativos Por una razón previsible, el nodo no está conectado a la grid. Por ejemplo, el nodo, o los servicios en el nodo, se ha apagado de forma controlada, el nodo se está reiniciando o el software se está actualizando. También puede haber una o más alertas activas. Dependiendo del problema subyacente, estos nodos suelen volver a estar en línea sin intervención.	Comprueba si hay alguna alerta que afecte a este nodo. Si hay una o varias alertas activas, "Selecciona cada alerta" y sigue las medidas recomendadas.

Si un nodo se desconecta de la red, es posible que tenga una alerta subyacente, pero solo aparecerá el icono «No conectado». Para ver las alertas activas de un nodo, selecciona el nodo.

Iconos de alerta

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

 **Crítico:** Existe una condición anómala que ha detenido las operaciones normales de un nodo o servicio de StorageGRID. Debes solucionar el problema subyacente de inmediato. Si no resuelves el problema, podría haber interrupciones en el servicio y pérdida de datos.

 **Grave:** Existe una situación anómala que está afectando al funcionamiento actual o que se está acercando al umbral de una alerta crítica. Deberías investigar las alertas graves y resolver cualquier problema subyacente para asegurarte de que la situación anómala no detenga el funcionamiento normal de un nodo o servicio de StorageGRID.

 **Menor:** El sistema funciona con normalidad, pero existe una situación anómala que, si continúa, podría afectar la capacidad del sistema para operar. Deberías supervisar y resolver las alertas menores que no se resuelvan por sí solas para asegurarte de que no resulten en un problema más grave.

Ver detalles de un sistema, un sitio o un nodo

Para filtrar la información que se muestra en la tabla Nodos, introduce una cadena de búsqueda en el campo **Buscar**. Puedes buscar por nombre del sistema, nombre para mostrar o tipo (por ejemplo, introduce **gat** para localizar rápidamente todos los Gateway Nodes).

Para consultar la información sobre la grid, el sitio o el nodo:

- Selecciona el nombre de la grid para ver un resumen agregado de las estadísticas de todo tu sistema StorageGRID.
- Selecciona una ubicación concreta del centro de datos para ver un resumen global de las estadísticas de todos los nodos de esa ubicación.
- Selecciona un nodo concreto para ver la información detallada de ese nodo.

Ver la pestaña Overview de StorageGRID

La pestaña «Descripción general» ofrece información básica sobre cada nodo. También muestra las alertas que afectan actualmente al nodo.

La pestaña «Resumen» se muestra para todos los nodos.

Información del nodo

La sección «Información del nodo» de la pestaña «Resumen» muestra información básica sobre el nodo.

NYC-ADM1 (Primary Admin Node) [🔗](#)

Overview

Hardware

Network

Storage

Load balancer

Tasks

Node information [?](#)

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

Show additional IP addresses [▼](#)

La información general de un nodo incluye lo siguiente:

- **Nombre de visualización** (solo se muestra si se ha cambiado el nombre del nodo): el nombre de visualización actual del nodo. Usa el procedimiento "[Cambiar el nombre de la grid, los sitios y los nodos](#)" para actualizar este valor.
- **Nombre del sistema**: El nombre que introdujiste para el nodo durante la instalación. Los nombres de los sistemas 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, que también se conoce como UUID.
- **Estado de la conexión**: Uno de tres estados. El icono para el estado más grave se muestra.

- **Desconocido** : Por una razón desconocida, el nodo no está conectado a la red o uno o más servicios están inactivos de forma inesperada. Por ejemplo, se ha perdido la conexión de red entre los nodos, hay un corte de corriente o un servicio está inactivo. También podría activarse la alerta **Unable to communicate with node**. Es posible que haya otras alertas activas. Esta situación requiere atención inmediata.



Un nodo puede aparecer como «Desconocido» durante las operaciones de apagado controlado. En estos casos, puedes ignorar el estado «Desconocido».

- **Fuera de servicio por motivos administrativos** : el nodo no está conectado a la grid por un motivo previsto. Por ejemplo, el nodo, o los servicios en el nodo, se ha apagado de forma controlada, el nodo se está reiniciando o el software se está actualizando. También puede haber una o más alertas activas.

- **Conectado** : el nodo está conectado a la red.

- **Espacio de almacenamiento utilizado**: solo para nodos de almacenamiento.
 - **Datos de objetos**: el porcentaje del espacio total utilizable para datos de objetos que se ha utilizado en el Storage Node.
 - **Metadatos de objetos**: El porcentaje del espacio total permitido para metadatos de objetos que se ha utilizado en el nodo de almacenamiento.
- **Versión del software**: La versión de StorageGRID que está instalada en el nodo.
- **Grupos de alta disponibilidad**: solo para nodos de administración y nodos de puerta de enlace. Se muestra si una interfaz de red del nodo está incluida en un grupo de alta disponibilidad y si esa interfaz es la interfaz principal.
- **Direcciones IP**: Las direcciones IP del nodo. Haz clic en **Mostrar direcciones IP adicionales** para ver las direcciones IPv4 e IPv6 del nodo y las asignaciones de interfaces.

Alertas

La sección de Alertas de la pestaña Resumen muestra cualquier "[alertas que afectan actualmente a este nodo y que no se han silenciado](#)". Selecciona 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 los nodos"](#).

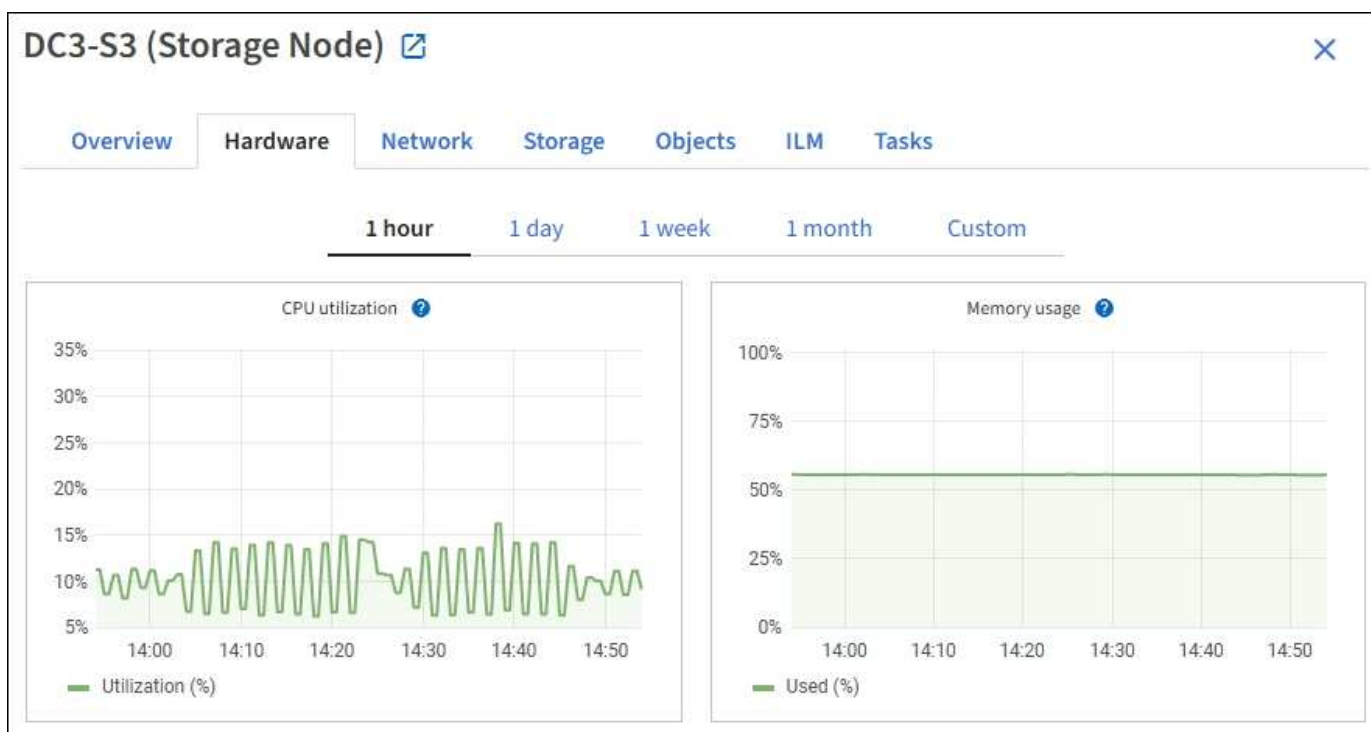
Ver la pestaña Hardware de StorageGRID

La pestaña «Hardware» muestra la utilización de CPU y el uso de memoria de cada nodo, y también información adicional sobre el hardware de los appliances.



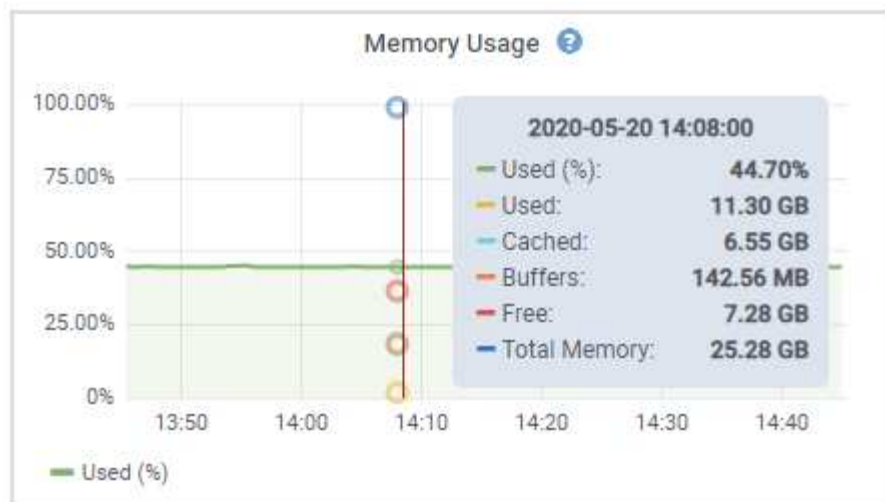
El Grid Manager se actualiza con cada versión y es posible que no coincida con las capturas de pantalla de ejemplo que aparecen en esta página.

La pestaña «Hardware» se muestra para todos los nodos.



Para visualizar un intervalo de tiempo diferente, selecciona uno de los controles situados encima del gráfico. Puedes visualizar la información disponible para intervalos de 1 hora, 1 día, 1 semana o 1 mes. También puedes establecer un intervalo personalizado, lo que te permite especificar rangos de fecha y hora.

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



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

Ver información sobre los nodos de almacenamiento de los appliances

La página «Nodos» muestra información sobre el estado del servicio y todos los recursos de computación, de disco y de red de cada Storage Node del appliance. También puedes 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 los datos de recepción y transmisión.

Pasos

1. En la página Nodos, selecciona un Storage Node de appliance.
2. Selecciona **Resumen**.

La sección «Información del nodo» de la pestaña «Resumen» muestra información resumida sobre el nodo, como el nombre del nodo, tipo, ID y estado de conexión. La lista de direcciones IP incluye el nombre de la interfaz para cada dirección, como sigue:

- **eth**: la red Grid, la red Admin o la red Client.
- **hic**: Uno de los puertos físicos de 10, 25 o 100 GbE del dispositivo. Estos puertos se pueden agrupar y conectar a la StorageGRID Grid Network (eth0) y Client Network (eth2).
- **mtc**: Uno de los puertos físicos de 1 GbE del dispositivo. Una o más interfaces mtc se agrupan para formar la interfaz de red de administración de StorageGRID (eth1). Puedes dejar otras interfaces mtc disponibles para que un técnico en el centro de datos tenga conectividad local temporal.

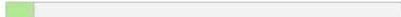
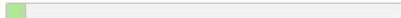
[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)Node information [?](#)

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

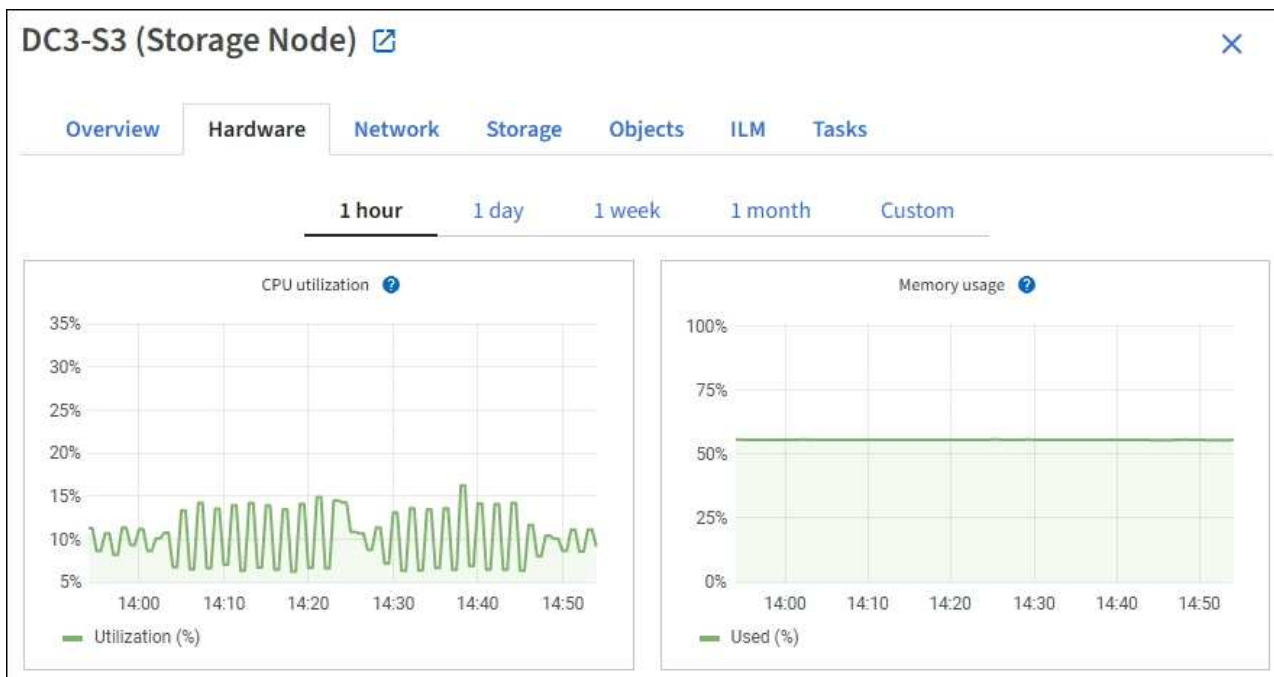
Alerts

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 de Alertas de la pestaña Resumen muestra cualquier alerta activa para el nodo.

3. Selecciona **Hardware** para ver más información sobre el dispositivo.

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



- b. Desplázate 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 «IP del controlador BMC de Compute» y «hardware de Compute», solo aparecen en los dispositivos que cuentan con esa función.

Los componentes de las estanterías de almacenamiento, y las estanterías de expansión si forman parte de la instalación, aparecen en una tabla independiente debajo de la tabla del appliance.

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 Appliance	Descripción
Modelo del appliance	El número de modelo de este dispositivo StorageGRID que aparece en SANtricity OS.
Nombre del controlador de almacenamiento	El nombre de este dispositivo StorageGRID que se muestra en SANtricity OS.
Dirección IP de gestión del controlador de almacenamiento A	Dirección IP del puerto de gestión 1 en el controlador de almacenamiento A. Usas esta dirección IP para acceder a SANtricity OS y solucionar problemas de almacenamiento.
Dirección IP de gestión del controlador de almacenamiento B	Dirección IP del puerto de gestión 1 en el controlador de almacenamiento B. Usas esta dirección IP para acceder a SANtricity OS y solucionar problemas de almacenamiento. Algunos modelos de dispositivos no tienen un controlador de almacenamiento B.

Campo en la tabla Appliance	Descripción
WWID del controlador de almacenamiento	El identificador global del controlador de almacenamiento que aparece en SANtricity OS.
Número de serie del chasis del storage appliance	El número de serie del chasis del appliance.
Versión del firmware del controlador de almacenamiento	La versión del firmware del controlador de almacenamiento de este dispositivo.
Versión del sistema operativo SANtricity del controlador de almacenamiento	La versión del sistema operativo SANtricity del controlador de almacenamiento A.
Versión de NVSRAM del controlador de almacenamiento	Versión NVSRAM del controlador de almacenamiento según lo informado por SANtricity System Manager. Para los modelos 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 indica que el estado del hardware de almacenamiento es «Requiere atención», el sistema StorageGRID también muestra este valor. Si el estado es «necesita atención», primero comprueba el controlador de almacenamiento usando SANtricity OS. Luego, asegúrate de que no existan otras alertas que apliquen al controlador de compute.
Número de unidades con error del controlador de almacenamiento	El número de unidades que no están 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 del controlador de almacenamiento.
Fuente de alimentación del controlador de almacenamiento B	El estado de la fuente de alimentación B del controlador de almacenamiento.
Tipo de unidad de almacenamiento de datos	El tipo de unidades en el dispositivo, como HDD (disco duro) o SSD (unidad de estado sólido).

Campo en la tabla Appliance	Descripción
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 los nodos con bandejas de expansión, usa el Tamaño de unidad de datos para cada shelf en su lugar. El tamaño efectivo de la unidad puede variar según la bandeja.
Modo RAID de almacenamiento	El modo RAID configurado para el dispositivo.
Conectividad de almacenamiento	El estado de la conectividad del almacenamiento.
Suministro eléctrico general	El estado de todas las fuentes de alimentación del appliance.
IP del BMC del controlador de cómputo	La dirección IP del puerto del controlador de gestión de la placa base (BMC) en el controlador de cómputo. Usas esta dirección IP para conectarte a la interfaz del BMC y así supervisar y diagnosticar el hardware del appliance. Este campo no se muestra en los modelos de dispositivos que no incorporan un BMC.
Número de serie del controlador de cómputo	El número de serie del controlador de cómputo.
Hardware informático	Estado del hardware del controlador de cálculo. Este campo no se muestra en los modelos de appliance que no tienen hardware de cálculo y hardware de almacenamiento independientes.
Temperatura de la CPU del controlador de cómputo	El estado de la temperatura de la CPU del controlador de cómputo.
Temperatura del chasis del controlador de cómputo	El estado de la temperatura del controlador de cómputo.

+

Columna en la tabla Storage shelves	Descripción
Número de serie del chasis de la estantería	El número de serie del chasis de la estantería de almacenamiento.

Columna en la tabla Storage shelves	Descripción
ID de estante	El identificador numérico de la estantería de almacenamiento. • 99: Bandeja del controlador de almacenamiento • 0: bandeja de expansión • 1: Segunda bandeja de expansión Nota: Las bandejas de expansión solo aplican a los modelos SG6060 y SG6160.
Estado de la bandeja	El estado general de la bandeja de almacenamiento.
Estado de la IOM	El estado de los módulos de entrada/salida (IOM) en cualquier bandeja de expansión. N/A si no es una bandeja de expansión.
Estado de la fuente de alimentación	El estado general de las fuentes de alimentación de la bandeja de almacenamiento.
Estado del cajón	Estado de los cajones de la estantería de almacenamiento. N/A si la estantería no contiene cajones.
Estado del ventilador	El estado general de los ventiladores de refrigeración de la estantería de almacenamiento.
Ranuras para unidades	El número total de ranuras para unidades en la bandeja de almacenamiento.
Unidades de datos	El número de unidades en la bandeja de almacenamiento que se usan para el almacenamiento de datos.
Tamaño de la unidad de datos	El tamaño efectivo de una unidad de datos en la bandeja de almacenamiento.
Unidades de caché	El número de unidades en la bandeja de almacenamiento que se utilizan como caché.
Tamaño de la unidad de caché	El tamaño de la unidad de caché más pequeña del bastidor de almacenamiento. Normalmente, todas las unidades de caché tienen el mismo tamaño.
Estado de la configuración	El estado de configuración de la bandeja de almacenamiento.

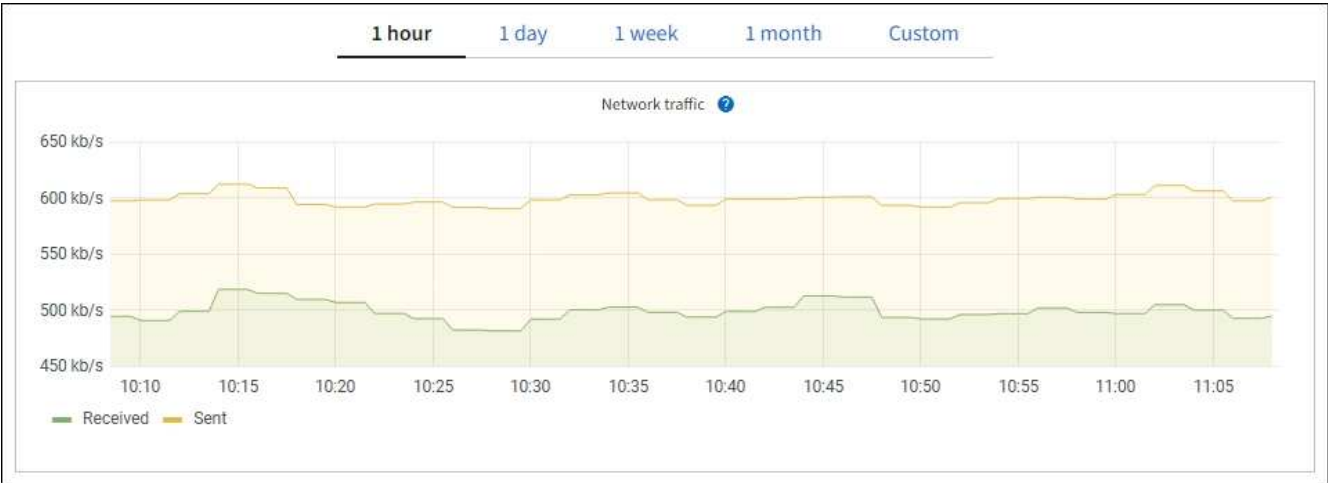
a. Confirma que todos los estados estén en "Nominal".

Si el estado no es "Nominal", revisa las alertas actuales. También puedes usar SANtricity System Manager para conocer más sobre algunos de estos valores de hardware. Consulta las instrucciones

para instalar y mantener tu appliance.

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

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



a. Consulta la sección de 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

Usa la siguiente tabla junto con los valores de la columna **Velocidad** en la tabla de Interfaces de red para determinar si los puertos de red de 10/25 GbE del appliance se configuraron para usar el modo activo/de respaldo o el modo LACP.

 Los valores que figuran en la tabla asumen que se usan los cuatro enlaces.

Modo de enlace	Modo bond	Velocidad de enlace HIC individual (hic1, hic2, hic3, hic4)	Velocidad esperada de la red Grid/Cliente (eth0, eth2)
Agregado	LACP	25	100
Corregido	LACP	25	50
Corregido	Activo/Backup	25	25
Agregado	LACP	10	40
Corregido	LACP	10	20

Modo de enlace	Modo bond	Velocidad de enlace HIC individual (hic1, hic2, hic3, hic4)	Velocidad esperada de la red Grid/Cliente (eth0, eth2)
Corregido	Activo/Backup	10	10

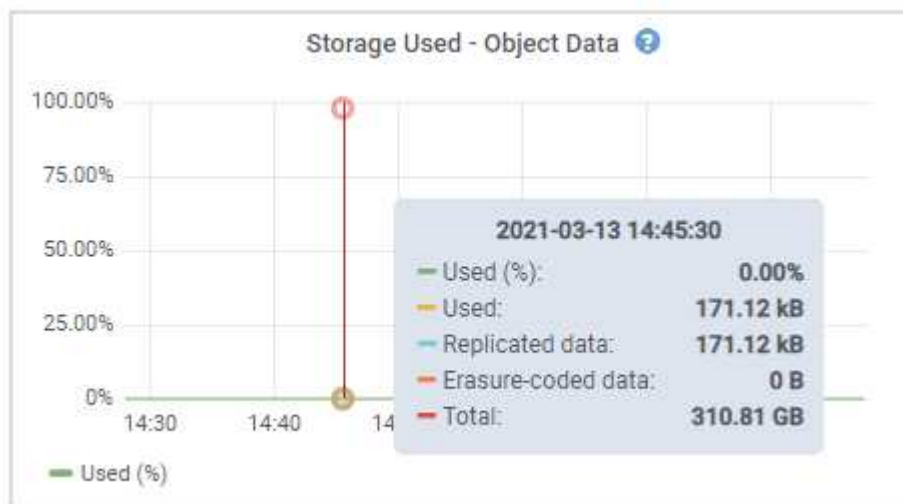
Consulta "[Configura conexiones de red](#)" para obtener más información sobre cómo configurar los puertos de 10/25 GbE.

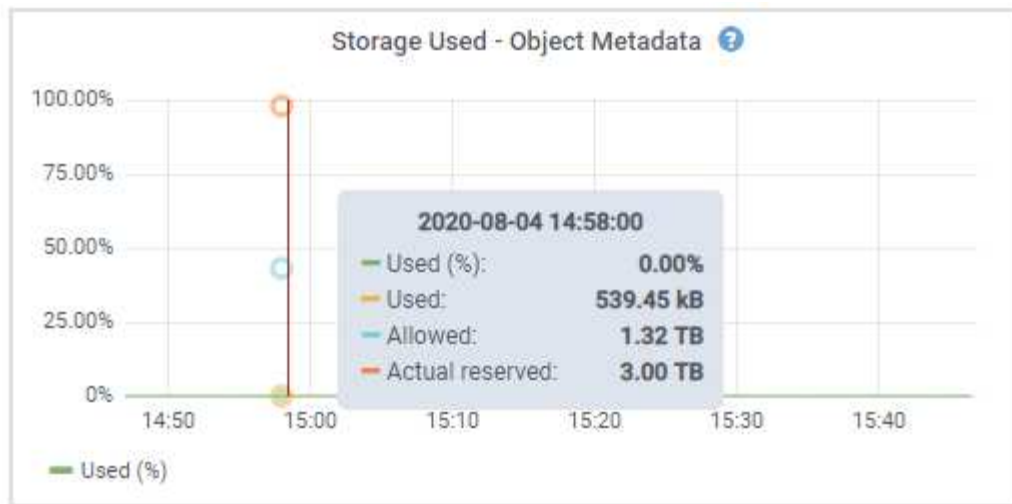
b. Consulta la sección Comunicación en red.

Las tablas «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. Selecciona **Storage** para ver gráficos que muestran los porcentajes de almacenamiento utilizado a lo largo del tiempo para los datos de objetos y los metadatos de objetos, así como información sobre los dispositivos de disco, los volúmenes y los almacenes de objetos.





- Desplázate hacia abajo para ver las cantidades de almacenamiento disponibles para cada volumen y almacén de objetos.

El nombre global de cada disco coincide con el identificador global de volumen (WWID) que aparece al consultar las propiedades estándar del volumen en SANtricity OS (el software de gestión conectado al controlador de almacenamiento del dispositivo).

Para ayudarte a interpretar las estadísticas de lectura y escritura del disco relacionadas con los puntos de montaje de los volúmenes, la primera parte del nombre que aparece en la columna **Nombre** de la tabla «Dispositivos de disco» (es decir, *sdc*, *sdd*, *sde*, y así sucesivamente) coincide con el valor que aparece 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 appliance

La página «Nodos» muestra información sobre el estado de los servicios y todos los recursos de computación, de disco y de red de cada dispositivo de servicios que se utiliza como Admin Node o Gateway Node. También puedes ver la memoria, el hardware de almacenamiento, los recursos de red, las interfaces de red, las direcciones de red y los datos recibidos y transmitidos.

Pasos

1. En la página Nodes, selecciona un appliance Admin Node o un appliance Gateway Node.
2. Selecciona **Resumen**.

La sección «Información del nodo» de la pestaña «Resumen» muestra información resumida sobre el

nodo, como el nombre del nodo, tipo, ID y estado de conexión. La lista de direcciones IP incluye el nombre de la interfaz para cada dirección, como sigue:

- **adl1b** y **adl1i**: Se muestran si se utiliza bonding activo/de respaldo para la interfaz de red de administración
- **eth**: la red Grid, la red Admin o la red Client.
- **hic**: Uno de los puertos físicos de 10, 25 o 100 GbE del dispositivo. Estos puertos se pueden agrupar y conectar a la StorageGRID Grid Network (eth0) y Client Network (eth2).
- **mtc**: Uno de los puertos físicos de 1 GbE del dispositivo. Una o varias interfaces mtc se agrupan para formar la interfaz de red de administración (eth1). Puedes dejar otras interfaces mtc disponibles para que un técnico del centro de datos disponga de conectividad local temporal.

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

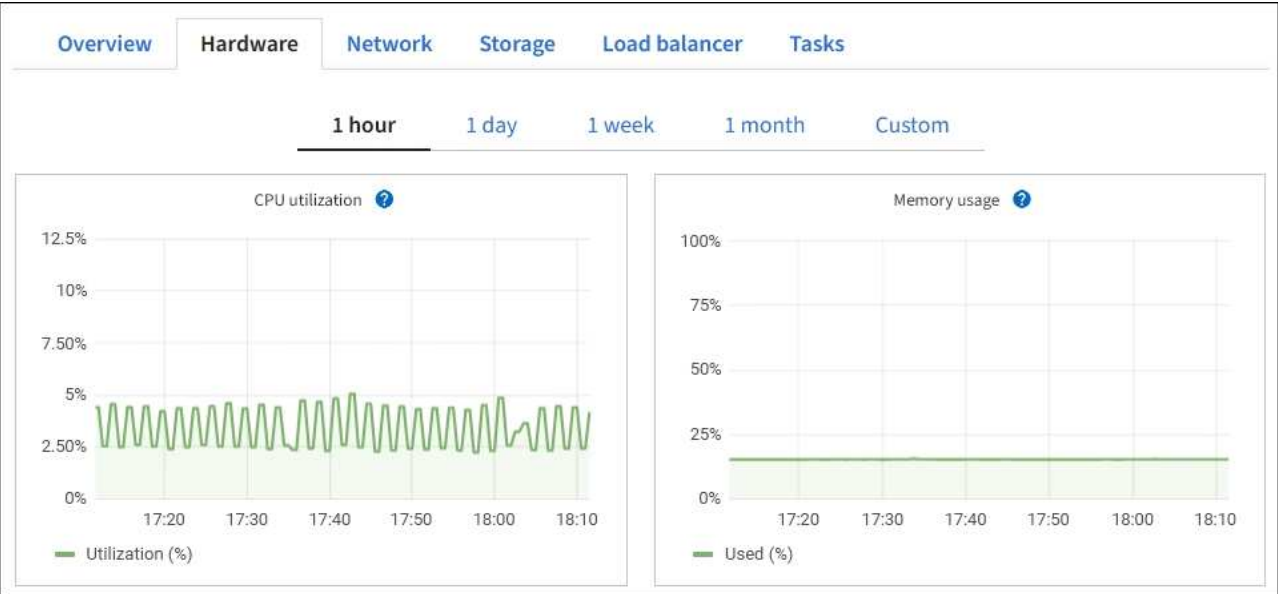
Interface 	IP address
eth2 (Client Network)	47.47.7.241
eth2 (Client Network)	fd20:332:332:0:e42:a1ff:fe86:b5b0
eth2 (Client Network)	fe80::e42:a1ff:fe86:b5b0
hic1	47.47.7.241
hic2	47.47.7.241
hic3	47.47.7.241

La sección de Alertas de la pestaña Resumen muestra cualquier alerta activa para el nodo.

3. Selecciona **Hardware** para ver más información sobre el dispositivo.

a. Consulta los gráficos de utilización de CPU y de memoria para determinar los porcentajes de uso de CPU y memoria a lo largo del tiempo. Para mostrar un intervalo de tiempo diferente, selecciona uno de los controles situados encima del gráfico. Puedes visualizar la información disponible para intervalos de 1 hora, 1 día, 1 semana o 1 mes. También puedes establecer un intervalo personalizado, lo que te permite especificar rangos de fecha y hora.

985



b. Desplázate hacia abajo para ver la tabla de componentes del appliance. 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 Appliance	Descripción
Modelo del appliance	El número de modelo de este dispositivo StorageGRID.

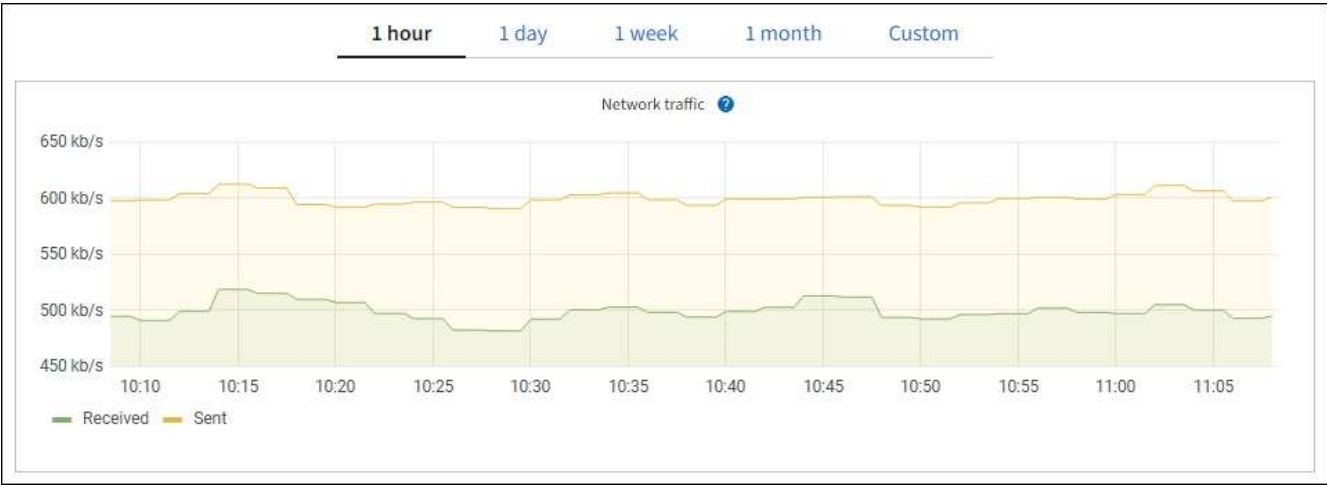
Campo en la tabla Appliance	Descripción
Número de unidades con error del controlador de almacenamiento	El número de unidades que no están óptimas.
Tipo de unidad de almacenamiento de datos	El tipo de unidades en el dispositivo, como HDD (disco duro) o SSD (unidad de estado sólido).
Tamaño de la unidad de datos de almacenamiento	El tamaño efectivo de una unidad de datos.
Modo RAID de almacenamiento	El modo RAID del dispositivo.
Suministro eléctrico general	El estado de todas las fuentes de alimentación del appliance.
IP del BMC del controlador de cómputo	La dirección IP del puerto del controlador de gestión de la placa base (BMC) en el controlador de cálculo. Puedes usar esta dirección IP para conectarte a la interfaz del BMC y así supervisar y diagnosticar el hardware del appliance. Este campo no se muestra en los modelos de dispositivos que no incorporan un BMC.
Número de serie del controlador de cómputo	El número de serie del controlador de cómputo.
Hardware informático	El estado del hardware del controlador de cómputo.
Temperatura de la CPU del controlador de cómputo	El estado de la temperatura de la CPU del controlador de cómputo.
Temperatura del chasis del controlador de cómputo	El estado de la temperatura del controlador de cómputo.

a. Confirma que todos los estados estén en "Nominal".

Si el estado no es «Nominal», revisa cualquier alerta actual.

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

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



a. Consulta la sección de 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	

Utiliza la siguiente tabla junto con los valores de la columna **Velocidad** de la tabla Network Interfaces para determinar si los cuatro puertos de red de 40/100-GbE del appliance se configuraron para usar el modo activo/de respaldo o el modo LACP.



Los valores que figuran en la tabla asumen que se usan los cuatro enlaces.

Modo de enlace	Modo bond	Velocidad de enlace HIC individual (hic1, hic2, hic3, hic4)	Velocidad esperada de la red Grid/cliente (eth0, eth2)
Agregado	LACP	100	400
Corregido	LACP	100	200
Corregido	Activo/Backup	100	100
Agregado	LACP	40	160
Corregido	LACP	40	80
Corregido	Activo/Backup	40	40

b. Consulta la sección Comunicación en red.

Las tablas «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. Selecciona **Storage** para ver información sobre los dispositivos de disco y los volúmenes del 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 Network de StorageGRID

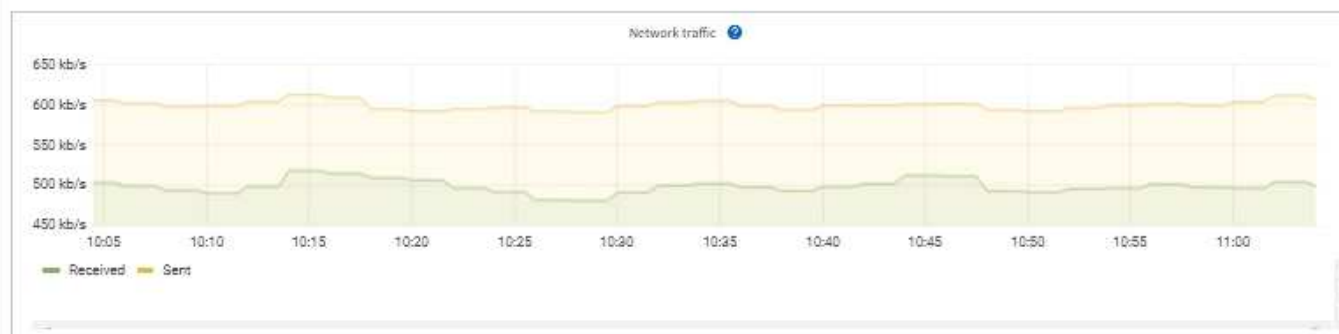
La pestaña Red muestra un gráfico con el tráfico de red recibido y enviado a través de todas las interfaces de red del nodo, el sitio o el grid.

La pestaña «Red» se muestra para todos los nodos, cada sitio y toda la grid.

Para visualizar un intervalo de tiempo diferente, selecciona uno de los controles situados encima del gráfico. Puedes visualizar la información disponible para intervalos de 1 hora, 1 día, 1 semana o 1 mes. También puedes establecer un intervalo personalizado, lo que te permite especificar rangos de fecha y hora.

En el caso de los nodos, la tabla de interfaces de red ofrece información sobre los puertos de red físicos de cada nodo. La tabla de comunicaciones de red ofrece detalles sobre las operaciones de recepción y transmisión de cada nodo y sobre cualquier contador de fallos informado por el controlador.

DC1-S2 (Storage Node)

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

Network 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

"Supervisa las conexiones de red y el rendimiento"

Ver la pestaña StorageGRID Storage

La pestaña Almacenamiento resume la disponibilidad del almacenamiento y otras métricas de almacenamiento.

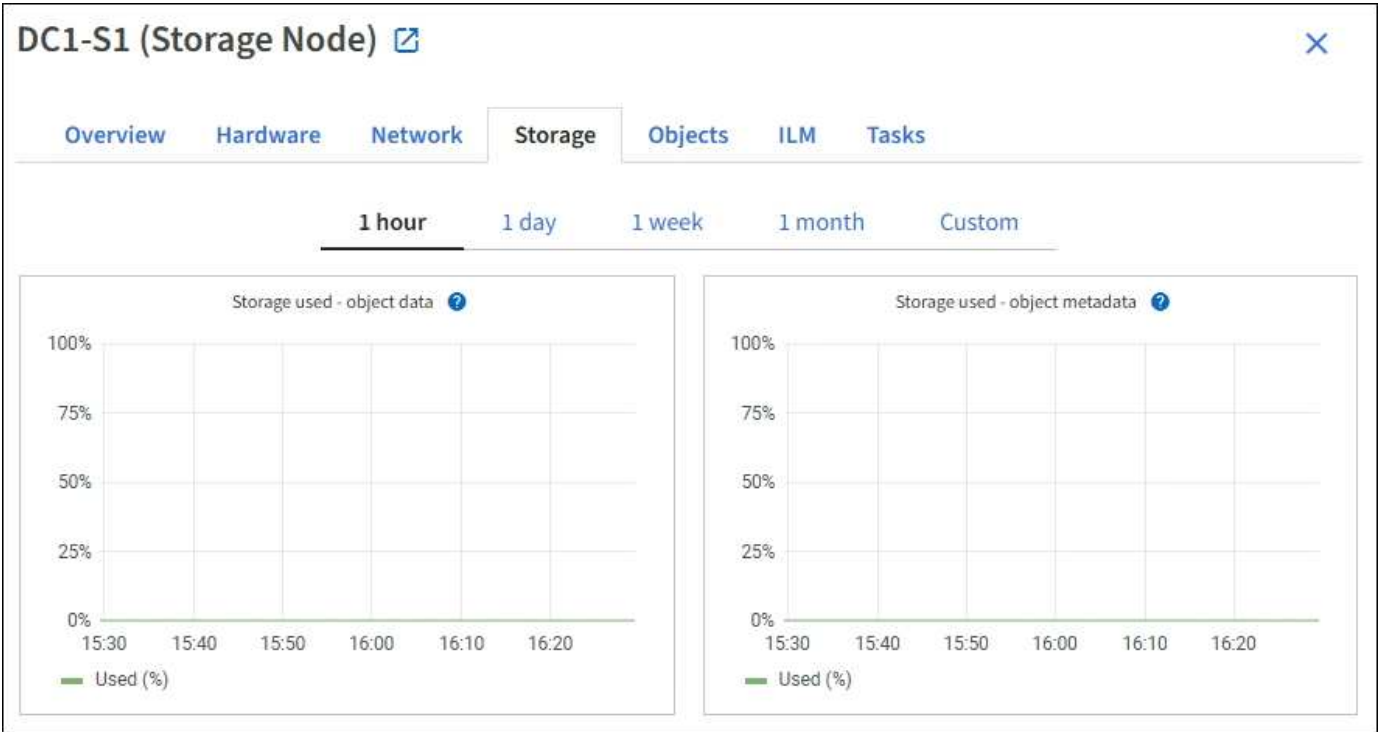
La pestaña «Almacenamiento» se muestra para todos los nodos, cada sitio y toda la grid.

Gráficos de almacenamiento utilizado

Para los nodos de almacenamiento, cada sitio y toda la grid, la pestaña de Almacenamiento incluye gráficos que muestran cuánto almacenamiento se ha utilizado para los datos de objetos y los metadatos de objetos a lo largo del tiempo.



Cuando un nodo no está conectado a la grid, como durante una actualización o en un estado desconectado, es posible que algunas métricas no estén disponibles o se excluyan de los totales del sitio y de la grid. Después de que un nodo se vuelva a conectar a la grid, espera 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 sobre los dispositivos de disco y los volúmenes del nodo. Para los nodos de almacenamiento, la tabla «Almacenes de objetos» ofrece 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

["Supervisa la capacidad de almacenamiento"](#)

Ver la pestaña Objects de StorageGRID

La pestaña «Objetos» ofrece información sobre ["Tasas de ingesta y recuperación en S3"](#).

La pestaña «Objetos» se muestra para cada nodo de almacenamiento, cada sitio y toda la grid. En el caso de los nodos de almacenamiento, la pestaña «Objetos» también ofrece el recuento de objetos e información sobre consultas de metadatos y verificaciones 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

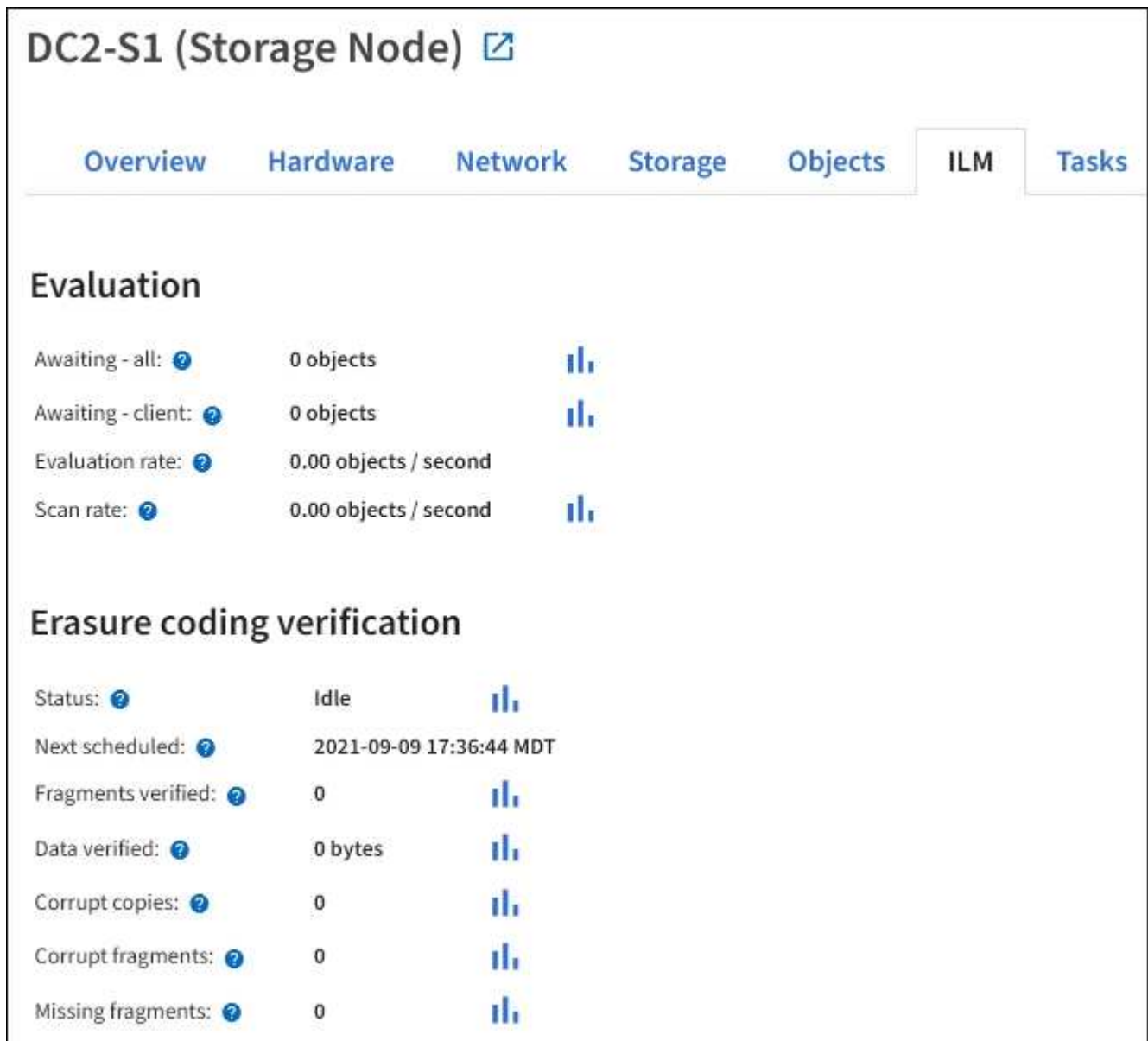
Quarantined objects: ? 0

Ver la pestaña ILM de StorageGRID

La pestaña «ILM» ofrece información sobre las operaciones de gestión del ciclo de vida de la información (ILM).

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

Para los nodos de almacenamiento, la pestaña ILM ofrece detalles sobre la evaluación de ILM y la verificación en segundo plano para los objetos con código de borrado.



Información relacionada

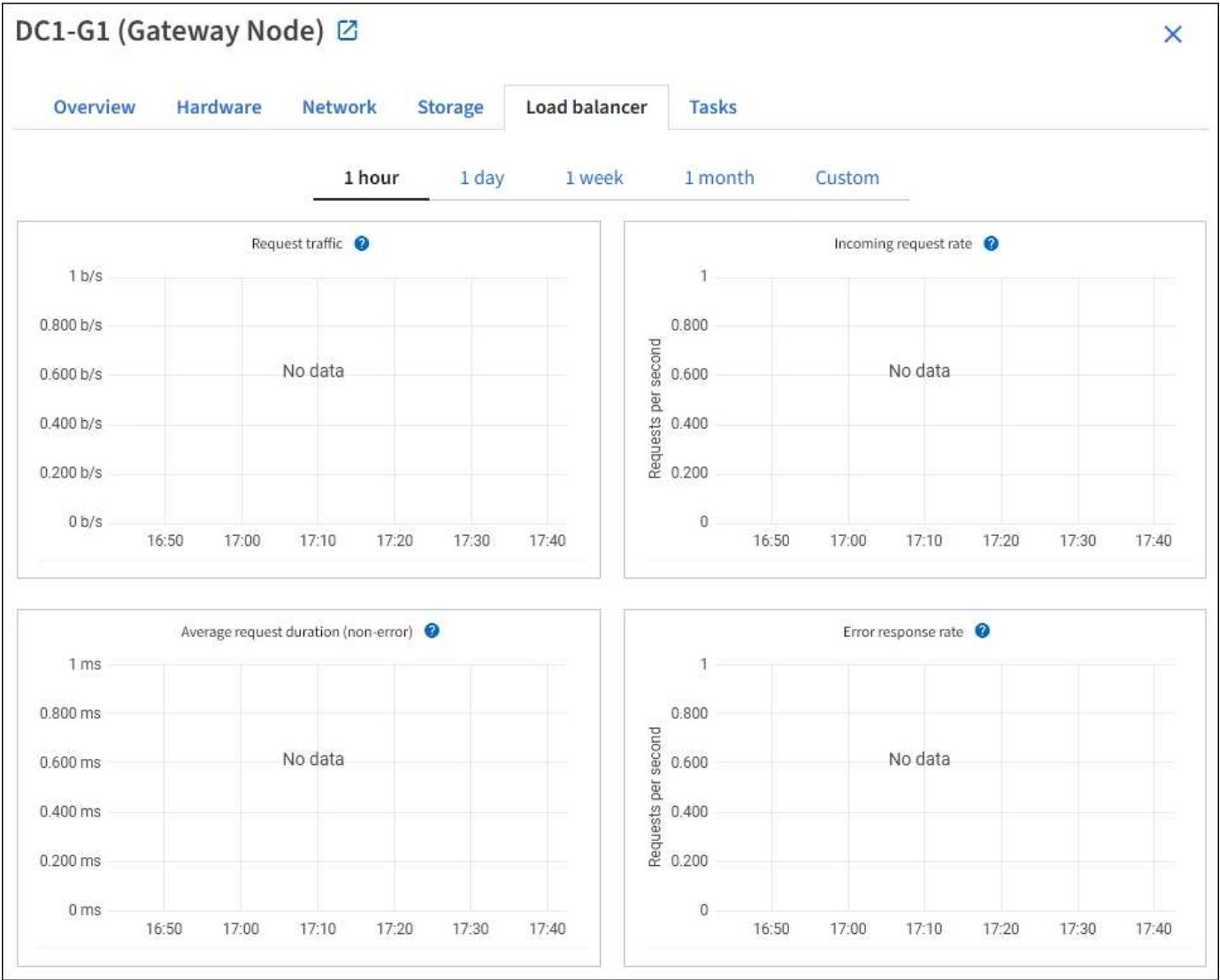
- ["Supervisa la gestión del ciclo de vida de la información"](#)
- ["Administrar StorageGRID"](#)

Ver la pestaña Load balancer de StorageGRID

La pestaña «Load Balancer» incluye gráficos de rendimiento y diagnóstico relacionados con el funcionamiento del servicio de Load Balancer.

La pestaña Load Balancer se muestra para los nodos de administración y los nodos de puerta de enlace, para cada sitio y para toda la grid. Para cada sitio, la pestaña Load Balancer ofrece un resumen agregado de las estadísticas de todos los nodos de ese sitio. Para toda la grid, la pestaña Load Balancer ofrece un resumen agregado de las estadísticas de todos los sitios.

Si no hay ninguna operación de E/S pasando por el servicio de equilibrador de carga, o si no hay ningún equilibrador de carga configurado, los gráficos muestran "Sin datos".





Este valor se actualiza al finalizar cada solicitud. Por ello, este valor puede diferir del rendimiento en tiempo real cuando la frecuencia de solicitudes es baja o en el caso de solicitudes de larga duración. Puedes consultar la pestaña Red para obtener una visión más realista del comportamiento actual de la red.

Tasa de solicitudes entrantes

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

Duración media de las solicitudes (sin errores)

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

Índice de respuestas con error

Este gráfico muestra una media móvil de 3 minutos del número de respuestas de error devueltas a los clientes por segundo, desglosado por el código de respuesta de error.

Información relacionada

- ["Supervisa las operaciones de equilibrio de carga"](#)
- ["Administrar StorageGRID"](#)

Ver la pestaña de servicios de la plataforma StorageGRID

La pestaña Servicios de la plataforma ofrece información sobre cualquier operación de servicios de plataforma S3 en un sitio.

La pestaña «Servicios de la plataforma» aparece en cada sitio. Esta pestaña ofrece 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 el número de solicitudes pendientes, la tasa de finalización de solicitudes y la tasa de fallos de solicitudes.

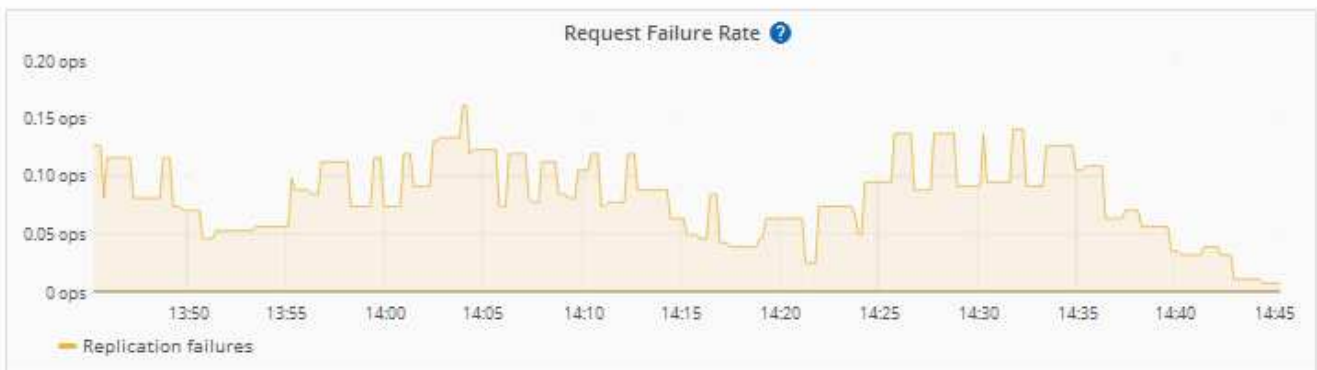
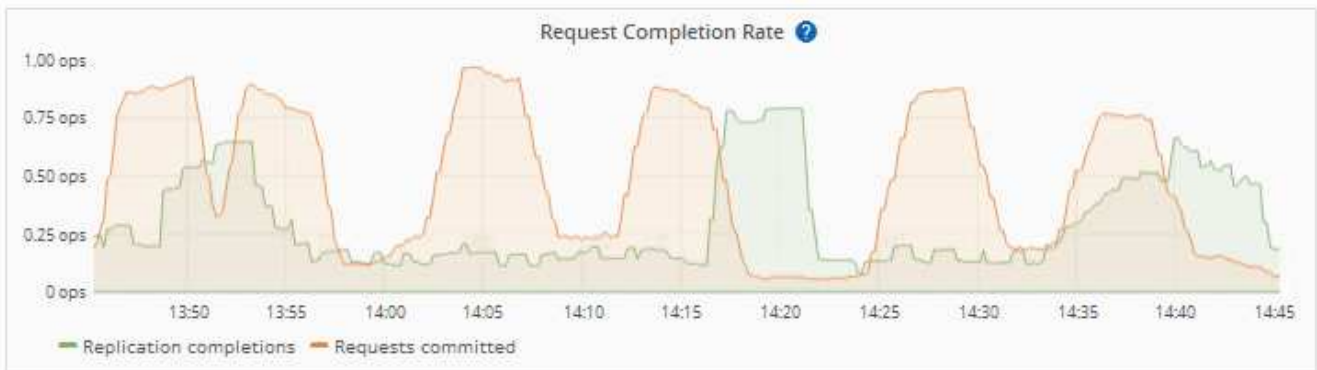
1 hour

1 day

1 week

1 month

Custom



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

Ver la pestaña Manage drives de StorageGRID

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

En la pestaña «Gestionar unidades», puedes hacer lo siguiente:

- Ver un esquema de las unidades de almacenamiento de datos en el dispositivo
- Ver una tabla que muestra la ubicación, el tipo, el estado, la versión del firmware y el número de serie de cada unidad
- Realiza tareas de resolución de problemas y mantenimiento en cada unidad

Para acceder a la pestaña Gestionar unidades, debes tener el ["Permiso de administrador de almacenamiento o acceso Root"](#).

Para obtener información sobre cómo utilizar la pestaña Manage drives, consulta ["Utiliza la pestaña Gestionar unidades"](#).

Ver la pestaña SANtricity System Manager de StorageGRID

La pestaña «SANtricity System Manager» te permite acceder a SANtricity System Manager sin necesidad de configurar ni conectar el puerto de gestión del dispositivo de almacenamiento. Puedes utilizar esta pestaña para consultar información sobre el diagnóstico del hardware y el entorno, así como sobre problemas relacionados con las unidades.



Acceder a SANtricity System Manager desde Grid Manager generalmente es solo para supervisar el hardware del dispositivo y configurar E-Series AutoSupport. Muchas funciones y operaciones dentro de SANtricity System Manager, como actualizar el firmware, no aplican para supervisar tu dispositivo StorageGRID. Para evitar problemas, sigue siempre las instrucciones de mantenimiento de hardware para tu dispositivo. Para actualizar el firmware de SANtricity, consulta el ["Procedimientos de configuración de mantenimiento"](#) para tu dispositivo de almacenamiento.



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

Con SANtricity System Manager, puedes hacer lo siguiente:

- Consulta datos de rendimiento como el rendimiento a nivel de la matriz de almacenamiento, la latencia de E/S, la utilización de CPU del controlador de almacenamiento y el rendimiento.
- Comprueba el estado de los componentes de hardware.
- Realiza tareas de soporte, como consultar datos de diagnóstico y configurar E-Series AutoSupport.



Para usar SANtricity System Manager para configurar un proxy para E-Series AutoSupport, consulta ["Envía paquetes de E-Series AutoSupport a través de StorageGRID"](#).

Para acceder a SANtricity System Manager a través de Grid Manager, debes tener la ["Permiso de administrador de almacenamiento o acceso Root"](#).



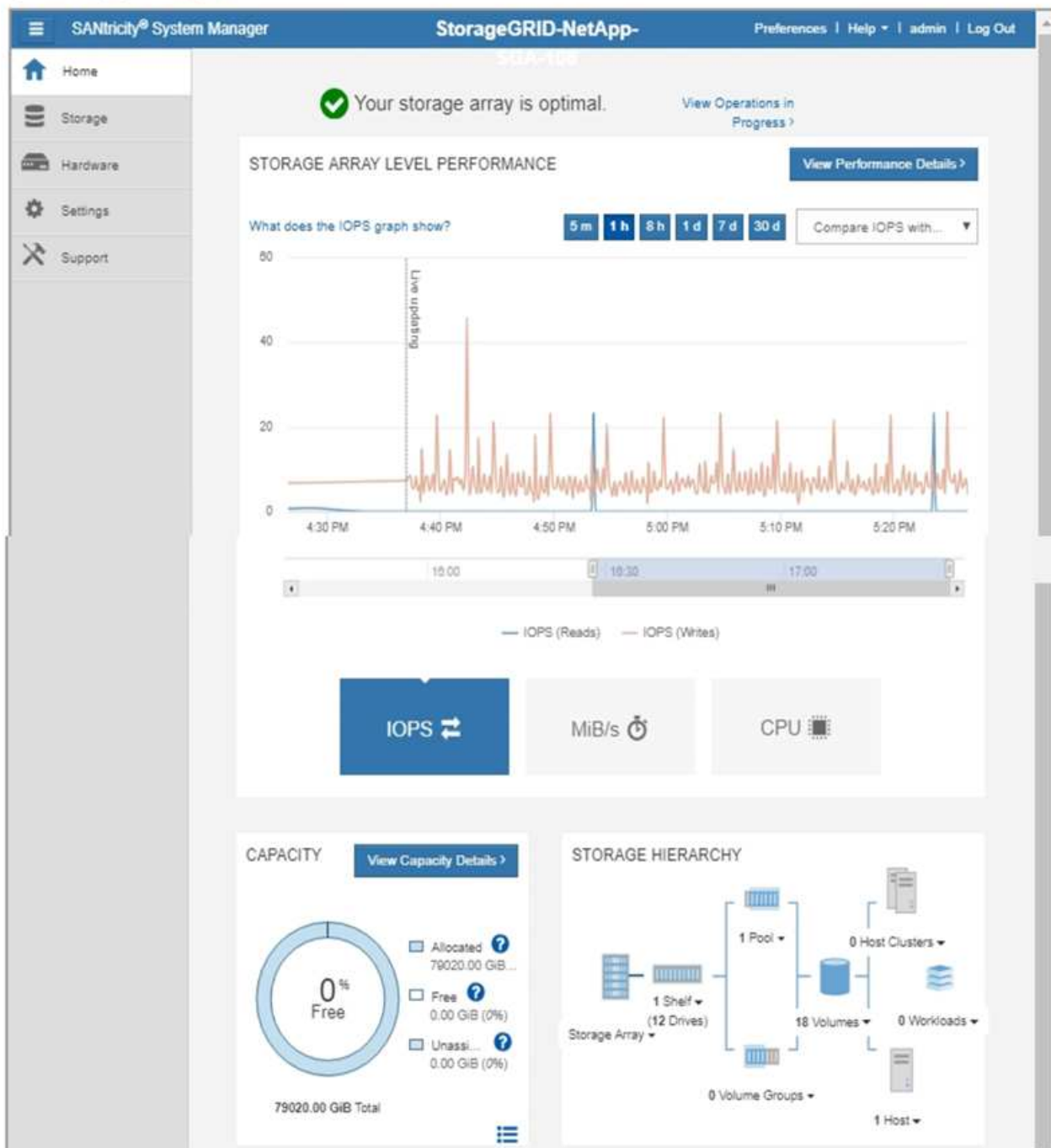
Debes disponer del firmware 8.70 o superior de SANtricity para acceder a SANtricity System Manager mediante Grid Manager.

Esta 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.



Puedes usar el enlace de SANtricity System Manager para abrir SANtricity System Manager en una nueva ventana del navegador y ver todo más fácilmente.

Para ver los detalles sobre el rendimiento y el uso de la capacidad de almacenamiento a nivel de la cabina,

coloca el cursor sobre cada gráfico.

Para obtener más detalles sobre cómo ver la información accesible desde la pestaña SANtricity System Manager, consulta ["NetApp E-Series y documentación de SANtricity"](#).

Información que debes supervisar regularmente

Qué y cuándo supervisar en StorageGRID

Aunque el sistema StorageGRID puede seguir funcionando cuando se producen errores o cuando algunas partes de la grid no están disponibles, deberías supervisar y resolver los posibles problemas antes de que afecten la eficiencia o la disponibilidad de la grid.

Antes de empezar

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

Acerca de las tareas de supervisión

Un sistema con mucha actividad genera grandes cantidades de información. La siguiente lista ofrece orientación sobre la información más importante que hay que supervisar de forma continua.

Qué hay que supervisar	Frecuencia
"Estado de salud del sistema"	Diario
Tasa a la que se está consumiendo "Capacidad de objetos y metadatos de Storage Node"	Semanal
"Operaciones de gestión del ciclo de vida de la información"	Semanal
"Redes y recursos del sistema"	Semanal
"Actividad del inquilino"	Semanal
"Operaciones del cliente S3"	Semanal
"Operaciones de equilibrio de carga"	Tras la configuración inicial y tras cualquier cambio en la configuración
"Conexiones de grid federation"	Semanal

Supervisa la salud del sistema en StorageGRID

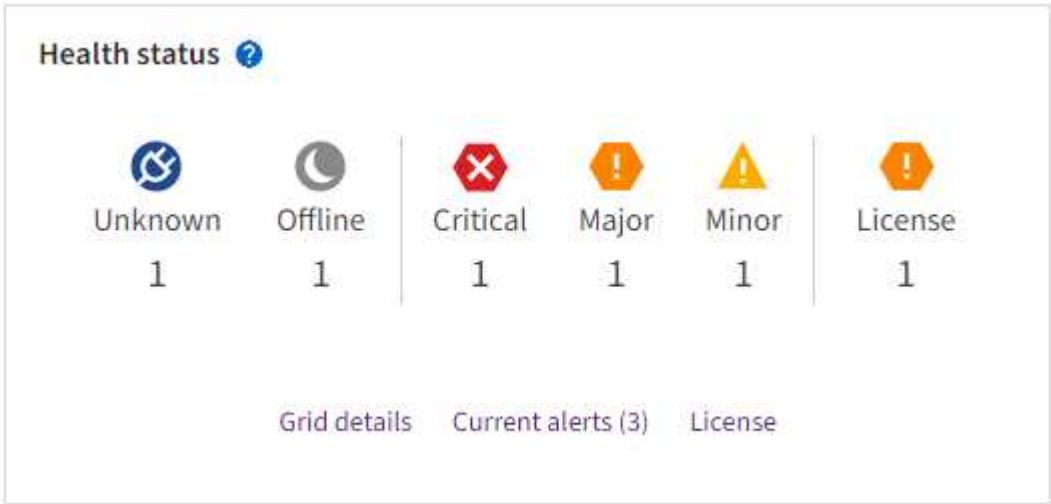
Supervisa diariamente el estado general de tu sistema StorageGRID.

Acerca de esta tarea

El sistema StorageGRID puede seguir funcionando aunque algunas partes de la red no estén disponibles. Los posibles problemas indicados por las alertas no tienen por qué ser problemas relacionados con el

funcionamiento del sistema. Investiga los problemas resumidos en la tarjeta de estado de salud del panel de Grid Manager.

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



Cuando hay incidencias, aparecen enlaces que te permiten consultar más detalles:

Enlace	Aparece cuando...
Detalles de la cuadrícula	Hay nodos desconectados (estado de conexión Unknown o Administratively Down).
Alertas actuales (críticas, mayores, menores)	Las alertas están actualmente activo .
Alertas resueltas recientemente	Alertas activadas durante la última semana ya se han resuelto .
Licencia	Hay un problema con la licencia de software de este sistema StorageGRID. Puedes "Actualizar la información de la licencia según sea necesario" .

Supervisa el estado de las conexiones de los nodos

Si uno o varios nodos se desconectan de la grid, las operaciones críticas de StorageGRID podrían verse afectadas. Supervisa el estado de conexión de los nodos y resuelve cualquier problema con prontitud.

Icono	Descripción	Acción requerida
	Sin conexión - Desconocido Por alguna razón desconocida, un nodo se ha desconectado o los servicios de dicho nodo han dejado de funcionar de forma inesperada. Por ejemplo, es posible que un servicio del nodo se haya detenido o que el nodo haya perdido la conexión a la red debido a un corte de corriente o a una interrupción inesperada. También podría activarse la alerta Unable to communicate with node. Es posible que también haya otras alertas activas.	Requiere atención inmediata. Selecciona cada alerta y sigue las acciones recomendadas. Por ejemplo, es posible que tengas que reiniciar un servicio que se haya detenido o reiniciar el host para el nodo. Nota: Es posible que un nodo aparezca como «Desconocido» durante las operaciones de apagado controlado. En estos casos, puedes ignorar el estado «Desconocido».
	Sin conexión - Fuera de servicio por motivos administrativos Por una razón previsible, el nodo no está conectado a la grid. Por ejemplo, el nodo, o los servicios en el nodo, se ha apagado de forma controlada, el nodo se está reiniciando o el software se está actualizando. También puede haber una o más alertas activas. Dependiendo del problema subyacente, estos nodos suelen volver a estar en línea sin intervención.	Comprueba si hay alguna alerta que afecte a este nodo. Si hay una o varias alertas activas, selecciona cada alerta y sigue las medidas recomendadas.
	Conectado El nodo está conectado a la grid.	No es necesario realizar ninguna acción.

Ver alertas actuales y resueltas

Alertas actuales: Cuando se activa una alerta, aparece un icono de alerta en el panel de control. También aparece un icono de alerta para el nodo en la página de Nodos. Si "[Las notificaciones por correo electrónico de alertas están configuradas](#)", también se enviará una notificación por correo electrónico, a menos que se haya silenciado la alerta.

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

Opcionalmente, has visto el vídeo:

[Resumen de alertas](#)

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

Encabezado de columna	Descripción
Nombre o título	El nombre de la alerta y su descripción.
Gravedad	La gravedad de la alerta. Para las alertas actuales, si hay varias alertas agrupadas, la fila del título muestra cuántas instancias de esa alerta están ocurriendo en cada gravedad.  Crítico: Existe una condición anómala que ha detenido las operaciones normales de un nodo o servicio de StorageGRID. Debes solucionar el problema subyacente de inmediato. Si no resuelves el problema, podría haber interrupciones en el servicio y pérdida de datos.  Grave: Existe una situación anómala que está afectando al funcionamiento actual o que se está acercando al umbral de una alerta crítica. Deberías investigar las alertas graves y resolver cualquier problema subyacente para asegurarte de que la situación anómala no detenga el funcionamiento normal de un nodo o servicio de StorageGRID.  Menor: El sistema funciona con normalidad, pero existe una situación anómala que, si continúa, podría afectar la capacidad del sistema para operar. Deberías supervisar y resolver las alertas menores que no se resuelvan por sí solas para asegurarte de que no resulten en un problema más grave.
Activado por tiempo	Alertas actuales: La fecha y la hora en que se activó la alerta, tanto en tu hora local como en UTC. Si hay varias alertas agrupadas, la fila del título muestra las horas de la instancia más reciente de la alerta (<i>newest</i>) y de la más antigua (<i>oldest</i>). Alertas resueltas: cuánto tiempo hace que se activó la alerta.
Sitio/Nodo	El nombre del sitio y del nodo en el que se está produciendo o se ha producido la alerta.
Estado	Si la alerta está activa, silenciada o resuelta. Si hay varias alertas agrupadas y se selecciona All alerts en el menú desplegable, la fila del título muestra cuántas instancias de esa alerta están activas y cuántas se han silenciado.
Hora de resolución (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. En algunas alertas, se muestran valores adicionales para ayudarte a comprender e investigar la alerta. Por ejemplo, los valores que se muestran para una alerta de Low object data storage 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 del título.

Encabezado de columna	Descripción
Valores activados (solo alertas resueltas)	El valor de la métrica que provocó que se activara la alerta. En algunas alertas, se muestran valores adicionales para ayudarte a comprender e investigar la alerta. Por ejemplo, los valores que se muestran para una alerta de Low object data storage 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. Selecciona el enlace **Alertas actuales** o **Alertas resueltas** para ver una lista de alertas en esas categorías. También puedes ver los detalles de una alerta seleccionando **Nodos > nodo > Resumen** y luego seleccionando la alerta en la tabla de Alertas.

De forma predeterminada, las alertas actuales se muestran de la siguiente manera:

- Las alertas activadas más recientemente se muestran en primer lugar.
- Varias alertas del mismo tipo se muestran como un grupo.
- Las alertas que se han silenciado no se muestran.
- En el caso de una alerta concreta en un nodo específico, si se alcanzan los umbrales para más de una gravedad, solo se muestra la alerta de mayor gravedad. Es decir, si se alcanzan los umbrales de alerta para las gravedades menor, mayor y crítica, solo se muestra la alerta crítica.

La página «Alertas actuales» se actualiza cada dos minutos.

2. Para expandir los grupos de alertas, selecciona el símbolo de flecha hacia abajo ▼. Para contraer alertas individuales en un grupo, selecciona el símbolo de flecha hacia arriba ▲ o selecciona el nombre del grupo.
3. Para mostrar alertas individuales en lugar de grupos de alertas, desmarca la casilla **Agrupar alertas**.
4. Para ordenar las alertas actuales o los grupos de alertas, selecciona las flechas arriba/abajo ⬆⬇ en el encabezado de cada columna.
 - Cuando se selecciona **Alertas de grupo**, se ordenan tanto los grupos de alertas como las alertas individuales de cada grupo. Por ejemplo, podrías querer ordenar las alertas de un grupo por **Hora de activación** para encontrar la instancia más reciente de una alerta específica.
 - Cuando se desmarca la opción **Group alerts**, se ordena toda la lista de alertas. Por ejemplo, es posible que quieras ordenar todas las alertas por **Node/Site** para ver todas las alertas que afectan a un nodo concreto.
5. Para filtrar las alertas actuales por estado (**Todas las alertas**, **Activas** o **Silenciadas**, utiliza el menú desplegable situado en la parte superior de la tabla.

Consulta ["Silenciar las notificaciones de alerta"](#).

6. Para ordenar las alertas resueltas:
 - Selecciona un intervalo de tiempo en el menú desplegable **When triggered**.
 - Selecciona una o más gravedades en el menú desplegable **Gravedad**.
 - Selecciona una o varias reglas de alerta predeterminadas o personalizadas en el menú desplegable **Regla de alerta** para filtrar las alertas resueltas relacionadas con una regla de alerta concreta.
 - Selecciona uno o más nodos en el menú desplegable **Nodo** para filtrar las alertas resueltas relacionadas con un nodo específico.

7. Para ver los detalles de una alerta concreta, selecciona la alerta. Aparecerá un cuadro de diálogo con los detalles y las acciones recomendadas para la alerta que seleccionaste.
8. (Opcional) Para una alerta concreta, selecciona **silence this alert** para silenciar la regla de alerta que provocó que se activara esta alerta.

Debes tener el ["Gestiona alertas o permisos de acceso root"](#) para desactivar una regla de alerta.



Ten cuidado a la hora de decidir silenciar una regla de alerta. Si se silencia una regla de alerta, es posible que no detectes un problema subyacente hasta que este impida que se complete una operación crítica.

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

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

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

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

10. Si lo deseas, selecciona **Editar regla** para modificar la regla de alerta que provocó que se activara esta alerta.

Debes tener el ["Gestiona alertas o permisos de acceso root"](#) para editar una regla de alerta.



Ten cuidado a la hora de editar una regla de alerta. Si modificas los valores de activación, es posible que no detectes un problema subyacente hasta que este impida que se complete una operación crítica.

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

Supervisa la capacidad de almacenamiento en StorageGRID

Supervisa el espacio útil total disponible para asegurarte de que el sistema StorageGRID no se quede sin espacio de almacenamiento para objetos ni para metadatos de objetos.

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

Puedes ["Ver información sobre la capacidad de almacenamiento"](#) para toda la grid, para cada sitio y para cada nodo de almacenamiento en tu sistema StorageGRID.

Supervisa la capacidad de almacenamiento de toda la grid

Supervisa la capacidad de almacenamiento total de tu grid para asegurarte de que queda suficiente espacio libre para los datos de objetos y los metadatos de objetos. Comprender cómo varía la capacidad de almacenamiento con el tiempo puede ayudarte a planificar la incorporación de Storage Nodes o volúmenes de almacenamiento antes de que se consuma la capacidad de almacenamiento utilizable del grid.

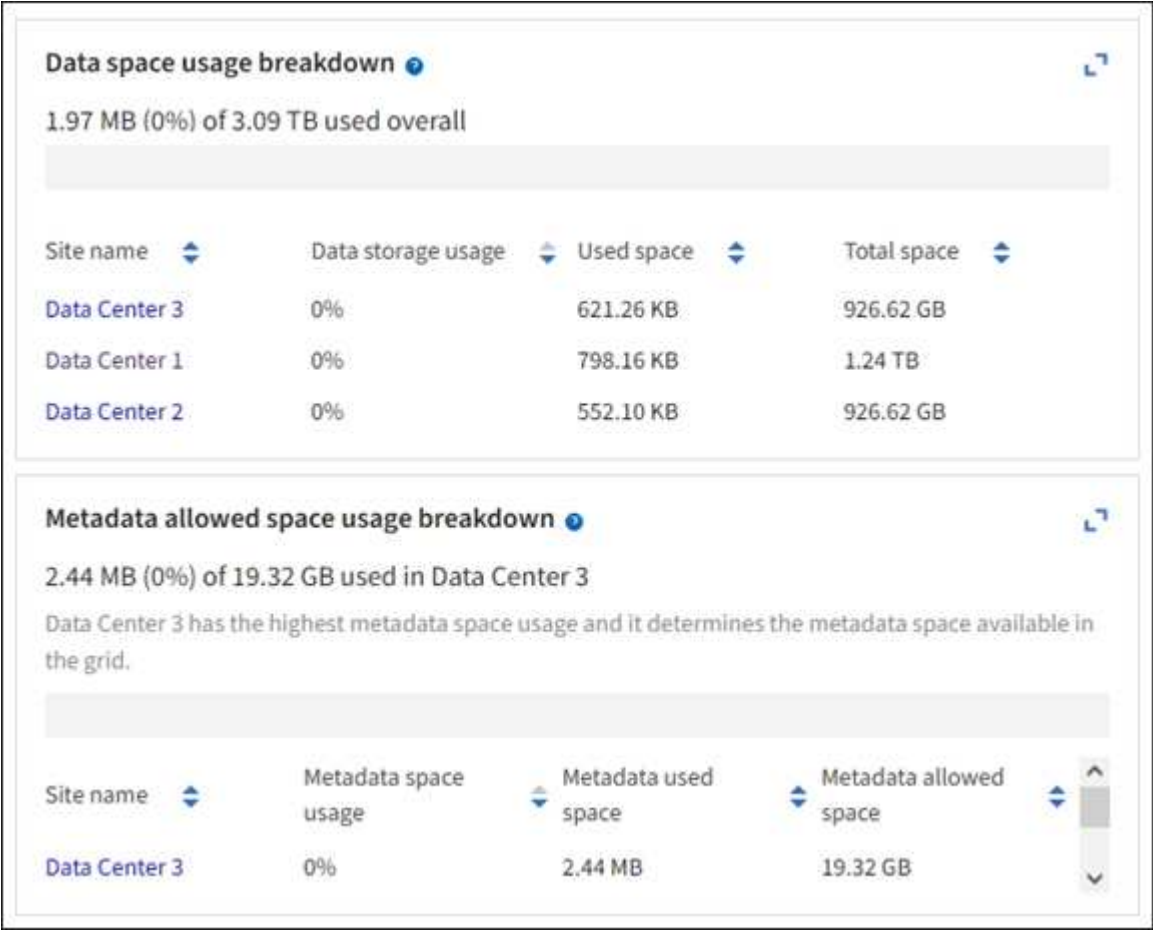
El panel de control de Grid Manager te permite evaluar rápidamente cuánto almacenamiento hay disponible para toda la grid y para cada centro de datos. La página Nodes ofrece valores más detallados sobre los datos

de objetos y los metadatos de objetos.

Pasos

- 1. Evalúa cuánto espacio de almacenamiento hay disponible para toda la grid y para cada centro de datos.
 - a. Selecciona **Dashboard > Overview**.
 - b. Fíjate en los valores que aparecen en las fichas «Desglose del uso del espacio de datos» y «Desglose del uso del espacio permitido para metadatos». En cada ficha se indica el porcentaje de uso del almacenamiento, la capacidad del espacio utilizado y el espacio total disponible o permitido por sitio.

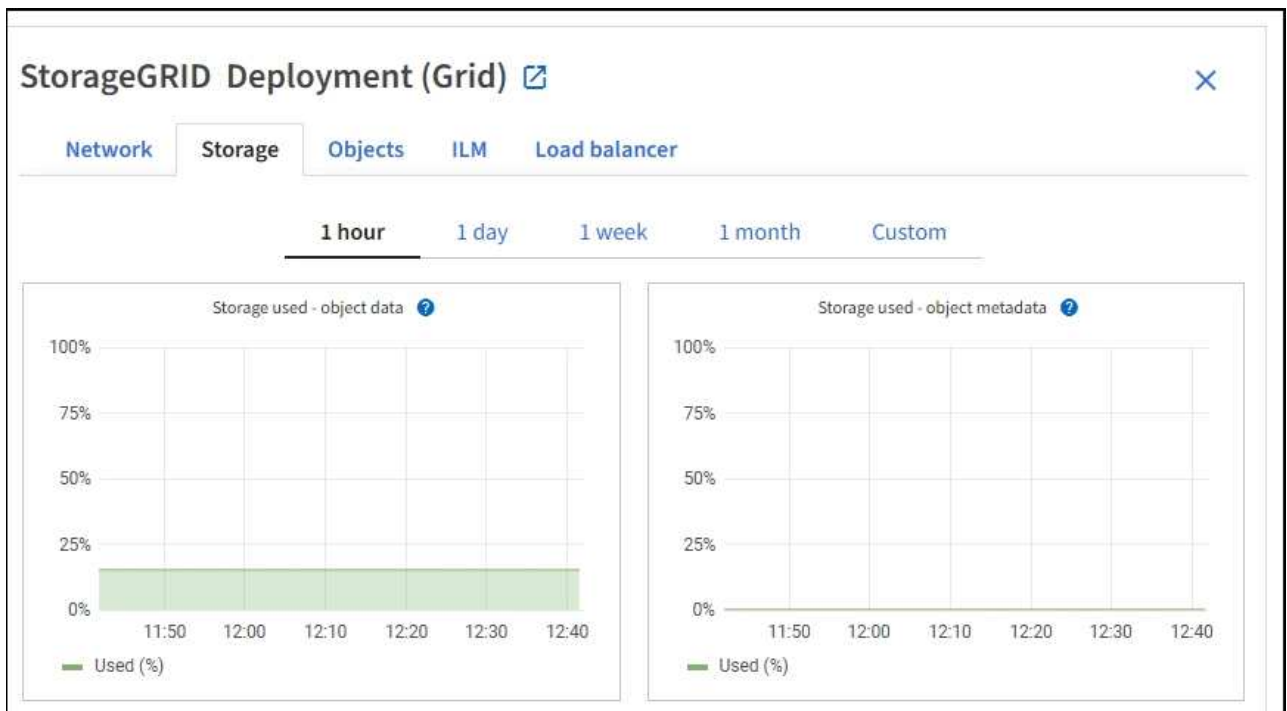
 El resumen no incluye los soportes de archivo.



- a. Fíjate en el gráfico de la ficha «Almacenamiento a lo largo del tiempo». Utiliza el menú desplegable de periodos de tiempo para ayudarte a determinar la rapidez con la que se consume el almacenamiento.



2. Utiliza la página «Nodos» para obtener más detalles sobre cuánto espacio de almacenamiento se ha utilizado y cuánto queda disponible en la grid para los datos de objetos y los metadatos de objetos.
 - a. Selecciona **Nodos**.
 - b. Selecciona **grid > Storage**.



- c. Coloca el cursor sobre los gráficos **Almacenamiento utilizado - datos de objetos** y **Almacenamiento utilizado - metadatos de objetos** para ver cuánto almacenamiento de objetos y cuánto almacenamiento de metadatos de objetos hay disponible para toda la grid, y cuánto se ha utilizado a lo largo del tiempo.



Los valores totales de un sitio o de la grid no incluyen los nodos que no hayan enviado métricas durante al menos cinco minutos, como los nodos que están fuera de línea.

3. Planifica una ampliación para añadir Storage Nodes o volúmenes de almacenamiento antes de que se consuma la capacidad de almacenamiento utilizable de la grid.

A la hora de planificar el calendario de una ampliación, ten en cuenta cuánto tiempo llevará adquirir e

instalar almacenamiento adicional.



Si tu política de ILM utiliza código de borrado, quizá prefieras ampliar la capacidad cuando los nodos de almacenamiento existentes estén llenos aproximadamente al 70 % para reducir el número de nodos que debes añadir.

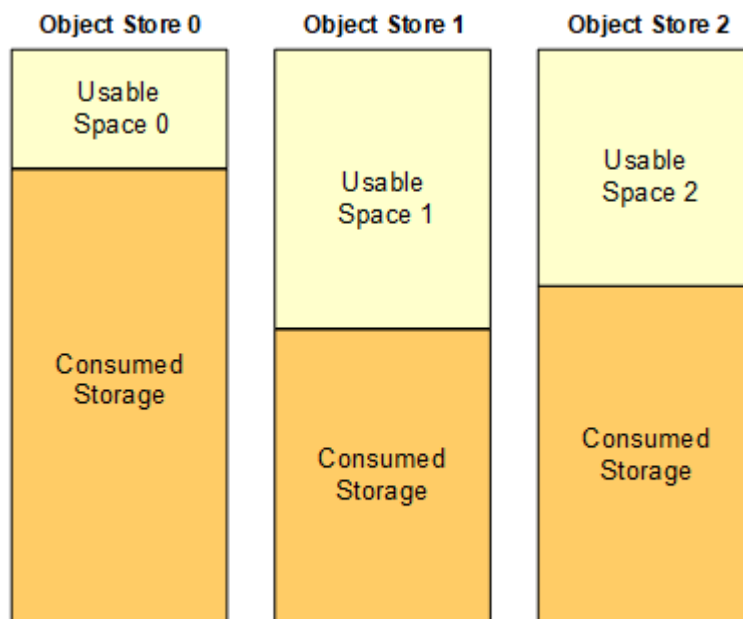
Para obtener más información sobre cómo planificar una ampliación del almacenamiento, consulta la ["Instrucciones para ampliar StorageGRID"](#).

Supervisar la capacidad de almacenamiento de cada Storage Node

Supervisa el espacio total utilizable de cada nodo de almacenamiento para asegurarte de que el nodo tenga suficiente espacio para nuevos datos de objetos.

Acerca de esta tarea

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



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

Pasos

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

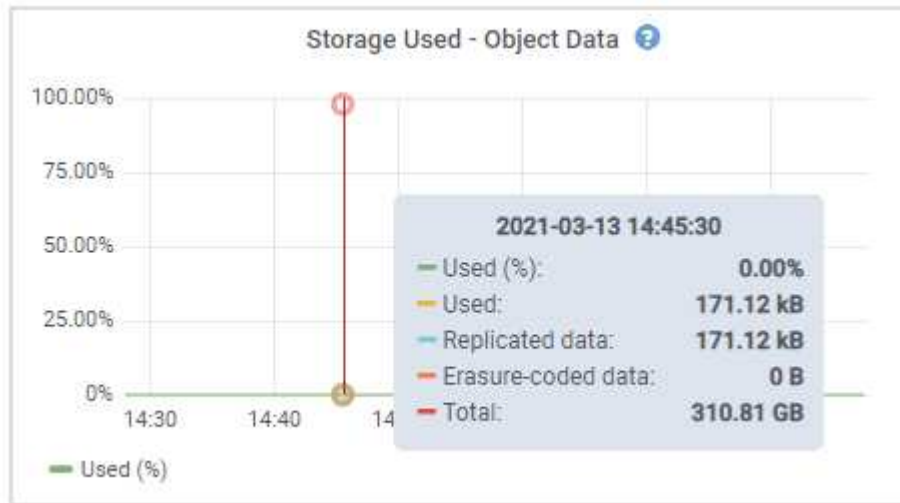
Aparecen los gráficos y las tablas correspondientes al nodo.

2. Coloca el cursor sobre el gráfico Storage used - object data.

Se muestran los siguientes valores:

- **Utilizado (%)**: el porcentaje del espacio total utilizable que se ha utilizado para datos de objetos.
- **Utilizado**: La cantidad del espacio total utilizable que se ha usado para los datos de objetos.
- **Datos replicados**: una estimación de la cantidad de datos de objetos replicados en este nodo, sitio o grid.

- **Datos con código de borrado:** Una estimación de la cantidad de datos de objetos con código de borrado en este nodo, sitio o grid.
- **Total:** La cantidad total de espacio utilizable en este nodo, sitio o grid. El valor Used es la métrica `storagegrid_storage_utilization_data_bytes`.



3. Consulta los valores disponibles en las tablas Volumes y Object stores, situadas debajo de los gráficos.



Para ver gráficos de estos valores, haz clic en los iconos 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

- Supervisa los valores a lo largo del tiempo para calcular la velocidad a la que se va consumiendo el espacio de almacenamiento utilizable.
- Para mantener el funcionamiento normal del sistema, añade Storage Nodes, añade volúmenes de almacenamiento o archiva los datos de objetos antes de que se consuma el espacio utilizable.

A la hora de planificar el calendario de una ampliación, ten en cuenta cuánto tiempo llevará adquirir e instalar almacenamiento adicional.



Si tu política de ILM utiliza código de borrado, quizá prefieras ampliar la capacidad cuando los nodos de almacenamiento existentes estén llenos aproximadamente al 70 % para reducir el número de nodos que debes añadir.

Para obtener más información sobre cómo planificar una ampliación del almacenamiento, consulta la

"Instrucciones para ampliar StorageGRID".

La alerta "[Almacenamiento de datos de objetos bajo](#)" se activa cuando queda espacio insuficiente para almacenar datos de objetos en un nodo de almacenamiento.

Supervisa la capacidad de metadatos de objetos para cada Storage Node

Supervisa el uso de metadatos de cada Storage Node para garantizar que quede espacio suficiente disponible para las operaciones esenciales de la base de datos. Debes añadir nuevos Storage Nodes en cada sitio antes de que los metadatos de los objetos superen el 100% del espacio permitido para metadatos.

Acerca de esta tarea

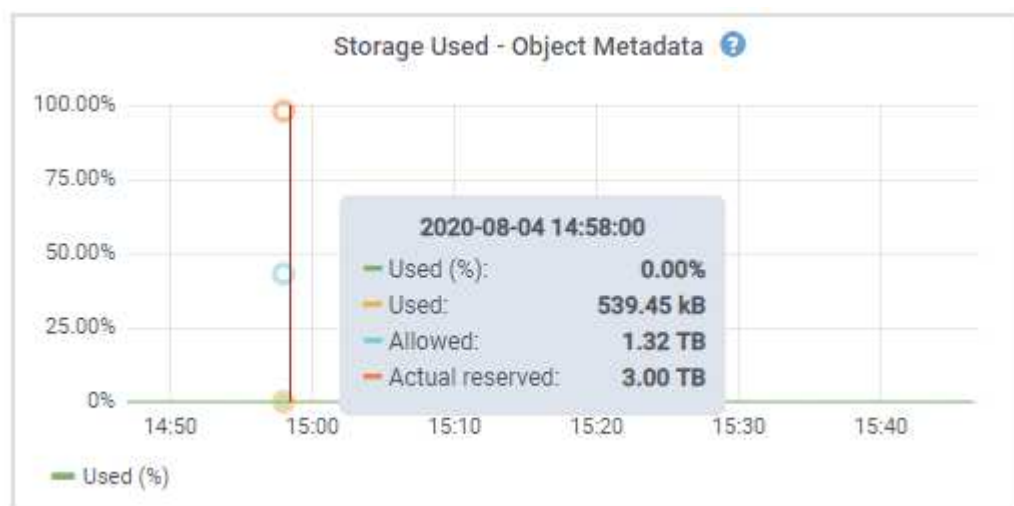
StorageGRID mantiene tres copias de los metadatos de los objetos en cada sitio para proporcionar redundancia y proteger los metadatos de los objetos contra la pérdida. Las tres copias se distribuyen de manera uniforme entre todos los Storage Nodes de cada sitio usando el espacio reservado para metadatos en el volumen de almacenamiento 0 de cada Storage Node.

En algunos casos, la capacidad de metadatos de objetos de la red puede agotarse más rápido que su capacidad de almacenamiento de objetos. Por ejemplo, si sueles incorporar grandes cantidades de objetos pequeños, puede que necesites añadir Storage Nodes para aumentar la capacidad de metadatos, aunque aún 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 de usuario, el número total de partes en una carga multiparte y la frecuencia de cambios en las ubicaciones de almacenamiento de ILM.

Pasos

1. Selecciona **Nodos > Nodo de almacenamiento > Almacenamiento**.
2. Coloca el cursor sobre el gráfico «Storage used - metadatos del objeto» para ver los valores correspondientes a un momento concreto.



Utilizado (%)

El porcentaje del espacio de metadatos permitido que se ha utilizado en este Storage Node.

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 Storage Node.

Métrica de Prometheus: `storagegrid_storage_utilization_metadata_bytes`

Permitido

El espacio disponible para los metadatos de los objetos en este Storage Node. Para saber cómo se determina este valor para cada Storage Node, consulta el ["Descripción completa del espacio de metadatos permitido"](#).

Métrica de Prometheus: `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 necesario para las operaciones esenciales de metadatos. Para saber cómo se calcula este valor para cada nodo de almacenamiento, consulta ["Descripción completa del espacio reservado para metadatos"](#).

La métrica Prometheus se añadirá en una futura versión.



Los valores totales de un sitio o de la grid no incluyen los nodos que no hayan enviado métricas durante al menos cinco minutos, como los nodos que están fuera de línea.

3. Si el valor de **Utilizado (%)** es del 70 % o superior, amplía tu sistema StorageGRID añadiendo nodos de almacenamiento a cada sitio.



La alerta **Low metadata storage** se activa cuando el valor de **Utilizado (%)** alcanza determinados umbrales. Pueden producirse resultados indeseados si los metadatos de los objetos usan más del 100% del espacio permitido.

Al añadir los nuevos nodos, el sistema reequilibra automáticamente los metadatos de los objetos entre todos los nodos de almacenamiento del sitio. Consulta ["Instrucciones para ampliar un sistema StorageGRID"](#).

Supervisa las previsiones de uso del espacio

Supervisa las previsiones de uso de espacio para los datos de los usuarios y los metadatos para estimar cuándo tendrás que ["expandir una grid"](#).

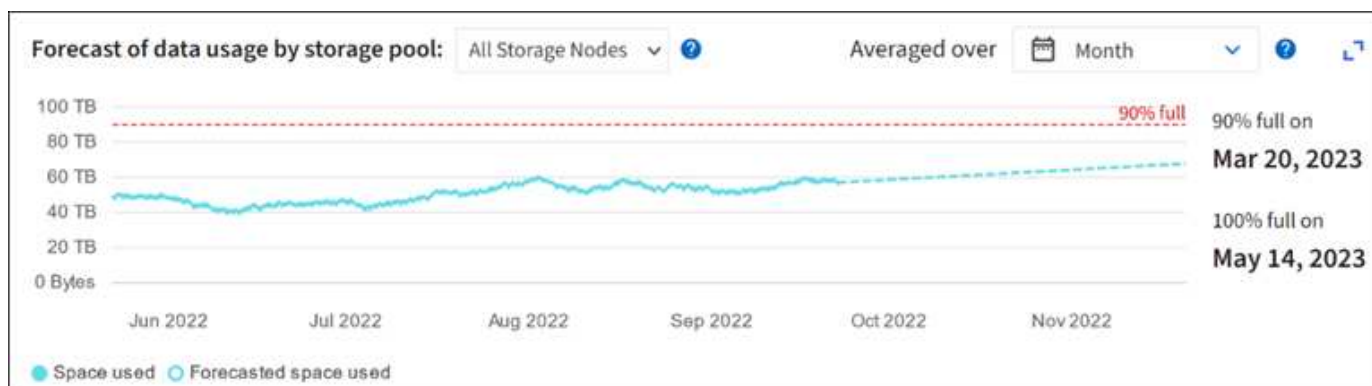
Si observas que la tasa de consumo varía con el tiempo, selecciona un intervalo más corto en el menú desplegable **Promedio sobre** para que se reflejen únicamente los patrones de ingesta más recientes. Si observas patrones estacionales, selecciona un intervalo más largo.

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

Pasos

1. En el panel de control, selecciona **Storage**.
2. Consulta las fichas del panel de control, Previsión del uso de datos por grupo de almacenamiento y Previsión del uso de metadatos por sitio.
3. Utiliza estos valores para estimar cuándo tendrás que añadir nuevos Storage Nodes para el

almacenamiento de datos y metadatos.



Supervisa la gestión del ciclo de vida de la información en StorageGRID

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

Acerca de esta tarea

El sistema StorageGRID gestiona los objetos aplicando las políticas de ILM activas. Las políticas de ILM y las reglas de ILM asociadas determinan cuántas copias se hacen, el tipo de copias que se crean, dónde se colocan las copias y cuánto tiempo se conserva cada copia.

La incorporación de objetos y otras actividades relacionadas con objetos pueden superar la tasa a la que StorageGRID puede evaluar el ILM, lo que provoca que el sistema ponga en cola los objetos cuyas instrucciones de ubicación según el ILM no se puedan cumplir casi en tiempo real. Debes supervisar si StorageGRID está manteniéndose al día con las acciones de los clientes.

Usa la pestaña de panel de control de Grid Manager

Pasos

Utiliza la pestaña ILM del panel de control de Grid Manager para supervisar las operaciones de ILM:

1. Inicia sesión en Grid Manager.
2. En el panel de control, selecciona la pestaña ILM y toma nota de los valores en la tarjeta de cola de ILM (Objetos) y en la tarjeta de tasa de evaluación de ILM.

Es normal que se produzcan picos temporales en la tarjeta «ILM queue (Objects)» del panel de control. Pero si la cola sigue aumentando y nunca disminuye, el grid necesita más recursos para operar eficientemente: ya sea más Storage Nodes o, si la política de ILM coloca los objetos en ubicaciones remotas, más ancho de banda de red.

Utiliza la página Nodes

Pasos

Además, comprueba las colas de ILM mediante la página **Nodos**:



Los gráficos de la página **Nodos** se sustituirán por las tarjetas correspondientes del panel de control en una futura versión de StorageGRID.

1. Selecciona **Nodos**.
2. Selecciona **nombre de la cuadrícula > ILM**.
3. Coloca el cursor sobre el gráfico de la cola de ILM para ver el valor de los siguientes atributos en un momento específico:
 - **Objetos en cola (por operaciones del cliente)**: el número total de objetos que están a la espera de ser evaluados por ILM debido a operaciones del cliente (por ejemplo, ingest).
 - **Objetos en cola (de todas las operaciones)**: el número total de objetos que esperan la evaluación de ILM.
 - **Frecuencia de escaneo (objetos/segundo)**: la frecuencia a la que se escanean los objetos en el grid y se ponen en cola para ILM.
 - **Tasa de evaluación (objetos/segundo)**: la tasa actual a la que se están evaluando los objetos según la política de ILM en el grid.



La sección de colas de ILM solo se incluye para el grid. Esta información no aparece en la pestaña ILM de un sitio o de un Storage Node.

4. En la sección «Cola de ILM», fíjate en los siguientes atributos.
 - **Duración del escaneo - estimada**: El tiempo estimado para completar un escaneo ILM completo de todos los objetos.



Una exploración completa no garantiza que se haya aplicado ILM a todos los objetos.

- **Intentos de reparación**: Número total de operaciones de reparación de objetos para datos replicados que se han intentado. Este recuento se incrementa cada vez que un Storage Node intenta reparar un objeto de alto riesgo. Las reparaciones ILM de alto riesgo tienen prioridad si la grid se vuelve ocupada.

El contador de reparaciones del mismo objeto podría volver a incrementarse si la replicación fallara tras la reparación. + Estos atributos pueden resultar útiles cuando estás supervisando el progreso de la recuperación de un volumen de Storage Node. Si el número de reparaciones intentadas ha dejado de aumentar y se ha completado un análisis completo, probablemente la reparación ya terminó.

5. Como alternativa, envía una consulta de Prometheus para `storagegrid_ilm_scan_period_estimated_minutes` y `storagegrid_ilm_repairs_attempted`.

Supervisa los recursos de red y del sistema en StorageGRID

La integridad y el ancho de banda de la red entre nodos y sitios, y el uso de recursos por nodos individuales de la grid, son críticos para un funcionamiento eficiente.

Supervisa las conexiones de red y el rendimiento

La conectividad de red y el ancho de banda son especialmente importantes si tu 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 ofrezca protección frente a la pérdida de un sitio. Si la red entre sitios no está disponible, la latencia de red es demasiado alta o el ancho de banda de la red es insuficiente, es posible que algunas reglas de ILM no puedan colocar los objetos donde se espera. Esto puede provocar errores de ingesta (cuando se selecciona la opción «Ingesta estricta» para las reglas de ILM) o un rendimiento deficiente de la ingesta y atascos en el ILM.

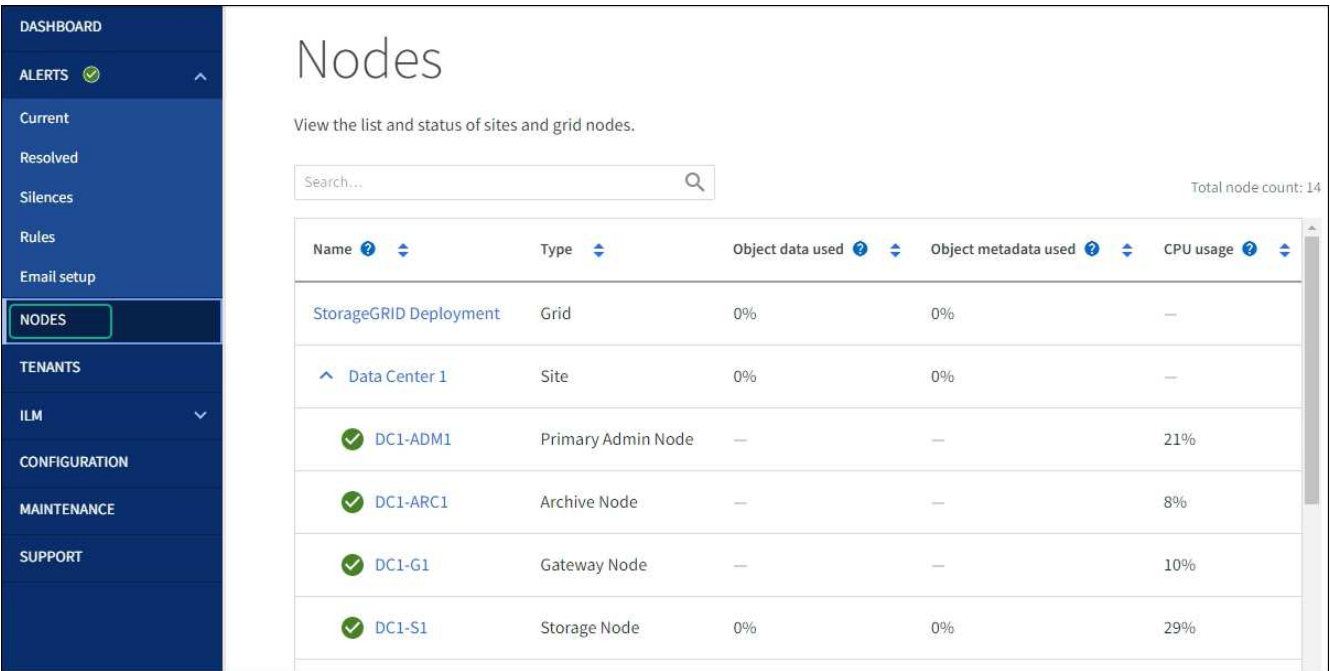
Utiliza el Grid Manager para supervisar la conectividad y el rendimiento de la red, de modo que puedas resolver cualquier problema con rapidez.

Además, considera "creación de políticas de clasificación del tráfico de red" para que puedas supervisar el tráfico relacionado con inquilinos, buckets, subredes o endpoints de balanceadores de carga específicos. Puedes establecer políticas de limitación de tráfico según sea necesario.

Pasos

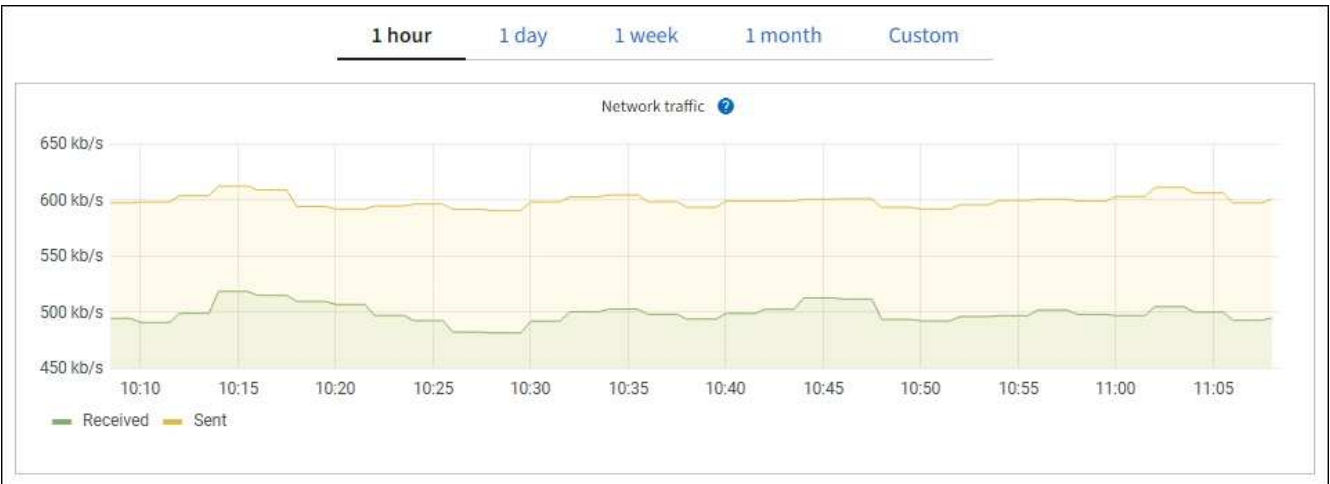
- 1. Selecciona **Nodos**.

Aparece la página «Nodos». Cada nodo de la grid se muestra en formato de tabla.



- 2. Selecciona el nombre del grid, un sitio específico del centro de datos o un nodo del grid y luego selecciona la pestaña **Red**.

El gráfico de tráfico de red ofrece un resumen del tráfico de red general para toda la grid, el sitio del centro de datos o para el nodo.



- a. Si seleccionaste un nodo de la red, desplázate hacia abajo para revisar la sección **Network Interfaces**

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. En el caso de los nodos de grid, desplázate hacia abajo para consultar la sección **Comunicación de red** de la página.

Las tablas «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. Utiliza las métricas asociadas a tus políticas de clasificación del tráfico para supervisar el tráfico de red.

- a. Selecciona **Configuración > Red > Clasificación del tráfico**.

Aparece la página «Políticas de clasificación del tráfico» y las políticas existentes se muestran en la tabla.

Traffic Classification Policies

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

+ Create Edit Remove Metrics		
Name	Description	ID
☐ ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
☒ Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bdc894b
Displaying 2 traffic classification policies.		

- a. Para ver los gráficos que muestran las métricas de red asociadas a una política, selecciona el botón de opción situado a la izquierda de la política y luego haz clic en **Métricas**.

b. Revisa los gráficos para comprender el tráfico de red asociado a la política.

Si se ha diseñado una política de clasificación del tráfico para limitar el tráfico de red, analiza con qué frecuencia se limita dicho tráfico y decide si la política sigue satisfaciendo tus necesidades. De vez en cuando, ["ajusta cada política de clasificación del tráfico según sea necesario"](#).

Información relacionada

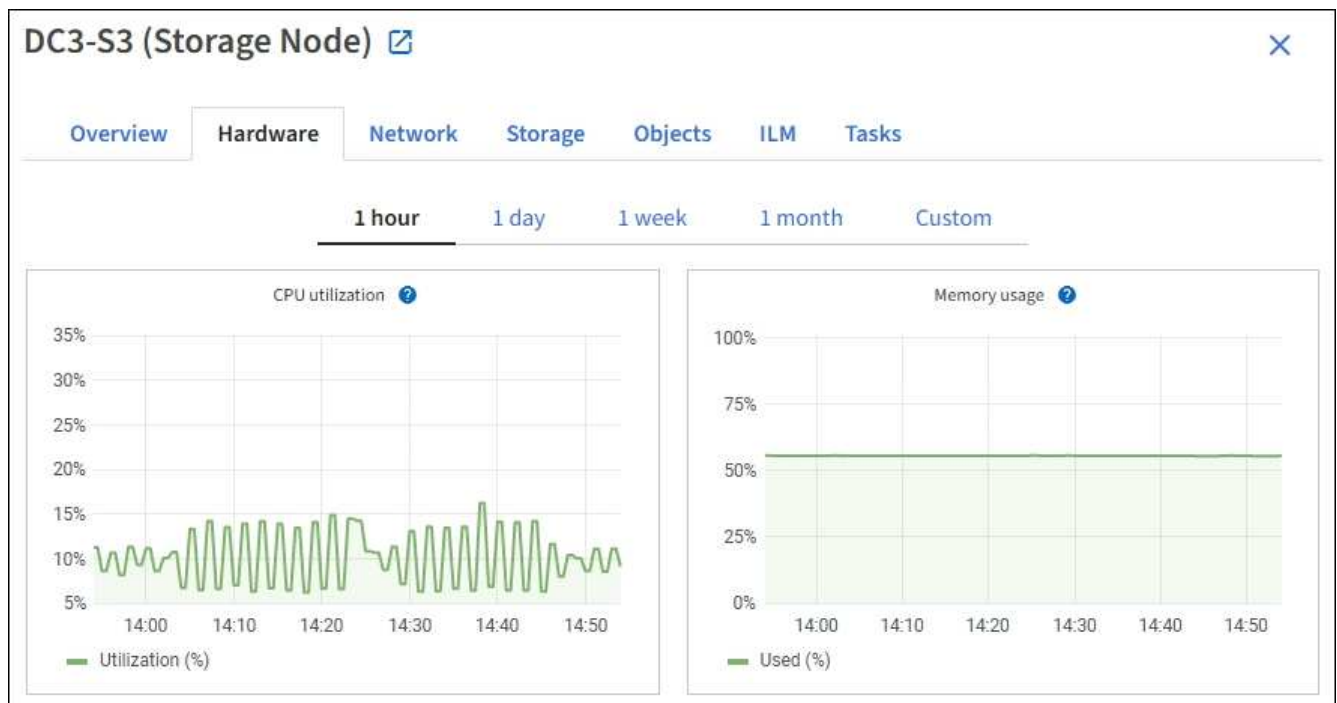
- ["Ver la pestaña Red"](#)
- ["Supervisa el estado de las conexiones de los nodos"](#)

Supervisa los recursos a nivel de nodo

Supervisa los nodos individuales de la red para comprobar sus niveles de uso de recursos. Si los nodos están constantemente sobrecargados, puede que se necesiten más nodos para que las operaciones sean eficientes.

Pasos

1. En la página **Nodos**, selecciona el nodo.
2. Selecciona la pestaña **Hardware** para ver los gráficos de utilización de CPU y uso de memoria.



3. Para visualizar un intervalo de tiempo diferente, selecciona uno de los controles situados encima del gráfico. Puedes visualizar la información disponible para intervalos de 1 hora, 1 día, 1 semana o 1 mes. También puedes establecer un intervalo personalizado, lo que te permite especificar rangos de fecha y hora.
4. Si el nodo está alojado en un dispositivo de almacenamiento o en un dispositivo de servicios, desplázate hacia abajo para ver las tablas de componentes. El estado de todos los componentes debe ser "Nominal". Investiga los componentes que tengan cualquier otro estado.

Información relacionada

- ["Ver información sobre los nodos de almacenamiento de los appliances"](#)
- ["Ver información sobre los nodos de administración y los nodos de puerta de enlace del appliance"](#)

Supervisa la actividad de los inquilinos en StorageGRID

Toda la actividad de los clientes S3 está asociada a las cuentas de los inquilinos de StorageGRID. Puedes utilizar el Grid Manager para supervisar el uso del almacenamiento o el tráfico de red de todos los inquilinos o de uno concreto. Puedes utilizar el registro de auditoría o los paneles de Grafana para recabar información más detallada sobre cómo utilizan StorageGRID los inquilinos.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Acceso raíz o permisos de cuentas de inquilino".

Ver todos los inquilinos

La página «Tenants» muestra información básica sobre todas las cuentas de tenant actuales.

Pasos

1. Selecciona **Tenants**.
2. Revisa la información que aparece en las páginas de Tenant.

Para cada inquilino se muestran el espacio lógico utilizado, el uso de la cuota, la cuota y el recuento de objetos. Si no se ha establecido una cuota para un inquilino, los campos uso de la cuota y cuota contienen un guion (—).

El tamaño lógico de todos los objetos pertenecientes a este inquilino incluye las subidas multiparte incompletas y en curso. El tamaño no incluye el espacio físico adicional utilizado para las políticas de ILM. Los valores de espacio utilizado son estimaciones. Estas estimaciones se ven afectadas por el momento en que se realizan las ingestas, la conectividad de red y el estado de los nodos.

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. Si lo deseas, inicia sesión en una cuenta de inquilino seleccionando el enlace de sign-in [→](#) en la columna **Sign in/Copiar URL**.

- Si lo deseas, copia la URL de la página de inicio de sesión de un inquilino seleccionando el enlace de copiar URL  en la columna **Sign in/Copy URL**.
- Si lo deseas, selecciona **Exportar a CSV** para ver y exportar un archivo .csv que contenga los valores de uso de todos los inquilinos.

Se te pedirá que abras o guardes el archivo .csv.

El contenido del archivo .csv es similar al del 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	1100000000	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 archivo .csv en una aplicación de hojas de cálculo o usarlo en automatización.

- Si no aparece ningún objeto en la lista, si lo deseas, selecciona **Acciones > Eliminar** para eliminar uno o varios tenants. Consulta "[Eliminar cuenta de inquilino](#)".

No puedes eliminar una cuenta de inquilino si la cuenta incluye algún bucket o contenedor.

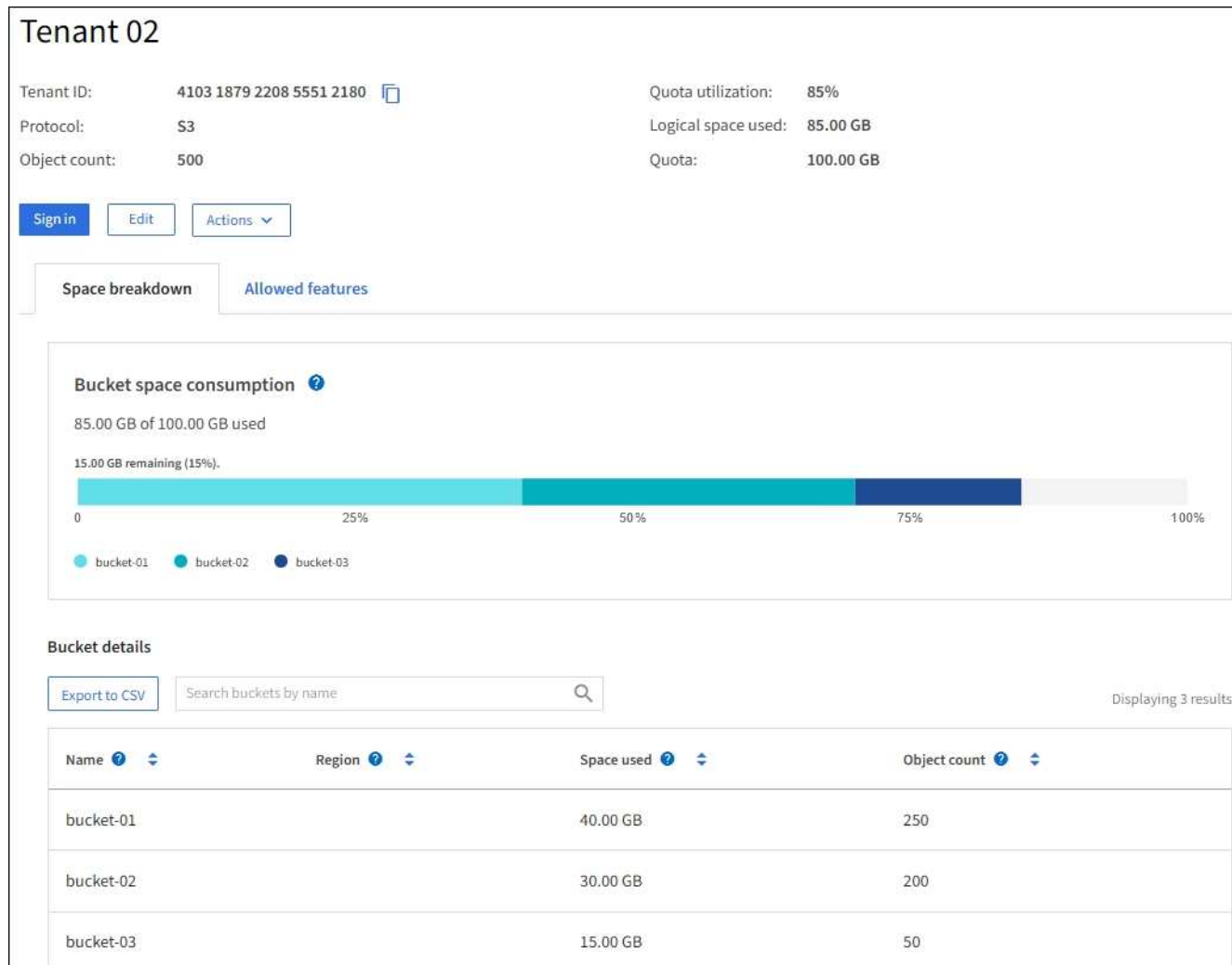
Ver un inquilino concreto

Puedes consultar los detalles de un tenant específico.

Pasos

- Selecciona el nombre del inquilino en la página Tenants.

Aparece la página de detalles del inquilino.



2. Consulta la información general sobre el inquilino que aparece en la parte superior de la página.

Esta sección de la página de detalles ofrece información resumida sobre el inquilino, incluyendo el número de objetos del inquilino, el uso de la cuota, el espacio lógico utilizado y la configuración de la cuota.



El tamaño lógico de todos los objetos pertenecientes a este inquilino incluye las subidas multiparte incompletas y en curso. El tamaño no incluye el espacio físico adicional utilizado para las políticas de ILM. Los valores de espacio utilizado son estimaciones. Estas estimaciones se ven afectadas por el momento en que se realizan las ingestas, la conectividad de red y el estado de los nodos.

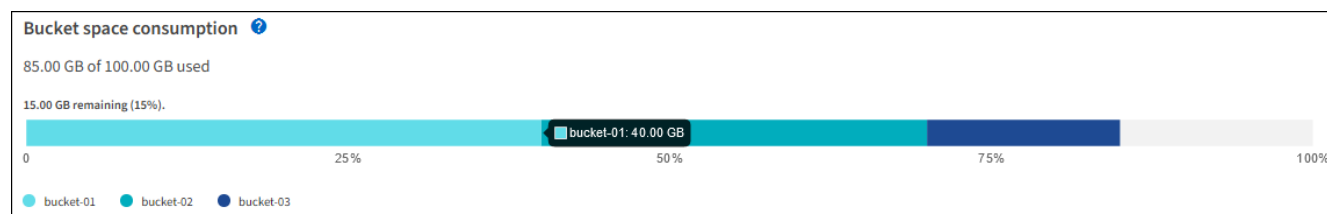
3. En la pestaña **Desglose de espacio**, revisa el gráfico **Consumo de espacio**.

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

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

Puedes situar el cursor sobre el gráfico de barras para ver el almacenamiento utilizado por cada bucket o

contenedor. Puedes situar 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 comprueba la cuota cuando un inquilino comienza a cargar objetos y rechaza nuevas cargas si el inquilino ha superado la cuota. Sin embargo, StorageGRID no tiene en cuenta el tamaño de la carga actual al determinar si se ha superado la cuota. Si se eliminan objetos, es posible que temporalmente se impida al inquilino cargar nuevos objetos hasta que se recalcule el uso de la cuota. El cálculo del uso de la cuota puede tardar 10 minutos o más.



El uso de la 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 dichos objetos y sus metadatos (tamaño físico).



Puedes activar la regla de alerta **Alto consumo de cuota del inquilino** para determinar si los inquilinos están consumiendo sus cuotas. Si está activada, esta alerta se activa cuando un inquilino ha usado el 90 % de su cuota. Para obtener instrucciones, consulta ["Editar reglas de alertas"](#).

4. En la pestaña **Desglose de espacio**, revisa los **detalles del bucket**.

Esta tabla muestra los buckets de S3 del inquilino. El espacio utilizado es la cantidad total de datos de los objetos que hay en el bucket o contenedor. Este valor no representa el espacio de almacenamiento necesario para las copias de ILM ni los metadatos de los objetos.

5. Si lo deseas, selecciona **Exportar a CSV** para ver y exportar un archivo .csv que contenga los valores de uso de cada bucket o contenedor.

El contenido de un archivo de S3 de un inquilino individual .csv tiene el siguiente aspecto:

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 archivo .csv en una aplicación de hojas de cálculo o usarlo en automatización.

- Si lo deseas, selecciona la pestaña **Funciones permitidas** para ver una lista de los permisos y las funciones que están habilitados para el inquilino. Consulta ["Editar cuenta de inquilino"](#) si necesitas modificar alguna de estas configuraciones.
- Si el usuario tiene el permiso **Utilizar conexión de federación de Grid**, opcionalmente selecciona la pestaña **Federación de Grid** para saber más sobre la conexión.

Consulta "[¿Qué es la federación de grid?](#)" y "[Gestiona los inquilinos permitidos para la federación de grid](#)".

Ver el tráfico de red

Si se han establecido políticas de clasificación del tráfico para un inquilino, revisa el tráfico de red de dicho inquilino.

Pasos

1. Selecciona **Configuración > Red > Clasificación del tráfico**.

Aparece la página «Políticas de clasificación del tráfico» y las políticas existentes se muestran en la tabla.

2. Revisa la lista de políticas para identificar aquellas que se aplican a un tenant específico.
3. Para ver las métricas asociadas a una política, selecciona el botón de opción situado a la izquierda de la política y selecciona **Métricas**.
4. Analiza los gráficos para determinar con qué frecuencia la política está limitando el tráfico y si necesitas ajustar la política.

Consulta "[Gestiona las políticas de clasificación del tráfico](#)" para más información.

Utiliza el registro de auditoría

Si lo deseas, puedes utilizar el registro de auditoría para realizar un seguimiento con mayor granularidad de las actividades de un tenant.

Por ejemplo, puedes supervisar los siguientes tipos de información:

- Operaciones específicas del cliente, como PUT, GET o DELETE
- Tamaños de los objetos
- La regla ILM aplicada a los objetos
- La dirección IP de origen de las solicitudes de los clientes

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

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

Usa métricas de Prometheus

Si lo deseas, puedes utilizar las métricas de Prometheus para generar informes sobre la actividad de los inquilinos.

- En el Grid Manager, selecciona **Soporte > Herramientas > Métricas**. Puedes utilizar los paneles de control existentes, como S3 Overview, para revisar las actividades de los clientes.



Las herramientas disponibles en la página de Métricas están destinadas principalmente al soporte técnico. Algunas funciones y opciones de menú de estas herramientas no están operativas de forma intencionada.

- En la parte superior de Grid Manager, selecciona el icono de ayuda y elige **API documentation**. Puedes utilizar las métricas de la sección de métricas de la Grid Management API para crear reglas de alerta

personalizadas y paneles de control para la actividad de los tenants.

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

Supervisa las operaciones del cliente S3 en StorageGRID

Puedes supervisar las tasas de consumo y recuperación de objetos, así como las métricas relativas al recuento de objetos, las consultas y la verificación. Puedes ver el número de intentos exitosos y fallidos de las aplicaciones cliente para leer, escribir y modificar objetos en el sistema StorageGRID.

Antes de empezar

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

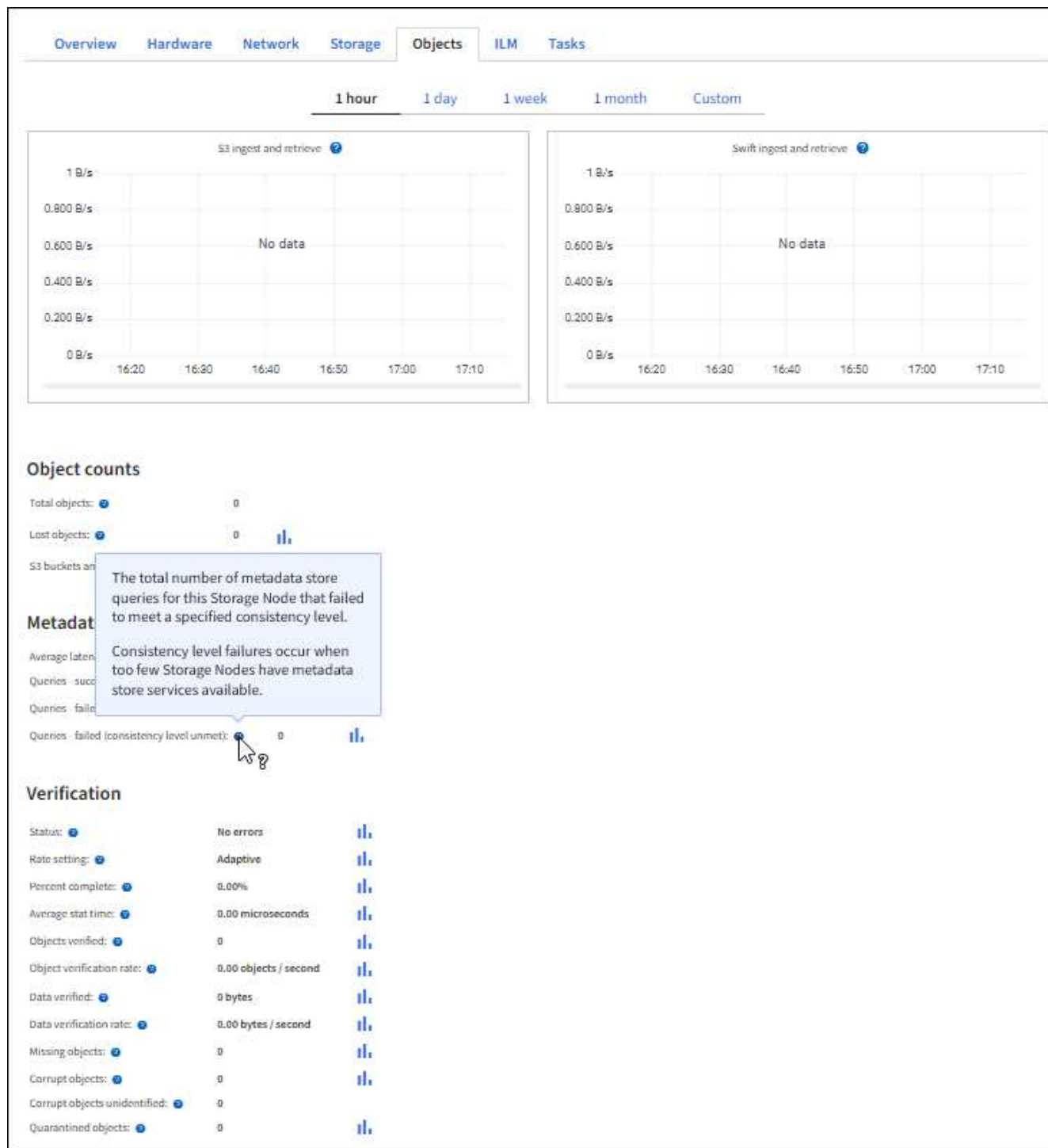
Pasos

1. Desde el panel de control, selecciona la pestaña **Performance**.
2. Consulta los gráficos de S3, que resumen el número de operaciones de cliente realizadas por los nodos de almacenamiento y el número de solicitudes de API recibidas por los nodos de almacenamiento durante el periodo seleccionado.
3. Selecciona **Nodos** para acceder a la página de Nodos.
4. En la página de inicio de Nodes (nivel de grid), selecciona la pestaña **Objects**.

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

5. Para consultar la información de un nodo de almacenamiento concreto, selecciona el nodo en la lista de la izquierda y selecciona la pestaña **Objetos**.

El gráfico muestra las tasas de ingestión y recuperación del nodo. La pestaña también incluye métricas sobre el recuento de objetos, las consultas de metadatos y las operaciones de verificación.



Supervisa las operaciones de equilibrio de carga en StorageGRID

Si utilizas un equilibrador de carga para gestionar las conexiones de los clientes a StorageGRID, debes supervisar las operaciones de equilibrio de carga tras la configuración inicial del sistema y cada vez que realices cambios en la configuración o lles a cabo una ampliación.

Acerca de esta tarea

Puedes utilizar el servicio de Load Balancer en los Admin Nodes o Gateway Nodes, o un equilibrador de carga externo de terceros, para distribuir las solicitudes de los clientes entre varios Storage Nodes.

Tras configurar el equilibrio de carga, debes comprobar que las operaciones de ingesta y recuperación de objetos se distribuyen de manera uniforme entre los Storage Nodes. Una distribución uniforme de las solicitudes garantiza que StorageGRID siga siendo capaz de responder a las solicitudes de los clientes bajo carga y puede ayudar a mantener el rendimiento para los clientes.

Si configuraste un grupo de alta disponibilidad (HA) de Gateway Nodes o Admin Nodes en modo activo-backup, solo un nodo del grupo distribuye activamente las solicitudes de los clientes.

Para más información, consulta ["Configura las conexiones del cliente S3"](#).

Pasos

1. Si los clientes de S3 se conectan mediante el servicio Load Balancer, comprueba que los nodos de administración o los nodos de puerta de enlace estén distribuyendo el tráfico como esperas:
 - a. Selecciona **Nodos**.
 - b. Selecciona un nodo de puerta de enlace o un nodo de administración.
 - c. En la pestaña **Resumen**, comprueba si una interfaz de nodo está en un grupo de alta disponibilidad y si la interfaz de nodo tiene el rol de Primary.

Los nodos con el rol de Primary y los nodos que no están en un grupo de HA deben estar distribuyendo activamente solicitudes a los clientes.

- d. Para cada nodo que deba distribuir activamente las solicitudes de los clientes, selecciona ["Pestaña Load Balancer"](#).
- e. Revisa el gráfico de tráfico de solicitudes del equilibrador de carga de la última semana para asegurarte de que el nodo ha estado distribuyendo activamente solicitudes.

Los nodos de un grupo de alta disponibilidad (HA) de tipo activo-backup pueden asumir el rol de Backup de vez en cuando. Durante ese tiempo los nodos no distribuyen las solicitudes de los clientes.
- f. Consulta el gráfico de la tasa de solicitudes entrantes del equilibrador de carga de la última semana para revisar el rendimiento de objetos del nodo.
- g. Repite estos pasos para cada nodo de administración o nodo de puerta de enlace en el sistema StorageGRID.
- h. Opcionalmente, usa las políticas de clasificación de tráfico para ver un análisis más detallado del tráfico que está siendo atendido por el servicio Load Balancer.

2. Comprueba que estas solicitudes se distribuyen de manera uniforme entre los nodos de almacenamiento.
 - a. Selecciona **Storage Node > LDR > HTTP**.
 - b. Comprueba el número de **sesiones entrantes actualmente establecidas**.
 - c. Repite este proceso para cada Storage Node en la grid.

El número de sesiones debería ser más o menos el mismo en todos los Storage Nodes.

Supervisa las conexiones de federación de grid de StorageGRID

Puedes supervisar información básica sobre todas ["conexiones de federación de grid"](#), información detallada sobre una conexión concreta o métricas de Prometheus sobre las operaciones de replicación entre grids. Puedes supervisar una conexión desde cualquiera de los dos grids.

Antes de empezar

- Has iniciado sesión en el Grid Manager de cualquiera de las dos grids usando un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#) de la grid en la que has iniciado sesión.

Ver todas las conexiones

La página de la federación de Grid muestra información básica sobre todas las conexiones de la federación de Grid y sobre todas las cuentas de inquilinos a las que se les permite utilizar conexiones de federación de Grid.

Pasos

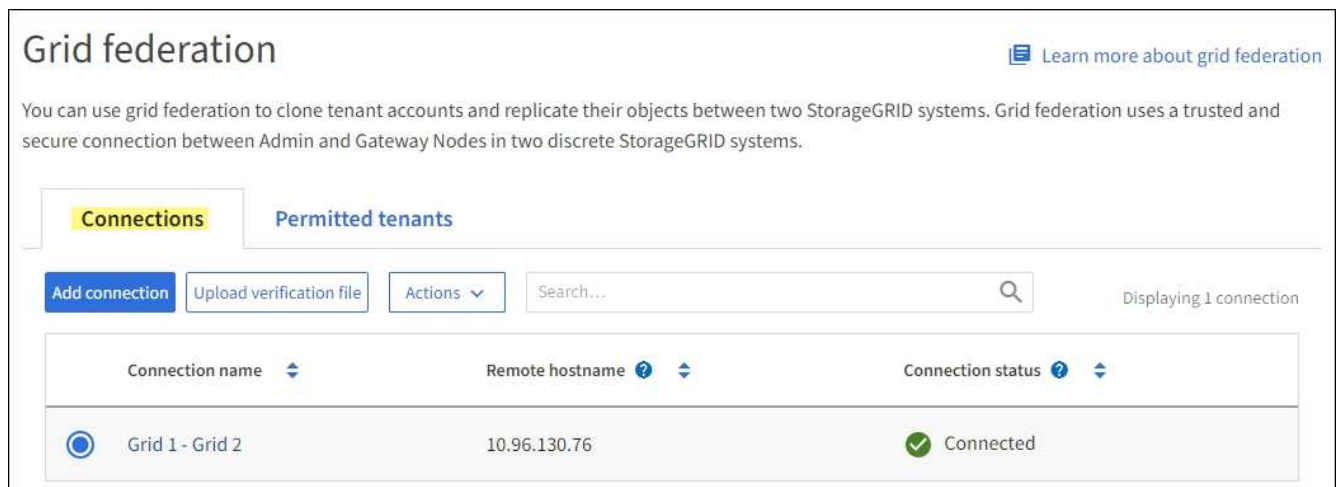
1. Selecciona **Configuración > Sistema > Grid federation**.

Aparece la página de la federación de Grid.

2. Para ver la información básica de todas las conexiones en esta grid, selecciona la pestaña **Conexiones**.

Desde esta pestaña, puedes:

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



The screenshot shows the 'Grid federation' page. At the top, there's a header with the title 'Grid federation' and a link 'Learn more about grid federation'. Below the header, a descriptive paragraph explains that grid federation is used to clone tenant accounts and replicate objects between two StorageGRID systems. The main content area has two tabs: 'Connections' (active) and 'Permitted tenants'. Under the 'Connections' tab, there are buttons for 'Add connection', 'Upload verification file', and 'Actions', along with a search bar. A table displays the connections, with one entry visible: 'Grid 1 - Grid 2' with a remote hostname of '10.96.130.76' and a status of 'Connected'.

Connection name	Remote hostname	Connection status
Grid 1 - Grid 2	10.96.130.76	Connected

3. Para ver la información básica de todas las cuentas de inquilinos de esta grid que tengan el permiso **Usar conexión de federación de grid**, selecciona la pestaña **Inquilinos autorizados**.

Desde esta pestaña, puedes:

- ["Consulta la página de detalles de cada inquilino permitido"](#).
- Consulta la página de detalles de cada conexión. Consulta [Ver una conexión concreta](#).
- Selecciona un inquilino autorizado y ["eliminar el permiso"](#).
- Comprueba si hay errores de replicación entre redes y elimina el último error, si lo hay. Consulta ["Solucionar errores de federación de grid"](#).

Grid federation [Learn more about grid federation](#)

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

[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

Puedes consultar los detalles de una conexión específica de la federación de grids.

Pasos

1. Selecciona cualquiera de las pestañas de la página Grid federation y luego selecciona el nombre de la conexión en la tabla.

Desde la página de detalles de la conexión, puedes:

- Consulta la información básica sobre el estado de la conexión, incluidos los nombres de host local y remoto, el puerto y el estado de la conexión.
 - Selecciona una conexión a ["editar, probar o eliminar"](#).
2. Al consultar una conexión concreta, selecciona la pestaña **Inquilinos autorizados** para ver los detalles sobre los inquilinos autorizados para esa conexión.

Desde esta pestaña, puedes:

- ["Consulta la página de detalles de cada inquilino permitido"](#).
- ["Quitar el permiso a un inquilino"](#) para usar la conexión.
- Comprueba si hay errores de replicación entre grids y elimina el último error. Consulta ["Solucionar errores de federación de grid"](#).

Grid 1 - Grid 2

Local hostname (this grid): 10.96.130.64

Port: 23000

Remote hostname (other grid): 10.96.130.76

Connection status: ✔ Connected

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

Permitted tenants

Certificates

[Remove permission](#)
[Clear error](#)

Displaying one result

Tenant name	Last error
☒ Tenant A	Check for errors

- Al visualizar una conexión concreta, selecciona la pestaña **Certificados** para ver los certificados de servidor y de cliente generados por el sistema para dicha conexión.

Desde esta pestaña, puedes:

- ["Rotar los certificados de conexión"](#).
- Selecciona **Server** o **Client** para ver o descargar el certificado correspondiente o copiar el certificado PEM.

Grid A-Grid B

Local hostname (this grid):10.96.106.230

Port:23000

Remote hostname (other grid):10.96.104.230

Connection status:

Connected

Edit

Download file

Test connection

Remove

Permitted tenants

Certificates

Rotate certificates

Server

Client

Download certificate

Copy certificate PEM

Metadata

Subject DN:/C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=10.96.106.230

Serial number:30:81:B8:DD:AE:B2:86:0A

Issuer DN:/C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=GPT

Issued on:2022-10-04T02:21:18.000Z

Expires on:2024-10-03T19:05:13.000Z

SHA-1 fingerprint:92:7A:03:AF:6D:1C:94:8C:33:24:08:84:F9:2B:01:23:7D:BE:F2:DF

SHA-256 fingerprint:54:97:3E:77:EB:D3:6A:0F:8F:EE:72:83:D0:39:86:02:32:A5:60:9D:6F:C0:A2:3C:76:DA:3F:4D:FF:64:5D:60

Alternative names:IP Address:10.96.106.230

Certificate PEM

-----BEGIN CERTIFICATE-----

MIIGdTCCBF2gAwIBAgIIMIG43a6yhgowDQYJKoZIhvcNAQENBQAwdzELMAkGA1UE

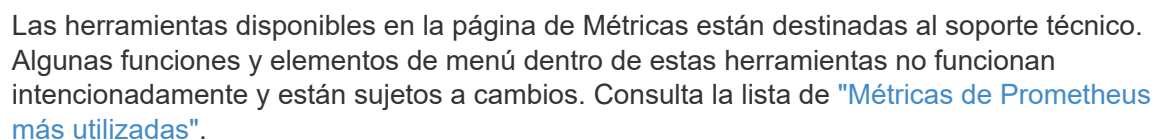
BhMCVVMhxEzARBgNVBAGhNCKNhbg1mb3JuaWExEjAQBgNVBACgMCVN1bm55dmFsZTEU

MBEFCgY5ZGVldjE1Lm55dmFsZTEU

-----END CERTIFICATE-----

Puedes usar el panel de Cross-Grid Replication en Grafana para ver las métricas de Prometheus sobre las operaciones de replicación entre grids en tu grid.

1. En el Grid Manager, selecciona **Soporte** > **Herramientas** > **Métricas**.



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

3. Para volver a intentar la replicación de los objetos cuya replicación ha fallado, consulta ["Identifica y vuelve a intentar las operaciones de replicación que hayan fallado"](#).

Gestiona alertas

Administra alertas en StorageGRID

El sistema de alertas ofrece una interfaz fácil de usar para detectar, evaluar y resolver los problemas que pueden surgir 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, ocurren las siguientes acciones:

- En el panel de control de Grid Manager aparece un icono de gravedad de alerta y el recuento de Alertas actuales se incrementa.
- La alerta se muestra en la página de resumen **Nodos** y en la pestaña **Nodos > node > Overview**.
- Se envía una notificación por correo electrónico, siempre que hayas configurado un servidor SMTP y hayas indicado las direcciones de correo electrónico de los destinatarios.
- Se envía una notificación del Protocolo simple de gestión de redes (SNMP), siempre que hayas configurado el agente SNMP de StorageGRID.

Puedes crear alertas personalizadas, editar o desactivar alertas, y gestionar las notificaciones de alertas.

Para obtener más información:

- Echa un vistazo a los vídeos:

[Resumen de alertas](#)

[Alertas personalizadas](#)

- Consulta el ["Referencia de alertas"](#).

Ver las reglas de alerta de StorageGRID

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

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

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

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Gestiona alertas o permisos de acceso root"](#).
- Opcionalmente, has visto el vídeo:

[Resumen de alertas](#)

Pasos

1. Selecciona **Alertas > Reglas**.

Aparece la página Alert Rules.

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. Revisa la información en la tabla de reglas de alertas:

Encabezado de columna	Descripción
Nombre	El nombre y la descripción únicos de la regla de alerta. Las reglas de alerta personalizadas aparecen en primer lugar, seguidas de las reglas de alerta predeterminadas. El nombre de la regla de alerta es el asunto de las notificaciones por correo electrónico.

Encabezado de columna	Descripción
Condiciones	Las expresiones de Prometheus que determinan cuándo se activa esta alerta. Una alerta puede activarse en uno o varios de los siguientes niveles de gravedad, pero no es necesario que se cumpla una condición para cada gravedad. • Crítico : Existe una situación anómala que ha detenido las operaciones normales de un nodo o servicio de StorageGRID. Debes solucionar el problema subyacente de inmediato. Si no resuelves el problema, podría haber interrupciones en el servicio y pérdida de datos. • Grave : existe una situación anómala que está afectando el funcionamiento actual o que se está acercando al umbral de una alerta crítica. Deberías investigar las alertas graves y resolver cualquier problema subyacente para asegurarte de que la situación anómala no detenga el funcionamiento normal de un nodo o servicio de StorageGRID. • Menor : El sistema está funcionando con normalidad, pero existe una condición anómala que podría afectar la capacidad del sistema para operar si continúa. Deberías supervisar y resolver las alertas menores que no se resuelvan por sí solas para asegurarte de que no resulten en un problema más grave.
Tipo	El tipo de regla de alerta: • Predeterminada: Una regla de alerta incluida en el sistema. Puedes desactivar una regla de alerta predeterminada o editar las condiciones y la duración de una regla de alerta predeterminada. No puedes eliminar una regla de alerta predeterminada. • Predeterminada*: Una regla de alerta predeterminada que incluye una condición o una duración modificadas. Si es necesario, puedes restablecer fácilmente una condición modificada a su valor predeterminado original. • Personalizada: Una regla de alerta que creaste tú. Puedes desactivar, editar y eliminar reglas de alerta personalizadas.
Estado	Si esta regla de alerta está activada o desactivada actualmente. Las condiciones de las reglas de alerta desactivadas no se evalúan, así que no se activan alertas.

Crea reglas de alerta personalizadas en StorageGRID

Puedes crear reglas de alerta personalizadas para definir tus propias condiciones para activar alertas.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Gestiona alertas o permisos de acceso root"](#).

- Seguro que conoces el "[Métricas de Prometheus más utilizadas](#)".
- Entiendes el "[Sintaxis de las consultas de Prometheus](#)".
- Opcionalmente, has visto el vídeo:

[Alertas personalizadas](#)

Acerca de esta tarea

StorageGRID no valida las alertas personalizadas. Si decides crear reglas de alerta personalizadas, sigue estas directrices generales:

- Echa un vistazo a las condiciones de las reglas de alerta predeterminadas y utilízalas como ejemplos para tus reglas de alerta personalizadas.
- Si defines más de una condición para una regla de alerta, utiliza la misma expresión para todas las condiciones. Luego, cambia el valor umbral de cada condición.
- Revisa con atención cada condición para detectar posibles errores ortográficos y de lógica.
- Utiliza únicamente las métricas que figuran en la Grid Management API.
- Al probar una expresión mediante la API de gestión de cuadrículas, ten en cuenta que una respuesta "correcta" puede consistir en un cuerpo de respuesta vacío (sin que se active ninguna alerta). Para ver si la alerta realmente se activa, puedes establecer temporalmente un umbral en un valor que esperas que sea verdadero en este momento.

Por ejemplo, para probar la expresión `node_memory_MemTotal_bytes < 24000000000`, primero ejecuta `node_memory_MemTotal_bytes >= 0` y asegúrate de que obtienes los resultados esperados (todos los nodos devuelven un valor). Luego, cambia el operador y el umbral a los valores previstos y ejecuta de nuevo. Si no hay resultados, significa que no hay alertas actuales para esta expresión.

- No des por sentado que una alerta personalizada funciona a menos que hayas comprobado que se activa en el momento previsto.

Pasos

1. Selecciona **Alertas > Reglas**.

Aparece la página Alert Rules.

2. Selecciona **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. Marca o desmarca la casilla **Habilitado** para determinar si esta regla de alerta está habilitada actualmente.

Si una regla de alerta está desactivada, sus expresiones no se evalúan y no se activan alertas.

4. Ingresar la siguiente información:

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

Campo	Descripción
Descripción	Una descripción del problema que se está produciendo. La descripción es el mensaje de alerta que aparece en la página Alertas y en las notificaciones por correo electrónico. Las descripciones de las reglas de alerta pueden tener entre 1 y 128 caracteres.
Medidas recomendadas	Opcionalmente, las acciones recomendadas que debes llevar a cabo cuando se active esta alerta. Introduce las acciones recomendadas como texto sin formato (sin códigos de formato). Las acciones recomendadas para las reglas de alerta pueden tener entre 0 y 1,024 caracteres.

- En la sección Condiciones, introduce una expresión de Prometheus para uno o más de los niveles de gravedad de las alertas.

Una expresión básica suele tener la forma:

```
[metric] [operator] [value]
```

Las expresiones pueden tener cualquier longitud, pero se muestran 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 en un nodo es inferior a 24,000,000,000 bytes (24 GB).

```
node_memory_MemTotal_bytes < 24000000000
```

Para ver las métricas disponibles y probar expresiones de Prometheus, selecciona el icono de ayuda  y sigue el enlace a la sección Metrics de la Grid Management API.

- En el campo **Duración**, introduce el tiempo durante el que una condición debe permanecer vigente de forma ininterrumpida antes de que se active la alerta y selecciona una unidad de tiempo.

Para activar una alerta de forma inmediata cuando se cumpla una condición, introduce **0**. Aumenta este valor para evitar que las condiciones temporales activen alertas.

El valor predeterminado es 5 minutos.

- Selecciona **Guardar**.

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

Edita las reglas de alerta en StorageGRID

Puedes editar una regla de alerta para modificar las condiciones de activación. En el caso de una regla de alerta personalizada, también puedes actualizar el nombre de la regla, la descripción y las acciones recomendadas.

Antes de empezar

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

- Tienes el "[Gestiona alertas o permisos de acceso root](#)".

Acerca de esta tarea

Al editar una regla de alerta predeterminada, puedes cambiar las condiciones para las alertas de gravedad menor, mayor y crítica, y la duración. Al editar una regla de alerta personalizada, también puedes editar el nombre, la descripción y las acciones recomendadas de la regla.



Ten cuidado a la hora de editar una regla de alerta. Si modificas los valores de activación, es posible que no detectes un problema subyacente hasta que este impida que se complete una operación crítica.

Pasos

1. Selecciona **Alertas > Reglas**.

Aparece la página Alert Rules.

2. Selecciona el botón de opción correspondiente a la regla de alerta que quieras editar.
3. Selecciona **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 desactivados 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. Marca o desmarca la casilla **Habilitado** para determinar si esta regla de alerta está habilitada actualmente.

Si una regla de alerta está desactivada, sus expresiones no se evalúan y no se activan alertas.



Si desactivas la regla de alerta de una alerta actual, debes esperar unos minutos para que la alerta deje de aparecer como alerta activa.



En general, no se recomienda desactivar una regla de alerta predeterminada. Si desactivas una regla de alerta, podrías no detectar un problema subyacente hasta que impida que se complete una operación crítica.

5. Para las reglas de alerta personalizadas, actualiza 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 aparece en la página Alertas y también es el asunto de las notificaciones por correo electrónico. Los nombres de las reglas de alerta pueden tener entre 1 y 64 caracteres.
Descripción	Una descripción del problema que se está produciendo. La descripción es el mensaje de alerta que aparece en la página Alertas y en las notificaciones por correo electrónico. Las descripciones de las reglas de alerta pueden tener entre 1 y 128 caracteres.
Medidas recomendadas	Opcionalmente, las acciones recomendadas que debes llevar a cabo cuando se active esta alerta. Introduce las acciones recomendadas como texto sin formato (sin códigos de formato). Las acciones recomendadas para las reglas de alerta pueden tener entre 0 y 1,024 caracteres.

6. En la sección Condiciones, introduce o actualiza la expresión de Prometheus para uno o más de los niveles de gravedad de las alertas.



Si quieres restablecer el valor original de una condición de una regla de alerta predeterminada que hayas modificado, selecciona los tres puntos situados a la derecha de la condición modificada.

Conditions ?

Minor	
Major	node_memory_MemTotal_bytes < 24000000000
Critical	node_memory_MemTotal_bytes <= 14000000000



Si actualizas las condiciones de una alerta activa, es posible que los cambios no se apliquen 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 se muestran 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 en un nodo es inferior a 24,000,000,000 bytes (24 GB).

```
node_memory_MemTotal_bytes < 24000000000
```

7. En el campo **Duración**, introduce el tiempo durante el que una condición debe permanecer vigente de forma ininterrumpida antes de que se active la alerta y selecciona la unidad de tiempo.

Para activar una alerta de forma inmediata cuando se cumpla una condición, introduce **0**. Aumenta este valor para evitar que las condiciones temporales activen alertas.

El valor predeterminado es 5 minutos.

8. Selecciona **Guardar**.

Si editaste una regla de alerta predeterminada, **Default** aparece en la columna Tipo. Si desactivaste una regla de alerta predeterminada o personalizada, **Disabled** aparece en la columna **Status**.

Desactiva las reglas de alerta en StorageGRID

Puedes cambiar el estado de activación o desactivación de una regla de alerta predeterminada o personalizada.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Gestiona alertas o permisos de acceso root"](#).

Acerca de esta tarea

Cuando se desactiva una regla de alerta, sus expresiones no se evalúan y no se activan alertas.



En general, no se recomienda desactivar una regla de alerta predeterminada. Si desactivas una regla de alerta, podrías no detectar un problema subyacente hasta que impida que se complete una operación crítica.

Pasos

1. Selecciona **Alertas > Reglas**.

Aparece la página Alert Rules.

2. Selecciona el botón de opción correspondiente a la regla de alerta que quieras desactivar o activar.

3. Selecciona **Editar regla**.

Aparece el cuadro de diálogo «Editar regla».

4. Marca o desmarca la casilla **Habilitado** para determinar si esta regla de alerta está habilitada actualmente.

Si una regla de alerta está desactivada, sus expresiones no se evalúan y no se activan alertas.



Si desactivas la regla de alerta de una alerta actual, debes esperar unos minutos para que la alerta deje de mostrarse como activa.

5. Selecciona **Guardar**.

Desactivado aparece en la columna **Estado**.

Eliminar reglas de alerta personalizadas en StorageGRID

Puedes eliminar una regla de alerta personalizada si ya no quieres utilizarla.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Gestiona alertas o permisos de acceso root"](#).

Pasos

1. Selecciona **Alertas > Reglas**.

Aparece la página Alert Rules.

2. Selecciona el botón de opción correspondiente a la regla de alerta personalizada que quieras eliminar.

No puedes eliminar una regla de alerta predeterminada.

3. Selecciona **Eliminar regla personalizada**.

Aparece un cuadro de diálogo de confirmación.

4. Selecciona **OK** para eliminar la regla de alerta.

Cualquier instancia activa de la alerta se resolverá en un plazo de 10 minutos.

Gestiona las notificaciones de alertas

Configura notificaciones SNMP para alertas de StorageGRID

Si quieres que StorageGRID envíe notificaciones SNMP cuando ocurran alertas, debes habilitar el agente SNMP de StorageGRID y configurar uno o más destinos de trap.

Puedes usar la opción **Configuración > Supervisión > Agente SNMP** en Grid Manager o los puntos finales SNMP de la API de gestión de Grid para habilitar y configurar el agente SNMP de StorageGRID. El agente SNMP es compatible con las tres versiones del protocolo SNMP.

Para saber cómo configurar el agente SNMP, consulta ["Usa la supervisión SNMP"](#).

Después de que configures el agente SNMP de StorageGRID, se pueden enviar dos tipos de notificaciones basadas en eventos:

- Las traps son notificaciones enviadas por el agente SNMP que no requieren confirmación por parte del sistema de gestión. Las traps sirven para notificar al sistema de gestión que algo ha ocurrido en StorageGRID, como que se haya activado una alerta. Las traps son compatibles con las tres versiones de SNMP.
- Los informes son similares a las trampas, pero requieren confirmación por parte del sistema de gestión. Si el agente SNMP no recibe una confirmación en un plazo determinado, vuelve a enviar el informe hasta que reciba una confirmación o se alcance el valor máximo de reintentos. Los informes son compatibles con SNMPv2c y SNMPv3.

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

Si tu implementación de StorageGRID incluye varios nodos de administración, el nodo de administración principal es el remitente preferido para las notificaciones de alertas, los paquetes AutoSupport y las trampas e informes SNMP. Si el nodo de administración principal deja de estar disponible, las notificaciones se envían

temporalmente desde otros nodos de administración. Consulta "[¿Qué es un nodo de administración?](#)".

Configura las notificaciones por correo electrónico para las alertas de StorageGRID

Si deseas que se envíen notificaciones por correo electrónico cuando se produzcan alertas, debes proporcionar información sobre tu servidor SMTP. También debes ingresar las direcciones de correo electrónico de los destinatarios de las notificaciones de alerta.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tienes el "[Gestiona alertas o permisos de acceso root](#)".

Acerca de esta tarea

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

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

Pasos

1. Selecciona **Alertas > Configuración del correo electrónico**.

Aparece la página «Configuración del correo electrónico».

2. Marca la casilla **Habilitar notificaciones por correo electrónico** para indicar que deseas 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), introduce la información que StorageGRID necesita para acceder a tu servidor SMTP.

Si tu servidor SMTP requiere autenticación, debes proporcionar tanto un nombre de usuario como una contraseña.

Campo	Introduce
Servidor de correo	El nombre de dominio completo (FQDN) o dirección IP del servidor SMTP.
Puerto	El puerto utilizado para acceder al servidor SMTP. Debe estar comprendido entre 1 y 65535.
Nombre de usuario (opcional)	Si tu servidor SMTP requiere autenticación, introduce el nombre de usuario con el que deseas autenticarte.

Campo	Introduce
Contraseña (opcional)	Si tu servidor SMTP requiere autenticación, introduce la contraseña con la que te vas a autenticar.

4. En la sección «Direcciones de correo electrónico», introduce las direcciones de correo electrónico del remitente y de cada destinatario.

- a. Para el campo **Dirección de correo electrónico del remitente**, especifica una dirección de correo electrónico válida que se usará como dirección De para las notificaciones de alertas.

Por ejemplo: `storagegrid-alerts@example.com`

- b. En la sección de destinatarios, introduce una dirección de correo electrónico para cada lista de correo o persona que deba recibir un correo electrónico cuando ocurra una alerta.

Selecciona el icono con el signo más  para añadir destinatarios.

5. Si se requiere Transport Layer Security (TLS) para las comunicaciones con el servidor SMTP, selecciona **Require TLS** en la sección Transport Layer Security (TLS).

- a. En el campo **Certificado de CA**, introduce el certificado de CA que se usará para verificar la identidad del servidor SMTP.

Puedes copiar y pegar el contenido en este campo, o seleccionar **Examinar** y seleccionar el archivo.

Debes 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 certificados de CA codificados en formato PEM, concatenados en el orden de la cadena de certificados.

- b. Marca la casilla **Enviar certificado de cliente** si tu servidor de correo SMTP exige que los remitentes proporcionen certificados de cliente para la autenticación.

- c. En el campo **Certificado de cliente**, introduce el certificado de cliente codificado en formato PEM que se va a enviar al servidor SMTP.

Puedes copiar y pegar el contenido en este campo, o seleccionar **Examinar** y seleccionar el archivo.

- d. En el campo **Clave privada**, introduce la clave privada del certificado de cliente en formato PEM sin cifrar.

Puedes copiar y pegar el contenido en este campo, o seleccionar **Examinar** y seleccionar el archivo.



Si necesitas modificar la configuración del correo electrónico, selecciona el icono del lápiz  para actualizar este campo.

6. En la sección «Filtros», selecciona qué niveles de gravedad de las alertas deben dar lugar a notificaciones por correo electrónico, a menos que la regla para una alerta específica haya sido silenciada.

Gravedad	Descripción
Menor, mayor, crítico	Se envía una notificación por correo electrónico cuando se cumple la condición de gravedad menor, mayor o crítica para una regla de alerta.

Gravedad	Descripción
Mayor, crítica	Se envía una notificación por correo electrónico cuando se cumple la condición grave o crítica de una regla de alerta. No se envían notificaciones para alertas menores.
Solo crítico	Solo se envía una notificación por correo electrónico cuando se cumple la condición crítica de una regla de alerta. No se envían notificaciones para alertas menores o graves.

7. Cuando estés listo para comprobar la configuración de tu correo electrónico, sigue estos pasos:

- a. Selecciona **Enviar correo electrónico de prueba**.

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

- b. Comprueba las bandejas de entrada de todos los destinatarios del correo electrónico y confirma que se recibió un correo electrónico de prueba.



Si no recibes el correo electrónico en unos minutos o si se activa la alerta **Error en la notificación por correo electrónico**, comprueba tu configuración e inténtalo de nuevo.

- c. Inicia sesión en cualquier otro nodo de administración y envía un correo electrónico de prueba para comprobar la conectividad desde todas las sedes.



Cuando pruebas las notificaciones de alerta, debes iniciar sesión en cada nodo de administración para verificar la conectividad. Esto es diferente a probar los paquetes de AutoSupport, donde todos los nodos de administración envían el correo electrónico de prueba.

8. Selecciona **Guardar**.

El envío de un correo electrónico de prueba no guarda tu configuración. Debes seleccionar **Guardar**.

Se han guardado los ajustes de correo electrónico.

Información incluida en las notificaciones por correo electrónico de alerta

Después de que configuras 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 esté silenciada por un silencio. Consulta ["Silenciar las 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	Cualquier acción recomendada para la alerta.
4	Detalles sobre cada instancia activa de la alerta, incluyendo el nodo y el sitio afectados, la gravedad de la alerta, la hora UTC en la que se activó la regla de alerta y el nombre del trabajo y del 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 un número excesivo de notificaciones por correo electrónico cuando se activan las alertas, StorageGRID intenta agrupar varias alertas en una misma notificación.

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

Comportamiento	Ejemplo
Cada notificación de alerta solo se aplica a las alertas que tienen el mismo nombre. Si se activan al mismo tiempo dos alertas con nombres diferentes, se envían dos notificaciones por correo electrónico.	- La alerta A se activa en dos nodos al mismo tiempo. Solo 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 por cada alerta.
En el caso de una alerta concreta en un nodo específico, si se alcanzan los umbrales para más de un nivel de gravedad, solo se envía una notificación correspondiente a la alerta de mayor gravedad.	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 durante ese tiempo se activan otras alertas con el mismo nombre, 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 ambos casos 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 se han silenciado), incluso si ya se habían notificado antes.	- 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 activas con el mismo nombre y una de ellas se resuelve, no se envía una nueva notificación si la alerta vuelve a producirse en el nodo para el que se resolvió.	- Se activa la alerta A para el nodo 1. Se envía una notificación. - Se activa la alerta A para el nodo 2. Se envía una segunda notificación. - La alerta A se resuelve para el nodo 2, pero sigue activa para el nodo 1. - Se activa de nuevo la alerta A para el nodo 2. No se envía ninguna notificación nueva porque la alerta sigue activa para el nodo 1.
StorageGRID sigue enviando notificaciones por correo electrónico una vez cada 7 días hasta que se resuelvan todas las incidencias de la alerta o se silencie la regla de alerta.	- El 8 de marzo se activa la alerta A para el nodo 1. Se envía una notificación. - La alerta A no se ha resuelto ni silenciado. Se envían notificaciones adicionales el 15 de marzo, el 22 de marzo, el 29 de marzo y así sucesivamente.

Soluciona problemas con las notificaciones por correo electrónico de alertas

Si se activa la alerta **Error en la notificación por correo electrónico** o no puedes recibir la notificación por correo electrónico de la alerta de prueba, sigue estos pasos para resolver el problema.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Gestiona alertas o permisos de acceso root"](#).

Pasos

1. Comprueba tu configuración.
 - a. Selecciona **Alertas > Configuración del correo electrónico**.
 - b. Comprueba que la configuración del servidor de correo electrónico (SMTP) sea correcta.
 - c. Comprueba que hayas indicado direcciones de correo electrónico válidas para los destinatarios.
2. Comprueba tu filtro de correo no deseado y asegúrate de que el correo electrónico no haya ido a parar a la carpeta de correo no deseado.
3. Pide al administrador de tu correo electrónico que confirme que los mensajes de la dirección del remitente no están siendo bloqueados.
4. Recopila el archivo de registro del nodo de administración y luego ponte en contacto con soporte técnico.

El soporte técnico puede utilizar la información de los registros para ayudar a determinar qué ha fallado. Por ejemplo, el archivo prometheus.log podría mostrar un error al conectarse al servidor que especificaste.

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

Silencia las notificaciones de alerta en StorageGRID

Opcionalmente, puedes configurar silencios para suprimir temporalmente las notificaciones de alertas.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Gestiona alertas o permisos de acceso root"](#).

Acerca de esta tarea

Puedes silenciar las reglas de alerta en toda la grid, en un único sitio o en un único nodo, y para una o varias gravedades. Cada silencio suprime todas las notificaciones de una única regla de alerta o de todas las reglas de alerta.

Si has activado el agente SNMP, los silenciamientos también suprimen las trampas e informes SNMP.



Ten cuidado a la hora de decidir silenciar una regla de alerta. Si silencias una alerta, es posible que no detectes un problema subyacente hasta que este impida que se complete una operación crítica.

Pasos

1. Selecciona **Alertas > Silencios**.

Aparece la página Silences.

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. Selecciona **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. Selecciona o introduce la siguiente información:

Campo	Descripción
Regla de alerta	El nombre de la regla de alerta que deseas silenciar. Puedes seleccionar cualquier regla de alerta predeterminada o personalizada, incluso si la regla de alerta está desactivada. Nota: Selecciona All rules si deseas desactivar todas las reglas de alerta que cumplan los criterios especificados en este cuadro de diálogo.

Campo	Descripción
Descripción	Si lo deseas, puedes incluir una descripción del silencio. Por ejemplo, describe el propósito de este silencio.
Duración	Cuánto tiempo quieres que este silencio permanezca activo, en minutos, horas o días. Un silencio puede estar en efecto desde 5 minutos hasta 1,825 días (5 años). Nota: No deberías silenciar una regla de alerta durante un periodo prolongado. Si una regla de alerta está silenciada, podrías no detectar un problema subyacente hasta que impida que se complete una operación crítica. Sin embargo, podrías necesitar usar un silencio prolongado si una alerta se activa por una configuración específica e intencionada, como podría ser el caso de las alertas Services appliance link down y Storage appliance link down.
Gravedad	¿Qué gravedad o gravedades de las alertas deben silenciarse? Si la alerta se activa en una de las gravedades seleccionadas, no se envían notificaciones.
Nodos	A qué nodo o nodos quieres que se aplique esta supresión. Puedes suprimir una regla de alerta o todas las reglas en toda la grid, en un único sitio o en un único nodo. Si seleccionas toda la grid, la supresión se aplica a todos los sitios y a todos los nodos. Si seleccionas un sitio, la supresión se aplica solo a los nodos de ese sitio. Nota: No puedes seleccionar más de un nodo ni más de un sitio para cada silencio. Debes crear silencios adicionales si quieres suprimir la misma regla de alerta en más de un nodo o en más de un sitio al mismo tiempo.

4. Selecciona **Guardar**.

5. Si quieres modificar o dar por finalizado un silencio antes de que caduque, puedes editarlo o eliminarlo.

Opción	Descripción
Editar un silencio	- Selecciona Alertas > Silencios. - En la tabla, selecciona el botón de opción correspondiente al silencio que quieras editar. - Selecciona Editar. - Modifica la descripción, el tiempo restante, las gravedades seleccionadas o el nodo afectado. - Selecciona Guardar.

Opción	Descripción
Eliminar un silencio	a. Selecciona Alertas > Silencios. b. En la tabla, selecciona el botón de opción correspondiente al silencio que quieras eliminar. c. Selecciona Eliminar. d. Selecciona Aceptar para confirmar que deseas eliminar este silencio. Nota: A partir de ahora se enviarán notificaciones cuando se active esta alerta (a menos que se suprima mediante otra configuración de silencio). Si esta alerta está activa en este momento, es posible que las notificaciones por correo electrónico o SNMP tarden unos minutos en enviarse y que la página de alertas tarde en actualizarse.

Información relacionada

["Configura el agente SNMP"](#)

Alertas en StorageGRID

Esta referencia enumera las alertas predeterminadas que aparecen en el Grid Manager. Las acciones recomendadas están en el mensaje de alerta que recibes.

Si lo necesitas, puedes crear reglas de alerta personalizadas que se adapten a tu enfoque de administración de sistemas.

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

Alertas de appliance

Nombre de la alerta	Descripción
La batería del appliance ha caducado	La batería del controlador de almacenamiento del appliance ha expirado.
La batería del appliance falló	La batería del controlador de almacenamiento del appliance ha fallado.
La batería del appliance tiene una capacidad de aprendizaje insuficiente	La batería del controlador de almacenamiento del aparato tiene una capacidad aprendida insuficiente.
La batería del appliance está a punto de agotarse	La batería del controlador de almacenamiento del aparato está a punto de agotarse.
Batería del appliance retirada	Falta la batería del controlador de almacenamiento del aparato.
La batería del appliance está demasiado caliente	La batería del controlador de almacenamiento del aparato está sobrecalentada.

Nombre de la alerta	Descripción
Error de comunicación BMC del dispositivo	Se ha perdido la comunicación con el controlador de administración de la placa base (BMC).
Se ha detectado un fallo en el dispositivo de arranque del appliance	Se detectó un problema con el dispositivo de arranque en el appliance.
Error en el dispositivo de backup de la caché del appliance	Ha fallado un dispositivo de copia de seguridad de caché persistente.
Capacidad insuficiente del dispositivo de backup de la caché del appliance	La capacidad del dispositivo de copia de seguridad de la caché es insuficiente.
El dispositivo de backup de la caché del appliance está protegido contra escritura	Un dispositivo de copia de seguridad de la caché está protegido contra escritura.
Discrepancia en el tamaño de la memoria caché del appliance	Los dos controladores del aparato tienen cachés de distintos tamaños.
Fallo de la batería CMOS del appliance	Se ha detectado un problema con la batería CMOS del appliance.
Temperatura del chasis del controlador de cómputo del appliance demasiado alta	La temperatura del controlador de cálculo en un dispositivo StorageGRID ha superado un umbral nominal.
La temperatura de la CPU del controlador de cómputo del appliance es demasiado alta	La temperatura de la CPU en el controlador de cómputo de un dispositivo StorageGRID ha superado un umbral nominal.
El controlador informático del dispositivo requiere atención	Se ha detectado un fallo de hardware en el controlador de cómputo de un dispositivo StorageGRID.
La fuente de alimentación A del controlador de cómputo del appliance tiene un problema	La fuente de alimentación A del controlador informático tiene un problema.
La fuente de alimentación B del controlador compute del appliance tiene un problema	La fuente de alimentación B en el controlador informático tiene un problema.
El servicio de supervisión del hardware informático del appliance se ha bloqueado	El servicio que supervisa el estado del hardware de almacenamiento se ha bloqueado.

Nombre de la alerta	Descripción
La unidad DAS del appliance ha superado el límite de datos escritos por día	Cada día se escribe una cantidad excesiva de datos en una unidad, lo que podría anular su garantía.
Se ha detectado un fallo en la unidad DAS del appliance	Se ha detectado un problema con una unidad de almacenamiento de conexión directa (DAS) en el appliance.
La unidad DAS del appliance está en la ranura o el nodo equivocado	Una unidad de almacenamiento de conexión directa (DAS) está en la ranura o el nodo equivocado
Luz localizadora de la unidad DAS del appliance encendida	La luz localizadora de la unidad para una o más unidades de almacenamiento de conexión directa (DAS) en un Storage Node del dispositivo está encendida.
Reconstrucción de la unidad DAS del appliance	Una unidad de almacenamiento de conexión directa (DAS) se está reconstruyendo. Esto es normal si se ha sustituido recientemente o si se ha extraído y vuelto a insertar.
Se ha detectado un fallo en el ventilador del appliance	Se detectó un problema con una unidad de ventilador en el dispositivo.
Se ha detectado un fallo en el canal de fibra del appliance	Se ha detectado un problema en el enlace Fibre Channel entre el controlador de almacenamiento del appliance y el controlador de cómputo
Fallo en el puerto HBA Fibre Channel del appliance	Un puerto HBA de Fibre Channel está fallando o ha fallado.
Las unidades de flash cache del appliance no funcionan de forma óptima	Las unidades utilizadas para la caché SSD no son óptimas.
Se retiró el interconector del appliance/canister de batería	Falta el cartucho de la batería/interconexión.
Falta el puerto LACP en el appliance	Un puerto de un dispositivo StorageGRID no forma parte del enlace LACP.
Se ha detectado un fallo en la tarjeta de interfaz de red del dispositivo	Se ha detectado un problema con una tarjeta de interfaz de red (NIC) del dispositivo.
El suministro eléctrico general del appliance está degradado	La potencia de un dispositivo StorageGRID se ha desviado de la tensión de funcionamiento recomendada.

Nombre de la alerta	Descripción
Es necesario actualizar el software SANtricity OS del dispositivo	La versión del software SANtricity es inferior al mínimo recomendado para esta versión de StorageGRID.
Aviso crítico del SSD del dispositivo	Un SSD de un dispositivo está mostrando una advertencia crítica.
Fallo del controlador de almacenamiento de appliance	El controlador de almacenamiento A de un dispositivo StorageGRID ha fallado.
Fallo del controlador de almacenamiento B del dispositivo	El controlador de almacenamiento B de un dispositivo StorageGRID ha fallado.
Fallo de unidad del controlador de almacenamiento del appliance	Una o varias unidades de un dispositivo StorageGRID han fallado o no están en estado óptimo.
Problema de hardware en el controlador de almacenamiento del appliance	El software SANtricity informa "requiere atención" para un componente en un dispositivo StorageGRID.
Fallo de la fuente de alimentación A del controlador de almacenamiento del appliance	La fuente de alimentación A de un dispositivo StorageGRID se ha desviado de la tensión de funcionamiento recomendada.
Fallo en la fuente de alimentación B del controlador de almacenamiento del appliance	La fuente de alimentación B en un dispositivo StorageGRID se ha desviado de la tensión de funcionamiento recomendada.
El servicio de supervisión del hardware de almacenamiento de Appliance está detenido	El servicio que supervisa el estado del hardware de almacenamiento se ha bloqueado.
Las estanterías de almacenamiento de los appliances están degradadas	El estado de uno de los componentes en la bandeja de almacenamiento de un dispositivo de almacenamiento está degradado.
Se ha superado la temperatura del dispositivo	Se ha superado la temperatura nominal o máxima del controlador de almacenamiento del appliance.
Se ha retirado el sensor de temperatura del appliance	Se ha retirado un sensor de temperatura.
Error de arranque seguro UEFI del appliance	Un dispositivo no se ha iniciado de forma segura.
La E/S de disco es muy lenta	Una E/S de disco muy lenta podría estar afectando el rendimiento del grid.

Nombre de la alerta	Descripción
Se ha detectado un fallo en el ventilador del dispositivo de almacenamiento	Se detectó un problema con una unidad de ventilador en el controlador de almacenamiento de un appliance.
La conectividad de almacenamiento del dispositivo de almacenamiento está degradada	Hay un problema con una o varias conexiones entre el controlador de cómputo y el controlador de almacenamiento.
No se puede acceder al dispositivo de almacenamiento	No se puede acceder a un dispositivo de almacenamiento.

Alertas de auditoría y syslog

Nombre de la alerta	Descripción
Se están añadiendo registros de auditoría a la cola en memoria	El nodo no puede enviar los 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 los registros al servidor syslog externo.
Cola de auditoría extensa	La cola del disco para los mensajes de auditoría está llena. Si no se soluciona esta situación, las operaciones de S3 podrían fallar.
Se están añadiendo registros a la cola en disco	El nodo no puede reenviar los registros al servidor syslog externo y la cola en disco se está llenando.

Alertas de bucket

Nombre de la alerta	Descripción
FabricPool el bucket tiene una configuración de consistencia no compatible	Un bucket FabricPool utiliza el nivel de consistencia Available o Strong-site, que no es compatible.
FabricPool el bucket tiene una configuración de control de versiones no compatible	Un bucket de FabricPool tiene habilitado el control de versiones o S3 Object Lock, que no son compatibles.

Alertas de Cassandra

Nombre de la alerta	Descripción
Error de auto-compactor de Cassandra	El autocompactor de Cassandra ha experimentado un error.

Nombre de la alerta	Descripción
Las métricas del autocompactor de Cassandra están desactualizadas	Las métricas que describen el autocompactor de Cassandra están desactualizadas.
Error de comunicación de Cassandra	Los nodos que ejecutan el servicio Cassandra están teniendo problemas para comunicarse entre sí.
Las compactaciones de Cassandra están sobrecargadas	El proceso de compactación de Cassandra está sobrecargado.
Error de escritura por exceso de tamaño en Cassandra	Un proceso interno de StorageGRID envió a Cassandra una solicitud de escritura que era demasiado grande.
Las métricas de reparación de Cassandra están desactualizadas	Las métricas que describen las tareas de reparación de Cassandra están desactualizadas.
El progreso de reparación de Cassandra es lento	Las reparaciones de la base de datos Cassandra avanzan lentamente.
El servicio de reparación de Cassandra no está disponible	El servicio de reparación de Cassandra no está disponible.
Corrupción de la tabla de Cassandra	Cassandra ha detectado corrupción en la tabla. Cassandra se reinicia automáticamente si detecta corrupción en la tabla.

Alertas de Cloud Storage Pool

Nombre de la alerta	Descripción
Error de conectividad del grupo de almacenamiento en la nube	La comprobación de estado de Cloud Storage Pools detectó uno o más errores nuevos.
Caducidad de la certificación de la entidad final de IAM Roles Anywhere	El certificado de entidad final de IAM Roles Anywhere está a punto de caducar.

Alertas de replicación entre grids

Nombre de la alerta	Descripción
Fallo permanente en la replicación entre grids	Se ha producido un error de replicación entre grids que requiere la intervención del usuario para solucionarlo.
Recursos de replicación entre grids no disponibles	Las solicitudes de replicación entre grids están pendientes porque un recurso no está disponible.

alertas DHCP

Nombre de la alerta	Descripción
La concesión de DHCP ha caducado	La concesión DHCP de una interfaz de red ha caducado.
La concesión de DHCP caduca en breve	La concesión DHCP de una interfaz de red está a punto de caducar.
El servidor DHCP no está disponible	El servidor DHCP no está disponible.

Alertas de depuración y seguimiento

Nombre de la alerta	Descripción
Depurar impacto en el rendimiento	Cuando el modo de depuración está activado, el rendimiento del sistema podría verse afectado negativamente.
Configuración de seguimiento activada	Cuando se activa la configuración de seguimiento, el rendimiento del sistema podría verse afectado negativamente.

Alertas por correo electrónico y AutoSupport

Nombre de la alerta	Descripción
AutoSupport no se pudo enviar el mensaje	El mensaje más reciente de AutoSupport no se pudo enviar.
Error en la resolución del nombre de dominio	El nodo de 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 de una alerta.
No se encontró el bucket de destino para el archivado de registros	Falta el bucket de destino para el archivado de registros, lo que impide que los registros se archiven en el bucket de destino.
Errores de notificación SNMP	Errores al enviar notificaciones SNMP inform a un destino de trap.
Acceso externo por SSH habilitado	El acceso externo por SSH lleva más de 24 horas activado.
Se detectó un inicio de sesión por SSH o consola	En las últimas 24 horas, un usuario ha iniciado sesión con Web Console o SSH.

Alertas de código de borrado (EC)

Nombre de la alerta	Descripción
Error en el reequilibrio de EC	El procedimiento de reequilibrio de EC ha fallado o se ha detenido.
Fallo en la reparación de EC	Ha fallado o se ha detenido una tarea de reparación de datos de EC.
La reparación de EC se ha estancado	Se ha estancado un trabajo de reparación de datos EC.
Error de verificación de fragmentos con código de borrado	Los fragmentos con código de borrado ya no se pueden verificar. Es posible que los fragmentos dañados no se puedan reparar.

Alertas sobre la expiración de los certificados

Nombre de la alerta	Descripción
Caducidad del certificado de la CA del proxy de administración	Uno o más certificados en el paquete de CA del servidor proxy de administración están a punto de caducar.
Caducidad del certificado de cliente	Uno o más certificados de cliente están a punto de caducar.
Caducidad del certificado global del servidor para S3	El certificado global del servidor de S3 está a punto de caducar.
Caducidad del certificado del endpoint del balanceador de carga	Uno o más certificados de los endpoints del balanceador de carga están a punto de expirar.
Caducidad del certificado del servidor para la interfaz de gestión	El certificado del servidor utilizado para la interfaz de administración está a punto de caducar.
Caducidad 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 externo de syslog	El certificado de cliente de un servidor syslog externo está a punto de caducar.
Caducidad del certificado del servidor syslog externo	El certificado del servidor que presenta el servidor syslog externo está a punto de caducar.

Alertas de la red de grid

Nombre de la alerta	Descripción
Desajuste de MTU en la red de grid	La configuración de MTU de la interfaz de red Grid Network (eth0) varía considerablemente entre los nodos del grid.

Alertas de la federación de grid

Nombre de la alerta	Descripción
Caducidad del certificado de federación de grid	Uno o más certificados de la federación de grid están a punto de caducar.
Error en la conexión de la federación de grid	La conexión de la federación de grid entre el grid local y el remoto no está funcionando.

Alertas de uso elevado o de latencia elevada

Nombre de la alerta	Descripción
Alto uso de heap de Java	Se está utilizando un alto porcentaje del espacio heap de Java.
Alta latencia en las consultas de metadatos	El tiempo medio de las consultas de metadatos de Cassandra es demasiado largo.

Alertas de federación de identidades

Nombre de la alerta	Descripción
Error de sincronización de la federación de identidades	No se pueden sincronizar los grupos y usuarios federados desde la fuente de identidades.
Error de sincronización de la federación de identidades de un inquilino	No se pueden sincronizar los grupos y usuarios federados desde la fuente de identidades configurada por un inquilino.

Alertas de gestión del ciclo de vida de la información (ILM)

Nombre de la alerta	Descripción
La asignación de ILM es inviable	No se puede aplicar una instrucción de asignación en una regla ILM para ciertos objetos.
Velocidad de exploración del ILM baja	La velocidad de escaneo del ILM está configurada en menos de 100 objetos/segundo.

Alertas del servidor de gestión de claves (KMS)

Nombre de la alerta	Descripción
Caducidad del certificado CA de KMS	El certificado de la autoridad de certificación (CA) utilizado para firmar el certificado del servidor de gestión de claves (KMS) está a punto de caducar.

Nombre de la alerta	Descripción
Caducidad del certificado de cliente KMS	El certificado de cliente de un servidor de gestión de claves está a punto de caducar
No se ha podido cargar la configuración de KMS	La configuración del servidor de gestión de claves existe pero no se pudo cargar.
Error de conectividad con KMS	Un nodo de dispositivo no pudo conectarse al servidor de gestión de claves de su sitio.
No se ha encontrado el nombre de la clave de cifrado de KMS	El servidor de gestión de claves configurado no tiene una clave de cifrado que coincida con el nombre proporcionado.
Error en la rotación de la clave de cifrado de KMS	Todos los volúmenes de los dispositivos se descifraron correctamente, pero uno o varios volúmenes no pudieron rotar a la clave más reciente.
KMS no está configurado	No existe ningún servidor de gestión de claves para este sitio.
La clave KMS no pudo descifrar el volumen de un dispositivo	Uno o más volúmenes en un dispositivo con el cifrado por nodo activado no se pudieron descifrar con la clave KMS actual.
Caducidad del certificado del servidor KMS	El certificado del servidor utilizado por el servidor de gestión de claves (KMS) está a punto de caducar.
Error de conectividad con el servidor KMS	Un nodo de dispositivo no pudo conectarse a uno o más servidores en el clúster de servidores de gestión de claves de su sitio.

Alertas del equilibrador de carga

Nombre de la alerta	Descripción
Conexiones elevadas del balanceador de carga sin solicitudes	Un porcentaje elevado de conexiones a los endpoints del equilibrador de carga se desconectaron sin realizar solicitudes.

Alertas de desfase horario local

Nombre de la alerta	Descripción
Gran diferencia horaria del reloj local	La diferencia entre la hora del reloj local y la hora del Protocolo de Tiempo de Red (NTP) es demasiado grande.

Alertas de memoria insuficiente o poco espacio

Nombre de la alerta	Descripción
Capacidad baja del disco del registro de auditoría	El espacio disponible para los registros de auditoría es escaso. Si no se soluciona este problema, las operaciones de S3 podrían fallar.
Memoria disponible del nodo insuficiente	La cantidad de RAM disponible en un nodo es escasa.
Espacio libre insuficiente en el grupo de almacenamiento	El espacio disponible para almacenar datos de objetos en el nodo de almacenamiento es escaso.
Memoria instalada del nodo insuficiente	La cantidad de memoria instalada en un nodo es baja.
Almacenamiento reducido de metadatos	El espacio disponible para almacenar los metadatos de los objetos es escaso.
Baja capacidad de disco según las métricas	El espacio disponible para la base de datos de métricas es escaso.
Almacenamiento de datos de objetos bajo	El espacio disponible para almacenar datos de objetos es escaso.
Anulación de la marca de agua de solo lectura baja	El valor de anulación de la marca de agua de solo lectura del volumen de almacenamiento es inferior a la marca de agua mínima optimizada para un Storage Node.
Capacidad insuficiente del disco raíz	El espacio disponible en el disco raíz es escaso.
Baja capacidad de datos del sistema	El espacio disponible en /var/local es escaso. Si no se soluciona este problema, las operaciones de S3 podrían fallar.
Espacio libre insuficiente en el directorio tmp	El espacio disponible en el directorio /tmp es escaso.

Alertas de nodos o de red de nodos

Nombre de la alerta	Descripción
No se ha alcanzado el quórum del ADC	El nodo de almacenamiento con el servicio ADC está fuera de línea. Las operaciones de ampliación y decomisionado quedan bloqueadas hasta que se restablezca el quórum de ADC.
Uso de recepción de la red de administración	El uso de la recepción en la red de administración es elevado.

Nombre de la alerta	Descripción
Uso de transmisión de la red de administración	El uso de la transmisión en la red de administración es elevado.
Error en la configuración del cortafuegos	No se pudo aplicar la configuración del cortafuegos.
Puntos finales de la interfaz de gestión en modo de reserva	Todos los puntos finales de la interfaz de gestión llevan demasiado tiempo recurriendo a los puertos predeterminados.
Error de conectividad de la red de nodos	Se han producido errores durante la transferencia de datos entre nodos.
Error en la trama de recepción de la red de nodos	Un alto porcentaje de las tramas de red recibidas por un nodo presentaban errores.
El nodo no está sincronizado con el servidor NTP	El nodo no está sincronizado con el servidor NTP.
Nodo no bloqueado con el servidor NTP	El nodo no está bloqueado a un servidor NTP.
Red de nodo que no es un dispositivo inactiva	Uno o varios dispositivos de red están inactivos o desconectados.
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.
Enlace del dispositivo de servicios caído en el puerto 1 de la red de administración	El puerto 1 de la red de administración del dispositivo está inactivo o desconectado.
Conexión del dispositivo de servicios interrumpida en la red del cliente	La interfaz del dispositivo a la red del cliente (eth2) está inactiva o desconectada.
Conexión del dispositivo de servicios interrumpida en el puerto de red 1	El puerto de red 1 del dispositivo está inactivo o desconectado.
El enlace del dispositivo de servicios está inactivo en el puerto de red 2	El puerto de red 2 del dispositivo está inactivo o desconectado.

Nombre de la alerta	Descripción
El enlace del dispositivo de servicios está inactivo en el puerto de red 3	El puerto de red 3 del dispositivo está inactivo o desconectado.
El enlace del dispositivo de servicios está inactivo en el puerto de red 4	El puerto de red 4 del dispositivo está inactivo o desconectado.
Enlace del dispositivo de almacenamiento 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 caído en el puerto 1 de la red de administración	El puerto 1 de la red de administración del dispositivo está inactivo o desconectado.
Conexión del dispositivo de almacenamiento caída 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.
El enlace del dispositivo de almacenamiento está inactivo en el puerto de red 2	El puerto de red 2 del dispositivo está inactivo o desconectado.
El enlace del dispositivo de almacenamiento está inactivo en el puerto de red 3	El puerto de red 3 del dispositivo está inactivo o desconectado.
El enlace del dispositivo de almacenamiento está inactivo en el puerto de red 4	El puerto de red 4 del dispositivo está inactivo o desconectado.
El nodo de almacenamiento no está en el estado de almacenamiento deseado	El servicio LDR en un nodo de almacenamiento no puede pasar al estado deseado debido a un error interno o a un problema relacionado con el volumen
Uso de la conexión TCP	El número de conexiones TCP en este nodo se está acercando al número máximo que se puede rastrear.
No se puede establecer comunicación con el nodo	Uno o varios servicios no responden, o no se puede acceder al nodo.
Reinicio inesperado del nodo	Un nodo se ha reiniciado de forma inesperada en las últimas 24 horas.

Alertas de objetos

Nombre de la alerta	Descripción
Error al comprobar la existencia del objeto	La tarea de comprobación de la existencia del objeto ha fallado.
La comprobación de la existencia del objeto se ha bloqueado	La tarea de comprobación de la existencia del objeto se ha atascado.
Objetos que podrían haberse perdido	Uno o más objetos potencialmente perdidos de la cuadrícula.
Objetos huérfanos detectados	Se han detectado objetos huérfanos.
El tamaño del objeto PUT en S3 es demasiado grande	Un cliente está intentando realizar una operación PUT de objeto que supera los límites de tamaño de S3.
Objeto corrupto no identificado detectado	Se ha encontrado un archivo en el almacenamiento de objetos replicados que no se ha podido identificar como un objeto replicado.

Alertas de corrupción de objetos

Nombre de la alerta	Descripción
Discrepancia en el tamaño de los objetos	Se detectó un tamaño de objeto inesperado durante el procedimiento de comprobación de existencia del objeto.

Alertas de los servicios de la plataforma

Nombre de la alerta	Descripción
Capacidad baja de solicitudes pendientes de Platform Services	El número de solicitudes pendientes de Platform Services se está acercando al límite de capacidad.
Servicios de plataforma no disponibles	Hay muy pocos nodos de almacenamiento con el servicio RSM en funcionamiento o disponibles en una sede.

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 requiere atención.
Es necesario restaurar el volumen de almacenamiento	Se ha recuperado un volumen de almacenamiento y necesita ser restaurado.

Nombre de la alerta	Descripción
Volumen de almacenamiento fuera de línea	Un volumen de almacenamiento lleva más de 5 minutos fuera de línea.
Se intentó volver a montar el volumen de almacenamiento	Un volumen de almacenamiento estaba sin conexión y se ha activado un remontaje automático. Esto podría indicar un problema con la unidad o errores en el sistema de archivos.
La restauración del volumen no pudo iniciar la reparación de los datos replicados	No se pudo iniciar automáticamente la reparación de los datos replicados para un volumen reparado.

Alertas de los servicios de StorageGRID

Nombre de la alerta	Descripción
Servicio nginx usando configuración de backup	La configuración del servicio nginx no es válida. Ahora se está utilizando la configuración anterior.
Servicio nginx-gw usando la configuración de backup	La configuración del servicio nginx-gw no es válida. Ahora se está utilizando la configuración anterior.
Es necesario reiniciar para desactivar FIPS	La política de seguridad no exige el modo FIPS, pero se utilizan módulos FIPS.
Es necesario reiniciar para habilitar FIPS	La política de seguridad exige el modo FIPS, pero no se están usando módulos FIPS.
Servicio SSH usando configuración de backup	La configuración del servicio SSH no es válida. Ahora se está utilizando la configuración anterior.

Alertas de inquilino

Nombre de la alerta	Descripción
Uso de cuota de inquilino alto	Se está utilizando un alto porcentaje del espacio de la cuota. Esta regla está desactivada por defecto porque podría generar demasiadas notificaciones.

Métricas de Prometheus más comunes en StorageGRID

Consulta esta lista de métricas de Prometheus de uso habitual para comprender mejor las condiciones de las reglas de alerta predeterminadas o para crear las condiciones de las reglas de alerta personalizadas.

También puedes [obtener una lista completa de todas las métricas](#).

Para obtener más información sobre la sintaxis de las consultas de Prometheus, consulta ["Consultando"](#)

Prometheus".

¿Qué son las métricas de Prometheus?

Las métricas de Prometheus son mediciones de series temporales. El servicio de Prometheus en los nodos de administración recopila estas métricas de los servicios de 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/` volumen alcanza la capacidad, primero se eliminan las métricas más antiguas.

¿Dónde se utilizan las métricas de Prometheus?

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

- **Página «Nodos»:** Los gráficos y diagramas de las pestañas disponibles en la página «Nodos» utilizan la herramienta de visualización Grafana para mostrar las métricas de series temporales recopiladas por Prometheus. Grafana muestra los datos de series temporales en formato de gráficos y diagramas, mientras que Prometheus actúa como fuente de datos de fondo.



- **Alertas:** Las alertas se activan en niveles de gravedad específicos cuando las condiciones de las reglas de alerta que usan métricas de Prometheus se evalúan como verdaderas.
- **API de gestión de la red:** Puedes utilizar las métricas de Prometheus en reglas de alerta personalizadas o con herramientas de automatización externas para supervisar tu sistema StorageGRID. Hay una lista completa de métricas de Prometheus disponible en la API de gestión de la red. (En la parte superior de Grid Manager, selecciona el icono de ayuda y selecciona **API documentation > metrics**.) Aunque hay más de mil métricas disponibles, solo necesitas un número relativamente pequeño para supervisar las operaciones más críticas de StorageGRID.



Las métricas que incluyen *private* en su nombre están destinadas exclusivamente a uso interno y pueden cambiar entre versiones de StorageGRID sin previo aviso.

- La página **Soporte > Herramientas > Diagnósticos** y la página **Soporte > Herramientas > Métricas**: estas páginas, destinadas principalmente al soporte técnico, ofrecen varias herramientas y gráficos que utilizan los valores de las métricas de Prometheus.



Algunas funciones y opciones del menú dentro de la página de Métricas no funcionan intencionadamente y pueden cambiar.

Lista de las métricas más habituales

La siguiente lista contiene las métricas de Prometheus más utilizadas.



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

alertmanager_notificaciones_fallidas_total

El número total de notificaciones de alerta fallidas.

node_filesystem_avail_bytes

La cantidad de espacio disponible en el sistema de archivos para los usuarios que no son root, en bytes.

node_memory_MemAvailable_bytes

Campo de información de memoria MemAvailable_bytes.

nodo_red_carrier

Valor de portador de `/sys/class/net/iface`.

node_network_receive_errs_total

Estadística de dispositivo de red `receive_errs`.

total de errores de transmisión de la red de nodos

Estadística de dispositivo de red `transmit_errs`.

storagegrid_administratively_down

El nodo no está conectado a la grid por un motivo previsible. Por ejemplo, el nodo o los servicios en el nodo se han apagado de forma controlada, el nodo se está reiniciando o se está actualizando el software.

estado_del_hardware_del_controlador_de_cómputo_de_storagegrid_appliance

El estado del hardware del controlador de cómputo en un appliance.

discos_defectuosos_de_storagegrid_appliance

Para el controlador de almacenamiento en un dispositivo, el número de unidades que no son óptimas.

estado_del_hardware_del_controlador_de_almacenamiento_de_storagegrid_appliance

El estado general del hardware del controlador de almacenamiento en un appliance.

StorageGRID: compartimentos y contenedores de contenido

El número total de buckets de S3 que conoce este Storage Node.

objetos_de_contenido_de_storagegrid

El número total de objetos de datos S3 conocidos por este nodo de almacenamiento. El recuento solo es válido para los objetos de datos creados por aplicaciones cliente que se conectan al sistema a través de S3.

storagegrid_content_objects_lost

El número total de objetos que este servicio detecta como desaparecidos del sistema StorageGRID. Deberías tomar medidas para averiguar la causa de la pérdida y si es posible recuperarlos.

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

storagegrid_http_sessions_incoming_attempted

El número total de sesiones HTTP que se han intentado establecer con un nodo de almacenamiento.

storagegrid_http_sessions_incoming_currently_established

El número de sesiones HTTP que están activas (abiertas) actualmente en el Storage Node.

storagegrid_http_sessions_incoming_failed

El número total de sesiones HTTP que no se completaron correctamente, ya sea debido a una solicitud HTTP con formato incorrecto o a un error durante el procesamiento de una operación.

storagegrid_http_sessions_incoming_successful

El número total de sesiones HTTP que se han completado correctamente.

storagegrid_ilm_awaiting_background_objects

El número total de objetos en este nodo que están esperando la evaluación de ILM tras el análisis.

storagegrid_ilm_awaiting_client_evaluation_objects_per_second

La frecuencia actual con la que se evalúan los objetos según la política de ILM en este nodo.

storagegrid_ilm_awaiting_client_objects

El número total de objetos en este nodo que están pendientes de evaluación por ILM a partir de operaciones del cliente (por ejemplo, la ingesta).

storagegrid_ilm_awaiting_total_objects

El número total de objetos pendientes de evaluación de ILM.

storagegrid_ilm_scan_objects_per_second

La frecuencia con la que se analizan y se ponen en cola para ILM los objetos que pertenecen a este nodo.

storagegrid_ilm_scan_period_estimated_minutes

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

Nota: Un análisis completo no garantiza que se haya aplicado ILM a todos los objetos que pertenecen a este nodo.

tiempo_de_caducidad_del_certificado_del_endpoint_del_load_balancer_de_StorageGRID

El tiempo de caducidad del certificado del endpoint del balanceador de carga en segundos desde la época.

latencia media de las consultas de metadatos de StorageGRID (milisegundos)

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

storagegrid_network_received_bytes

La cantidad total de datos recibidos desde la instalación.

bytes_transmitidos_por_la_red_de_StorageGRID

La cantidad total de datos enviados desde la instalación.

porcentaje_de_utilización_de_la_CPU_del_nodo_de_StorageGRID

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

storagegrid_ntp_fuente_de_tiempo_elegida_desviación_milisegundos

Desfase sistemático del tiempo proporcionado por una fuente de tiempo seleccionada. El desfase se produce cuando el retraso para llegar a una fuente de tiempo no es igual al tiempo que tarda dicha fuente en llegar al cliente NTP.

storagegrid_ntp_locked

El nodo no está bloqueado a un servidor Network Time Protocol (NTP).

storagegrid_s3_data_transfers_bytes_ingested

La cantidad total de datos importados desde los clientes de S3 a este Storage Node desde la última vez que se restableció el atributo.

storagegrid_s3_data_transfers_bytes_retrieved

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

storagegrid_s3_operations_failed

El número total de operaciones de S3 fallidas (códigos de estado HTTP 4xx y 5xx), excluyendo aquellas causadas por fallo de autorización de 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 de S3 fallidas que se deben a un error de autorización.

storagegrid_servercertificate_management_interface_cert_expiry_days

El número de días antes de que caduque el certificado de la Management Interface.

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days

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

storagegrid_service_cpu_seconds

La cantidad acumulada de tiempo que la CPU ha sido utilizada por este servicio desde la instalación.

uso_de_memoria_del_servicio_storagegrid_bytes

La cantidad de memoria (RAM) que este servicio está utilizando actualmente. Este valor es idéntico al que muestra la utilidad top de Linux como RES.

storagegrid_service_network_received_bytes

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

bytes transmitidos por la red del servicio de StorageGRID

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.

storagegrid_service_runtime_seconds

El tiempo total que lleva en funcionamiento el servicio desde su instalación.

storagegrid_service_uptime_seconds

El tiempo total que lleva en funcionamiento el servicio desde su último reinicio.

storagegrid_storage_state_current

Situación actual de los servicios de almacenamiento. Los valores de los atributos son:

- 10 = Desconectado
- 15 = Mantenimiento
- 20 = Solo lectura
- 30 = En línea

storagegrid_storage_status

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

storagegrid_utilización_del_almacenamiento_datos_bytes

Una estimación del tamaño total de los datos de objetos replicados y codificados con código de borrado en el Storage Node.

storagegrid_storage_utilization_metadata_allowed_bytes

El espacio total del volumen 0 de cada Storage Node que está permitido para los metadatos de los objetos. Este valor siempre es menor que el espacio real reservado para metadatos en un nodo, porque una parte del espacio reservado se requiere para operaciones esenciales de la base de datos (como compactación y reparación) y futuras actualizaciones de hardware y software. El espacio permitido para los metadatos de los objetos controla la capacidad total de objetos.

bytes de metadatos de utilización de StorageGRID

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

storagegrid_storage_utilization_total_space_bytes

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

storagegrid_storage_utilization_usable_space_bytes

La cantidad total de espacio de almacenamiento de objetos restante. Se calcula sumando el espacio disponible de todos los almacenes de objetos del Storage Node.

storagegrid_tenant_usage_data_bytes

El tamaño lógico de todos los objetos del tenant.

storagegrid_tenant_usage_object_count

El número de objetos del tenant.

cuota_de_uso_del_tenant_de_StorageGRID_en_bytes

La cantidad máxima de espacio lógico disponible para los objetos del inquilino. Si no se especifica una

métrica de cuota, se dispone de una cantidad ilimitada de espacio.

Obtener una lista de todas las métricas

Para obtener la lista completa de métricas, utiliza la Grid Management API.

Pasos

1. En la parte superior del Grid Manager, selecciona el icono de ayuda y selecciona **API documentation**.
2. Localiza las operaciones de **métricas**.
3. Ejecuta la operación `GET /grid/metric-names`.
4. Descarga los resultados.

Referencia de los archivos de registro

Archivos de registro de StorageGRID

StorageGRID proporciona registros que se utilizan para capturar eventos, mensajes de diagnóstico y condiciones de error. Es posible que te pidan que recopiles los archivos de registro y los envíes 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 del archivo bycast.log"](#)



La información proporcionada para cada tipo de registro es meramente orientativa. Estos registros están destinados a la resolución avanzada de problemas por parte del soporte técnico. Las técnicas avanzadas que implican reconstruir el historial del problema utilizando los registros de auditoría y los archivos de registro de la aplicación quedan fuera del alcance de estas instrucciones.

Accede a los registros

Para acceder a los registros, puedes ["recopilar archivos de registro y datos del sistema"](#) desde uno o varios nodos como un solo archivo comprimido de registros. O puedes acceder a los archivos de registro individuales de cada nodo de grid de la siguiente manera:

Pasos

1. Introduce el siguiente comando: `ssh admin@grid_node_IP`
2. Introduce la contraseña que figura en el archivo `Passwords.txt`.
3. Introduce el siguiente comando para pasar a ser usuario root: `su -`
4. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Exportar los registros al servidor syslog

Exportar los registros al servidor syslog ofrece estas capacidades:

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

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

Categorías de archivos de registro

El archivo de registros de StorageGRID contiene los registros descritos para cada categoría y archivos adicionales que contienen métricas y la salida de los comandos de depuración.

Ubicación del archivo	Descripción
auditoría	Mensajes de auditoría generados durante el funcionamiento normal del sistema.
registros-del-sistema-operativo-base	Información básica sobre el sistema operativo, incluidas las versiones de las imágenes de StorageGRID.
paquetes	Información de configuración global (bundles).
cache-svc	Registros del servicio de caché (solo en Gateway Nodes).
cassandra	Información de la base de datos Cassandra y registros de reparación de Reaper.
ec	Información de los VCS sobre el nodo actual e información del grupo EC por ID de perfil.
grid	Registros generales de grid, incluidos los registros de depuración (<code>broadcast.log</code>) y los registros <code>servermanager</code> .
grid.json	Archivo de configuración de grid compartido por todos los nodos. Además, <code>node.json</code> es específico del nodo actual.
hagroups	Métricas y registros de los grupos de alta disponibilidad.
instalar	<code>Gdu-server</code> y los registros de instalación.
Lambda-arbitrador	Registros relacionados con la solicitud de proxy de S3 Select.
leakd	Registros del servicio leakd.
lumberjack.log	Mensajes de depuración relacionados con la recopilación de registros.

Ubicación del archivo	Descripción
Métricas	Registros de servicio de Grafana, Jaeger, node exporter y Prometheus.
miscd	Registros diversos de acceso y errores.
mysql	La configuración de la base de datos mariaDB y los registros relacionados.
red	Registros generados por scripts relacionados con la red y el servicio Dynip.
nginx	Archivos de configuración y registros del equilibrador de carga y de la federación de grid. También incluye los registros de tráfico de Grid Manager y Tenant Manager.
nginx-gw	• <code>access.log</code>: Mensajes de registro de solicitudes de Grid Manager y Tenant manager. ◦ Estos mensajes llevan el prefijo <code>mgmt</code>: cuando se exportan mediante <code>syslog</code>. ◦ El formato de estos mensajes de registro es <code>[<code>\$time_iso8601</code>] <code>\$remote_addr</code> <code>\$status</code> <code>\$bytes_sent</code> <code>\$request_length</code> <code>\$request_time</code> "<code>\$endpointId</code>" "<code>\$request</code>" "<code>\$http_host</code>" "<code>\$http_user_agent</code>" "<code>\$http_referer</code>"</code> • <code>cgr-access.log.gz</code>: Solicitudes de replicación entre grids entrantes. ◦ Estos mensajes llevan el prefijo <code>cgr</code>: cuando se exportan mediante <code>syslog</code>. ◦ El formato de estos mensajes de registro es <code>[<code>\$time_iso8601</code>] <code>\$remote_addr</code> <code>\$status</code> <code>\$bytes_sent</code> <code>\$request_length</code> <code>\$request_time</code> "<code>\$endpointId</code>" "<code>\$upstream_addr</code>" "<code>\$request</code>" "<code>\$http_host</code>"</code> • <code>endpoint-access.log.gz</code>: solicitudes de S3 a los puntos de conexión del equilibrador de carga. ◦ Estos mensajes llevan el prefijo <code>endpoint</code>: cuando se exportan mediante <code>syslog</code>. ◦ El formato de estos mensajes de registro es <code>[<code>\$time_iso8601</code>] <code>\$remote_addr</code> <code>\$status</code> <code>\$bytes_sent</code> <code>\$request_length</code> <code>\$request_time</code> "<code>\$endpointId</code>" "<code>\$upstream_addr</code>" "<code>\$request</code>" "<code>\$http_host</code>"</code> • <code>nginx-gw-dns-check.log</code>: relacionado con la nueva alerta de comprobación del DNS.
ntp	Archivo de configuración de NTP y registros.
Objetos huérfanos	Registros relacionados con objetos huérfanos.

Ubicación del archivo	Descripción
os	Archivo de estado del nodo y de la grid, incluidos los servicios <code>pid</code> .
otros	Archivos de registro en <code>/var/local/log</code> que no se recopilan en otras carpetas.
rendimiento	Información sobre el rendimiento de la CPU, la red y la E/S de disco.
prometheus-data	Métricas actuales de Prometheus, si la recopilación de registros incluye datos de Prometheus.
aprovisionamiento	Registros relacionados con el proceso de aprovisionamiento de grid.
raft	Registros del clúster de Raft usados en los servicios de plataforma.
ssh	Registros relacionados con la configuración y el servicio SSH.
snmp	Configuración del agente SNMP utilizada para enviar notificaciones SNMP.
sockets-data	Datos de sockets para la depuración de red.
system-commands.txt	Salida de los comandos de contenedores de StorageGRID. Contiene información del sistema, como la red y el uso del disco.
sincronizar-paquete-de-recuperación	Relacionado con mantener la coherencia del paquete de recuperación más reciente en todos los nodos de administración y nodos de almacenamiento que alojan el servicio ADC.

Registros del software StorageGRID

Puedes utilizar los registros de StorageGRID para solucionar problemas.



Si deseas enviar tus registros a un servidor syslog externo o cambiar el destino de la información de auditoría, como el `bcast.log` y el `nms.log`, consulta ["Configura la gestión de registros"](#).

Registros generales de StorageGRID

Nombre del archivo	Notas	Encontrado en
<code>/var/local/log/bcast.log</code>	El archivo principal de resolución de problemas de StorageGRID.	Todos los nodos

Nombre del archivo	Notas	Encontrado en
/var/local/log/bycast-err.log	Contiene un subconjunto de <code>bycast.log</code> (mensajes con gravedad ERROR y CRITICAL). Los mensajes CRITICAL también se muestran en el sistema.	Todos los nodos
/var/local/core/	Contiene los archivos de volcado de memoria que se hayan creado si el programa termina de forma anómala. Las posibles causas incluyen fallos de aserción, violaciones o tiempos de espera de los hilos. Nota: El archivo <code>`/var/local/core/kexec_cmd</code> suele encontrarse en los nodos del appliance y no indica ningún 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 los 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 los 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 los servicios de nginx-gw).	Nodos de administración y de pasarela
/var/local/log/update-cipher-configurations.log	Contiene registros relacionados con la configuración de las políticas de TLS y SSH.	Todos los nodos

Registros de la federación de grid

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 grid.	Todos los nodos

Registros de NMS

Nombre del archivo	Notas	Encontrado en
/var/local/log/nms.log	• Captura las notificaciones del Grid Manager y del Tenant Manager. • Registra los eventos relacionados con el funcionamiento del servicio NMS. Por ejemplo, notificaciones por correo electrónico y cambios en la configuración. • Contiene actualizaciones del paquete XML derivadas de los cambios de configuración realizados en el sistema. • Contiene mensajes de error relacionados con el submuestreo de atributos que se realiza 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. • Contiene registros relacionados con AutoSupport.	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 gestión hacia los servicios internos de StorageGRID.	Nodos de administración

Registros del Administrador de servidores

Nombre del archivo	Notas	Encontrado en
/var/local/log/servermanager.log	Archivo de registro de la aplicación Administrador de servidores 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 de la GUI del Administrador de servidores.	Todos los nodos
/var/local/log/gridstat.errlog	Archivo de registro de la interfaz gráfica de usuario del Administrador de servidores.	Todos los nodos

Registros de los 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/adx.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/cache-svc.log + /var/local/log/cache-svc.errlog	Registros del servicio de caché.	Nodos de puerta de enlace
/var/local/log/cassandra/system.log	Información para el almacén de metadatos (base de datos Cassandra) que puede usarse si ocurren problemas al añadir nuevos nodos de almacenamiento o si la tarea de reparación de nodetool se queda atascada.	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 Cassandra.	Nodos de almacenamiento
/var/local/log/cassandra-reaper.errlog	Información sobre el error del 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 hayan actualizado desde una versión anterior de StorageGRID. Contiene información obsoleta.	Nodos de almacenamiento
/var/local/log/dds.errlog		Nodos de almacenamiento
/var/local/log/dmv.errlog		Nodos de almacenamiento
/var/local/log/dynip*	Contiene los registros relacionados con el servicio dynip, que supervisa la grid en busca de cambios en las direcciones IP dinámicas 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 el Grid Manager.	Nodos de administración
/var/local/log/hagroups.log	El registro asociado a los grupos de alta disponibilidad.	Nodos de administración y nodos de pasarela
/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 pasarela
/var/local/log/idnt.errlog		Nodos de almacenamiento que ejecutan el servicio ADC
/var/local/log/jaeger.log	El registro asociado al servicio jaeger, que se utiliza para la recopilación de trazas.	Todos los nodos
/var/local/log/kstn.errlog		Nodos de almacenamiento que ejecutan el servicio ADC

Nombre del archivo	Notas	Encontrado en
/var/local/log/lambda*	Contiene los registros del servicio S3 Select.	Nodos de administración y de pasarela Solo algunos nodos de administración y de pasarela contienen este registro. Consulta el "Requisitos y limitaciones de S3 Select para los nodos de administración y Gateway" .
/var/local/log/ldr.errlog		Nodos de almacenamiento
/var/local/log/miscd/*.log	Contiene los registros del servicio MISCd (Information Service Control Daemon), que proporciona una interfaz para consultar y gestionar servicios en otros nodos y para gestionar configuraciones del entorno en el nodo, como consultar el estado de los servicios que se ejecutan en otros nodos.	Todos los nodos
/var/local/log/nginx/*.log	Contiene los registros del servicio nginx, que actúa como mecanismo de autenticación y comunicación segura para varios servicios de grid (como Prometheus y Dynip) para que puedan comunicarse con servicios en otros nodos a través de APIs HTTPS.	Todos los nodos
/var/local/log/nginx-gw/*.log	Contiene registros generales relacionados con el servicio nginx-gw, incluidos los registros de errores y los registros de los puertos de administración restringidos en los Admin Nodes.	Nodos de administración y nodos de pasarela
/var/local/log/nginx-gw/cgr-access.log.gz	Contiene registros de acceso relacionados con el tráfico de replicación entre grids.	Nodos de administración, nodos de puerta de enlace o ambos, según la configuración de la federación de grid. Solo se encuentran en el grid de destino para la replicación entre grids.

Nombre del archivo	Notas	Encontrado en
/var/local/log/nginx-gw/endpoint-access.log.gz	Contiene los registros de acceso del servicio Load Balancer, que proporciona el balanceo de carga del tráfico S3 de los clientes a los Storage Nodes.	Nodos de administración y nodos de pasarela
/var/local/log/persistence*	Contiene los registros del servicio de persistencia, que gestiona los archivos del disco raíz que deben conservarse tras un reinicio.	Todos los nodos
/var/local/log/prometheus.log	Para todos los nodos, contiene el registro del servicio node exporter y el registro del servicio de métricas ade-exporter. 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 que utiliza el servicio RSM para el protocolo Raft.	Nodos de almacenamiento con servicio RSM
/var/local/log/rms.errlog	Contiene los registros del servicio Replicated State Machine Service (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 los nombres de dominio alojados virtualmente en S3. Consulta las instrucciones para implementar aplicaciones cliente de S3.	Nodos de administración y de pasarela
/var/local/log/update-snmp-firewall.*	Contiene registros relacionados con los puertos del firewall que se gestionan para SNMP.	Todos los nodos
/var/local/log/update-sysl.log	Contiene registros relacionados con los cambios realizados en la configuración de syslog del sistema.	Todos los nodos
/var/local/log/update-traffic-classes.log	Contiene registros relacionados con los cambios en la configuración de los clasificadores de tráfico.	Nodos de administración y de pasarela

Nombre del archivo	Notas	Encontrado en
/var/local/log/update-utcn.log	Contiene registros relacionados con el modo Untrusted Client Network en este nodo.	Todos los nodos

Información relacionada

- ["Acerca del archivo bycast.log"](#)
- ["Usa la API de REST de S3"](#)

Registros de implementación y mantenimiento en StorageGRID

Puedes 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 la instalación.	Todos los nodos
/var/local/log/expansion-progress.log	Creado durante las operaciones de ampliación. Contiene un registro de los eventos de ampliación.	Nodos de almacenamiento
/var/local/log/pa-move.log	Creado mientras se ejecutaba el script <code>pa-move.sh</code> .	Nodo de administración principal
/var/local/log/pa-move-new_pa.log	Creado mientras se ejecutaba el script <code>pa-move.sh</code> .	Nodo de administración principal
/var/local/log/pa-move-old_pa.log	Creado mientras se ejecutaba el script <code>pa-move.sh</code> .	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 gestionados por el nodo de administración principal.	Nodos de administración
/var/local/log/send_admin_hw.log	Creado durante la instalación. Contiene información de depuración relacionada con las comunicaciones de un nodo con el nodo de administración principal.	Todos los nodos
/var/local/log/upgrade.log	Creado durante la actualización del software. Contiene un registro de los eventos de actualización del software.	Todos los nodos

Conoce el StorageGRID bycast.log

El archivo `/var/local/log/bycast.log` es el archivo principal de resolución de problemas del software StorageGRID. Hay un archivo `bycast.log` para cada nodo de grid. El archivo contiene mensajes específicos de ese nodo de grid.

El archivo `/var/local/log/bycast-err.log` es un subconjunto de `bycast.log`. Contiene mensajes de gravedad ERROR y CRITICAL.

Si lo deseas, puedes cambiar la ubicación de destino de los registros de auditoría y enviar la información de auditoría a un servidor syslog externo. Los registros locales de auditoría se siguen generando y almacenando cuando se configura un servidor syslog externo. Consulta ["Configura la gestión de registros y el servidor syslog externo"](#).

Rotación de archivos para bycast.log

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

El archivo guardado pasa a llamarse `bycast.log.1`, y el nuevo archivo se llama `bycast.log`. Cuando el nuevo `bycast.log` alcanza 1 GB, `bycast.log.1` cambia de nombre y se comprime para convertirse en `bycast.log.2.gz`, y `bycast.log` pasa a llamarse `bycast.log.1`.

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

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



Si un archivo de registro se ha comprimido, no debes descomprimirlo en la misma ubicación en la que se guardó. Descomprimir el archivo en la misma ubicación puede interferir con los scripts de rotación de registros.

Si lo deseas, puedes cambiar la ubicación de destino de los registros de auditoría y enviar la información de auditoría a un servidor syslog externo. Los registros locales de auditoría se siguen generando y almacenando cuando se configura un servidor syslog externo. Consulta ["Configura la gestión de registros y el servidor syslog externo"](#).

Información relacionada

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

Mensajes en bycast.log

Los mensajes en `bycast.log` son escritos por el ADE (Asynchronous Distributed Environment). ADE es el entorno de ejecución que usan los servicios de cada nodo de la grid.

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
ID del proceso ADE	0357819531
Nombre del módulo	SVMR
Identificador de 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 del estado del volumen 3 ha fallado con el motivo 'TOUT'

Gravedades de los mensajes en bycast.log

Los mensajes en `bycast.log` tienen niveles de gravedad asignados.

Por ejemplo:

- **AVISO** — Se ha producido un evento que debe registrarse. La mayoría de los mensajes de registro se encuentran en este nivel.
- **ADVERTENCIA** — Ha ocurrido una condición inesperada.
- **ERROR** — Se ha producido un error grave que afectará las operaciones.
- **CRÍTICO** — Se ha producido una situación anómala que ha interrumpido el funcionamiento normal. Debes solucionar el problema 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 muestra los códigos no numéricos más comunes en `bycast.log`. El significado exacto de un código no numérico depende del contexto en el que se informa.

Código de error	Significado
SUCS	No hay ningún error
GERR	Desconocido
Cancelar	Cancelado

Código de error	Significado
ABRT	Abortado
TOUT	Tiempo de espera
INVL	No válido
NFND	No encontrado
VERSIÓN	Versión
CONF	Configuración
FALLO	Con errores
ICPL	Incompleto
HECHO	Hecho
SUNV	Servicio no disponible

La siguiente tabla muestra los códigos de error numéricos en `bycast.log`.

Número de error	Código de error	Significado
001	EPERM	Operación no permitida
002	ENOENT	No existe tal archivo ni directorio
003	ESRCH	No existe tal proceso
004	EINTR	Llamada al sistema interrumpida
005	EIO	Error de E/S
006	ENXIO	No existe ningún dispositivo ni dirección de ese tipo
007	E2BIG	La lista de argumentos es demasiado larga
008	ENOEXEC	Error de formato exec
009	EBADF	Número de archivo incorrecto

Número de error	Código de error	Significado
010	ECHILD	No hay procesos secundarios
011	EAGAIN	Inténtalo de nuevo
012	ENOMEM	Memoria insuficiente
013	EACCES	Permiso denegado
014	EFAULT	Dirección incorrecta
015	ENOTBLK	Se requiere un dispositivo de bloque
016	EBUSY	Dispositivo o recurso ocupado
017	EEXIST	El archivo ya existe
018	EXDEV	Enlace entre dispositivos
019	ENODEV	No existe ningún dispositivo de ese tipo
020	ENOTDIR	No es un directorio
021	EISDIR	Es un directorio
022	EINVAL	Argumento no válido
023	ENFILE	Desbordamiento de la tabla de archivos
024	EMFILE	Hay demasiados archivos abiertos
025	ENOTTY	No es una máquina de escribir
026	ETXTBSY	Archivo de texto ocupado
027	EFBIG	El archivo es demasiado grande
028	ENOSPC	No queda espacio en el dispositivo
029	ESPIPE	Búsqueda ilegal
030	EROFS	Sistema de archivos de solo lectura

Número de error	Código de error	Significado
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 interbloqueo de recursos
036	ENAMETOOLONG	El nombre del archivo es demasiado largo
037	ENOLCK	No hay bloqueos de registros disponibles
038	ENOSYS	Función no implementada
039	ENOTEMPTY	El directorio no está vacío
040	ELOOP	Se han encontrado demasiados enlaces simbólicos
041		
042	ENOMSG	No hay ningún mensaje del tipo deseado
043	EIDRM	Identificador eliminado
044	ECHRNG	El número de canal está fuera de rango
045	EL2NSYNC	Nivel 2 no sincronizado
046	EL3HLT	Nivel 3 detenido
047	EL3RST	Restablecimiento de nivel 3
048	ELNRNG	El número de enlace está fuera de rango
049	EUNATCH	El controlador de protocolo no está conectado
050	ENOCSI	No hay ninguna estructura CSI disponible
051	EL2HLT	Nivel 2 detenido

Número de error	Código de error	Significado
052	EBADE	Intercambio 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 un flujo
061	ENODATA	No hay datos disponibles
062	ETIME	El temporizador expiró
063	ENOSR	Recursos de streams agotados
064	ENONET	La máquina no está en la red
065	ENOPKG	El paquete no está instalado
066	EREMOTE	El objeto es remoto
067	ENOLINK	El enlace se ha interrumpido
068	EADV	Error de anuncio
069	ESRMNT	Error de srmount
070	ECOMM	Error de comunicación al enviar
071	EPROTO	Error de protocolo
072	EMULTIHOP	Se intentó multihop

Número de error	Código de error	Significado
073	EDOTDOT	Error específico de RFS
074	EBADMSG	No es un mensaje de datos
075	EOVERFLOW	El valor es demasiado grande para el tipo de datos definido
076	ENOTUNIQ	El nombre no es único en la red
077	EBADFD	Descriptor de archivo en estado anómalo
078	EREMCHG	Dirección remota cambiada
079	ELIBACC	No se puede acceder a una biblioteca compartida necesaria
080	ELIBBAD	Accediendo a una biblioteca compartida dañada
081	ELIBSCN	
082	ELIBMAX	Se está intentando vincular demasiadas bibliotecas compartidas
083	ELIBEXEC	No se puede ejecutar directamente una biblioteca compartida
084	EILSEQ	Secuencia de bytes no válida
085	ERESTART	La llamada al sistema interrumpida debe reiniciarse
086	ESTRPIPE	Error en la canalización de flujos
087	EUSERS	Demasiados usuarios
088	ENOTSOCK	Operación de socket en un elemento que no es un socket
089	EDESTADDRREQ	Dirección de destino requerida
090	EMSGSIZE	Mensaje demasiado largo
091	EPROTOTYPE	Tipo de protocolo incorrecto para el socket

Número de error	Código de error	Significado
092	ENOPROTOOPT	Protocolo no disponible
093	EPROTONOSUPPORT	Protocolo no compatible
094	ESOCKTNOSUPPORT	Tipo de socket no compatible
095	EOPNOTSUPP	Operación no admitida en el punto final de transporte
096	EPFNOSUPPORT	Familia de protocolos no compatible
097	EAFNOSUPPORT	La familia de direcciones no es compatible con el protocolo
098	EADDRINUSE	La dirección ya está en uso
099	EADDRNOTAVAIL	No se puede asignar la dirección solicitada
100	ENETDOWN	La red no funciona
101	ENETUNREACH	La red no está disponible
102	ENETRESET	La red perdió la conexión debido a un reinicio
103	ECONNABORTED	El software provocó que se interrumpiera la conexión
104	ECONNRESET	Conexión restablecida por el interlocutor
105	ENOBUFS	No hay espacio disponible en el búfer
106	EISCONN	El punto final de transporte ya está conectado
107	ENOTCONN	El punto final de transporte no está conectado
108	ESHUTDOWN	No se puede enviar tras el cierre del punto final de transporte
109	DEMASIADAS REFERENCIAS	Demasiadas referencias: no se puede empalmar
110	ETIMEDOUT	Se agotó el tiempo de espera de la conexión
111	ECONNREFUSED	Conexión rechazada

Número de error	Código de error	Significado
112	EHOSTDOWN	El host está inactivo
113	EHOSTUNREACH	No hay ruta al host
114	YA	Operación ya en curso
115	EN PROGRESO	Operación en curso
116		
117	EUCLEAN	Hay que limpiar la estructura
118	ENOTNAM	No es un archivo de tipo XENIX
119	ENAVAIL	No hay semáforos XENIX disponibles
120	EISNAM	Es un archivo de tipo con nombre
121	EREMOTEIO	Error de E/S remota
122	EDQUOT	Cuota superada
123	ENOMEDIUM	No se ha encontrado ningún medio
124	EMEDIUMTYPE	Tipo de soporte incorrecto
125	CANCELADO	Operación cancelada
126	ENOKEY	La clave requerida no está disponible
127	LA CLAVE HA CADUCADO	La clave ha caducado
128	EKEYREVOKED	Se ha revocado la clave
129	EKEYREJECTED	La clave fue rechazada por el servicio
130	EOWNERDEAD	Para mutex robustos: el propietario murió
131	ENOTRECOVERABLE	Para mutex robustos: estado no recuperable

Configura la gestión de registros y el servidor syslog externo

Servidores syslog externos en StorageGRID

Un servidor syslog externo es un servidor ajeno a StorageGRID que puedes usar para recopilar información de auditoría del sistema en una única ubicación. Usar un servidor syslog externo te permite reducir el tráfico de red en tus nodos de administración y gestionar la información de manera más eficiente. Para StorageGRID, el formato de los paquetes de mensajes syslog salientes cumple con RFC 3164.

Los tipos de información de auditoría que puedes 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 elevaciones de privilegios a root
- Registros de la aplicación que podrían solicitarse en caso de que sea necesario abrir un caso de soporte para solucionar un problema que hayas encontrado

Cuándo utilizar un servidor syslog externo

Un servidor syslog externo resulta especialmente útil si tienes una grid grande, usas varios tipos de aplicaciones S3 o quieres conservar todos los datos de auditoría. Enviar información de auditoría a un servidor syslog externo te permite:

- Recopila y gestiona la información de auditoría, como los mensajes de auditoría, los registros de aplicaciones y los eventos de seguridad, de forma más eficiente.
- Reduce el tráfico de red en tus 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 los registros se envían a un servidor syslog externo, los registros individuales que superan los 8,192 bytes se truncan al final del mensaje para ajustarse a las limitaciones habituales de las implementaciones de servidores syslog externos.



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

Cómo configurar un servidor syslog externo

Para saber cómo configurar un servidor syslog externo, consulta ["Configura la gestión de registros y el servidor syslog externo"](#).

Si tienes previsto configurar el uso del protocolo TLS o RELP/TLS, debes tener los siguientes certificados:

- **Certificados CA del servidor:** Uno o varios certificados CA de confianza para verificar el servidor syslog externo en formato PEM. Si no se especifica, se usará el certificado CA predeterminado de Grid.
- **Certificado de cliente:** El certificado de cliente para la autenticación en el servidor syslog externo en codificación PEM.

- **Clave privada del cliente:** clave privada del certificado de cliente en formato PEM.



Si utilizas un certificado de cliente, también debes utilizar una clave privada de cliente. Si facilitas una clave privada cifrada, también debes facilitar la frase de contraseña. No hay un beneficio significativo de seguridad al usar una clave privada cifrada porque tanto la clave como la frase de contraseña deben almacenarse; por simplicidad, se recomienda usar una clave privada sin cifrar, si está disponible.

Cómo calcular el tamaño del servidor syslog externo

Normalmente, tu grid se dimensiona para alcanzar un rendimiento requerido, definido en términos de operaciones S3 por segundo o bytes por segundo. Por ejemplo, podrías tener el requisito de que tu grid gestione 1,000 operaciones S3 por segundo, o 2,000 MB por segundo, de ingesta y recuperación de objetos. Deberías dimensionar tu servidor syslog externo según los requisitos de datos de tu grid.

En esta sección se ofrecen algunas fórmulas heurísticas que te ayudarán a calcular la frecuencia y el tamaño medio de los mensajes de registro de distintos tipos que tu servidor syslog externo debe ser capaz de gestionar, expresados en términos de las características de rendimiento conocidas o deseadas de la grid (operaciones S3 por segundo).

Usa las operaciones de S3 por segundo en las fórmulas de estimación

Si tu grid se dimensionó para un rendimiento expresado en bytes por segundo, debes convertir este dimensionamiento a operaciones S3 por segundo para poder usar las fórmulas de estimación. Para convertir el rendimiento del grid, primero debes determinar el tamaño promedio de los objetos, lo cual puedes hacer usando la información de los registros de auditoría y las métricas existentes (si las hay), o usando tu conocimiento de las aplicaciones que usarán StorageGRID. Por ejemplo, si tu grid se dimensionó para alcanzar un rendimiento de 2,000 MB/segundo y el tamaño promedio de los objetos es de 2 MB, entonces tu grid se dimensionó para poder manejar 1,000 operaciones S3 por segundo (2,000 MB / 2 MB).



Las fórmulas para el dimensionamiento de servidores syslog externos que se incluyen en las secciones siguientes ofrecen estimaciones para casos habituales (en lugar de estimaciones para el peor de los casos). Dependiendo de tu configuración y carga de trabajo, podrías ver una tasa de mensajes syslog o un volumen de datos syslog mayor o menor que el que predicen las fórmulas. Las fórmulas están pensadas solo como una guía.

Fórmulas de estimación para los registros de auditoría

Si no tienes información sobre tu carga de trabajo de S3 aparte del número de operaciones de S3 por segundo que se espera que admita tu grid, puedes estimar el volumen de registros de auditoría que tu servidor syslog externo tendrá que manejar usando las siguientes fórmulas, bajo la suposición de que dejas los niveles de auditoría en los valores predeterminados (todas las categorías en Normal, excepto Storage, que está en Error):

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

Por ejemplo, si tu grid está dimensionada para 1,000 operaciones S3 por segundo, tu servidor syslog externo debería estar dimensionado para admitir 2,000 mensajes syslog por segundo y debería ser capaz de recibir (y normalmente almacenar) datos de registros de auditoría a una velocidad de 1.6 MB por segundo.

Si conoces mejor tu carga de trabajo, podrás realizar estimaciones más precisas. En el caso de los registros de auditoría, las variables adicionales más importantes son el porcentaje de operaciones de S3 que son PUT (frente a GET) y el tamaño medio, en bytes, de los siguientes campos de S3 (las abreviaturas de 4 caracteres utilizadas en la tabla son los nombres de los campos del registro de auditoría):

Código	Campo	Descripción
SACC	Nombre de la cuenta de 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 de tenant de S3 (propietario del bucket)	El nombre de la cuenta de inquilino del propietario del bucket. Se usa para identificar el acceso entre cuentas o el acceso anónimo.
S3BK	Bucket de S3	El nombre del depósito de S3.
S3KY	Clave de S3	El nombre de la clave S3, sin incluir el nombre del bucket. Las operaciones en buckets no incluyen este campo.

Utilicemos la letra P para representar el porcentaje de operaciones de S3 que son PUT, donde $0 \leq P \leq 1$ (así que para una carga de trabajo 100% PUT, $P = 1$, y para una carga de trabajo 100% GET, $P = 0$).

Utilicemos K para representar el tamaño medio de la suma de los nombres de las cuentas de S3, los buckets de S3 y las claves de S3. Supongamos que el nombre de la cuenta de S3 es siempre my-s3-account (13 bytes), que 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 puedes determinar los valores de P y K, puedes estimar el volumen de registros de auditoría que tu servidor syslog externo tendrá que manejar usando las siguientes fórmulas, bajo la suposición de que dejas los niveles de auditoría en los valores predeterminados (todas las categorías en Normal, excepto Storage, que está en Error):

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

Por ejemplo, si tu grid está dimensionada para 1,000 operaciones S3 por segundo, tu carga de trabajo es 50% PUTs, y los nombres de tus cuentas S3, nombres de buckets y nombres de objetos tienen un promedio de 90 bytes, tu servidor externo de syslog debería estar dimensionado para soportar 1,500 mensajes de syslog por segundo y debería poder recibir (y normalmente almacenar) datos de registros 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 asumen el uso de la configuración predeterminada del nivel de auditoría (todas las categorías establecidas en Normal, excepto Storage, que está configurada en Error). No se dispone de fórmulas detalladas para estimar la tasa y el tamaño medio de los

mensajes de auditoría para configuraciones del nivel de auditoría no predeterminadas. Sin embargo, la siguiente tabla puede usarse para hacer una estimación aproximada de la tasa; puedes usar la fórmula de tamaño promedio proporcionada para los registros de auditoría, pero ten en cuenta que probablemente el resultado sea una sobreestimación porque los mensajes de auditoría "adicionales" son, en promedio, más pequeños que los mensajes de auditoría predeterminados.

Estado	Fórmula
Replicación: todos los niveles de auditoría están configurados en Depuración o Normal	Tasa del registro de auditoría = $8 \times$ tasa de operaciones de S3
Código de borrado: todos los niveles de auditoría configurados en Debug o Normal	Utiliza la misma fórmula que para la configuración predeterminada

Fórmulas de estimación para eventos de seguridad

Los eventos de seguridad no están relacionados con las operaciones de S3 y, por lo general, generan un volumen insignificante de registros y datos. Por estos motivos, no se proporcionan fórmulas de estimación.

Fórmulas de estimación para los registros de aplicaciones

Si no tienes información sobre tu carga de trabajo de S3 aparte del número de operaciones de S3 por segundo que se espera que admita tu grid, puedes estimar el volumen de registros de aplicaciones que tu servidor syslog externo tendrá que manejar usando las siguientes fórmulas:

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Así que, por ejemplo, si tu grid está dimensionado para 1,000 operaciones S3 por segundo, tu servidor syslog externo debería estar dimensionado para admitir 3,300 registros de aplicación por segundo y poder recibir (y almacenar) datos de registros de aplicación a una velocidad de aproximadamente 1.2 MB por segundo.

Si conoces mejor tu carga de trabajo, podrás realizar estimaciones más precisas. Para los registros de aplicaciones, las variables adicionales más importantes son la estrategia de protección de datos (replicación vs. código de borrado), el porcentaje de operaciones S3 que son PUT (vs. GET/otras), y el tamaño promedio, en bytes, de los siguientes campos de S3 (las abreviaturas de 4 caracteres usadas en la tabla son los nombres de los campos del registro de auditoría):

Código	Campo	Descripción
SACC	Nombre de la cuenta de 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 de tenant de S3 (propietario del bucket)	El nombre de la cuenta de inquilino del propietario del bucket. Se usa para identificar el acceso entre cuentas o el acceso anónimo.
S3BK	Bucket de S3	El nombre del depósito de S3.

Código	Campo	Descripción
S3KY	Clave de S3	El nombre de la clave S3, sin incluir el nombre del bucket. Las operaciones en buckets no incluyen este campo.

Ejemplos de estimaciones de dimensionamiento

Esta sección explica casos de ejemplo de cómo usar las fórmulas de estimación para grids con los siguientes métodos de protección de datos:

- Replicación
- Codificación de borrado

Si utilizas la replicación para la protección de datos

Sea P el porcentaje de operaciones de S3 que son PUT, donde $0 \leq P \leq 1$ (así que para una carga de trabajo 100% PUT, $P = 1$, y para una carga de trabajo 100% GET, $P = 0$).

Sea K el tamaño medio de la suma de los nombres de las cuentas de S3, los buckets de S3 y las claves de S3. Supón que el nombre de la cuenta de S3 es siempre 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 puedes determinar los valores de P y K , puedes estimar el volumen de registros de aplicación que tu servidor syslog externo tendrá que ser capaz de manejar usando 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
```

Así, por ejemplo, si tu grid está dimensionado para 1,000 operaciones S3 por segundo, tu carga de trabajo es 50% PUTs, y los nombres de tus cuentas S3, nombres de buckets y nombres de objetos tienen un promedio de 90 bytes, tu servidor externo de syslog debería estar dimensionado para soportar 1800 registros de aplicación por segundo y estará recibiendo (y normalmente almacenando) datos de aplicación a una velocidad de 0.5 MB por segundo.

Si utilizas el código de borrado para la protección de datos

Sea P el porcentaje de operaciones de S3 que son PUT, donde $0 \leq P \leq 1$ (así que para una carga de trabajo 100% PUT, $P = 1$, y para una carga de trabajo 100% GET, $P = 0$).

Sea K el tamaño medio de la suma de los nombres de las cuentas de S3, los buckets de S3 y las claves de S3. Supón que el nombre de la cuenta de S3 es siempre 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 puedes determinar los valores de P y K , puedes estimar el volumen de registros de aplicación que tu

servidor syslog externo tendrá que ser capaz de manejar usando las siguientes fórmulas.

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

Así que, por ejemplo, si tu grid está dimensionado para 1,000 operaciones S3 por segundo, tu carga de trabajo es 50% PUTs, y los nombres de tus cuentas S3, buckets y objetos tienen un promedio de 90 bytes, tu servidor externo de syslog debería estar dimensionado para soportar 2,250 registros de aplicación por segundo y debería poder recibir (y normalmente almacenar) datos de aplicación a una velocidad de 0.6 MB por segundo.

Configura la gestión de registros en StorageGRID

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

Todos los nodos de StorageGRID generan mensajes de auditoría y registros para realizar un seguimiento de la actividad y los eventos del sistema. Los mensajes de auditoría y los registros son herramientas esenciales para la supervisión y la resolución de problemas.

Si lo deseas, puedes ["configurar un servidor syslog externo"](#) para guardar la información de auditoría de forma remota. Usar un servidor externo minimiza el impacto en el rendimiento del registro de mensajes de auditoría sin reducir la exhaustividad de los datos de auditoría. Un servidor syslog externo es especialmente útil si tienes una grid grande, usas varios tipos de aplicaciones S3 o quieres conservar todos los datos de auditoría.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- Si planeas configurar un servidor syslog externo, ya revisaste y seguiste las ["consideraciones para usar un servidor syslog externo"](#).
- Si tienes previsto configurar un servidor syslog externo usando el protocolo TLS o RELP/TLS, cuentas con los certificados de CA del servidor y de cliente necesarios, y la clave privada del cliente.

Cambiar los niveles de los mensajes de auditoría

Puedes 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 del almacenamiento de objetos"
Gestión	Normal	"Mensaje de auditoría de gestión"

Categoría de auditoría	Configuración predeterminada	Más información
Lecturas del cliente	Normal	"Mensajes de auditoría de lectura del cliente"
El cliente escribe	Normal	"Mensajes de auditoría de escritura del cliente"
ILM	Normal	"Mensajes de auditoría de ILM"
Replicación entre grids	Error	"CGRR: Solicitud de replicación entre grids"



Durante las actualizaciones, las configuraciones del nivel de auditoría no surtirán efecto de forma inmediata.

Pasos

1. Selecciona **Configuración > Supervisión > Gestión de registros**.
2. Para cada categoría de mensaje de auditoría, selecciona un nivel de auditoría de la lista desplegable:

Nivel de auditoría	Descripción
Apagado	No se registran mensajes de auditoría de la categoría.
Error	Solo se registran los mensajes de error: mensajes de auditoría cuyo código de resultado no sea "successful" (SUCS).
Normal	Se registran los mensajes transaccionales estándar: los mensajes que se indican en estas instrucciones para la categoría.
Depuración	Obsoleto. Este nivel se comporta igual que el nivel de auditoría Normal.

Los mensajes incluidos en cada nivel concreto comprenden aquellos que se registrarían en los niveles superiores. Por ejemplo, el nivel Normal incluye todos los mensajes de error.



Si no necesitas un registro detallado de las operaciones de lectura de los clientes para tus aplicaciones S3, puedes cambiar la configuración de **Lecturas de clientes** a **Error** para reducir el número de mensajes de auditoría registrados en el registro de auditoría.

3. Selecciona **Guardar**.

Define los encabezados de las solicitudes HTTP

Si lo deseas, puedes definir cualquier encabezado de solicitud HTTP que quieras incluir en los mensajes de auditoría de lectura y escritura del cliente.

Pasos

1. En la sección **Encabezados del protocolo de auditoría**, define los encabezados de solicitud HTTP que

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

Utiliza un asterisco (*) como comodín para buscar cero o más caracteres. Utiliza la secuencia de escape (*) para buscar un asterisco literal.

2. Selecciona **Add another header** para crear encabezados adicionales, si es necesario.

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



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

3. Selecciona **Guardar**

Configura la ubicación del registro

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

Si quieres guardar los archivos de registro internamente, selecciona un tenant y un bucket para el almacenamiento de registros y activa el archivado de registros.

Usa un servidor syslog externo

Si lo deseas, puedes configurar un servidor syslog externo para guardar los registros de auditoría, los registros de aplicaciones y los registros de eventos de seguridad en una ubicación fuera de tu grid.



Si no quieres utilizar un servidor syslog externo, omite este paso y ve a [Selecciona la ubicación del registro](#).



Si las opciones de configuración disponibles en este procedimiento no son lo suficientemente flexibles como para satisfacer tus necesidades, se pueden aplicar opciones de configuración adicionales usando los `audit-destinations` endpoints, que están en la sección privada de la API de ["API de gestión de grid"](#). Por ejemplo, puedes usar la API si quieres usar diferentes servidores syslog para distintos grupos de nodos.

Ingresa la información de syslog

Accede al asistente para configurar el servidor syslog externo e introduce la información que StorageGRID necesita para acceder al servidor syslog externo.

Pasos

1. En la pestaña «Nodo local y servidor externo», selecciona **Configurar servidor syslog externo**. O bien, si ya has configurado un servidor syslog externo, selecciona **Editar servidor syslog externo**.

Aparece el asistente para configurar un servidor syslog externo.

2. En el paso **Introducir información de syslog** del asistente, introduce un nombre de dominio completo válido o una dirección IPv4 o IPv6 del servidor syslog externo en el campo **Host**.

3. Introduce el puerto de destino en el servidor syslog externo (debe ser un número entero entre 1 y 65535). El puerto predeterminado es 514.
4. Selecciona el protocolo que se utiliza para enviar la información de auditoría al servidor syslog externo.

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

Todas las opciones de protocolo requieren compatibilidad y configuración por parte del servidor syslog externo. Debes elegir una opción que sea compatible con el servidor syslog externo.



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

5. Selecciona **Continuar**.
6. Si seleccionaste **TLS** o **RELPL/TLS**, sube los certificados de la autoridad de certificación (CA) del servidor, el certificado del cliente y la clave privada del cliente.
 - a. Selecciona **Examinar** para el certificado o la clave que quieras usar.
 - b. Selecciona el certificado o el archivo de clave.
 - c. Selecciona **Abrir** para subir el archivo.

Aparece una marca de verificación verde junto al nombre del certificado o del archivo de clave, notificándote que se ha subido correctamente.

7. Selecciona **Continuar**.

Gestiona el contenido de syslog

Puedes seleccionar qué información enviar al servidor syslog externo.

Pasos

1. En el paso **Gestionar el contenido de syslog** del asistente, selecciona cada tipo de información de auditoría que quieras 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 cuando un usuario inicia sesión como root
 - **Enviar registros de la aplicación:** Envía "[Archivos de registro del software StorageGRID](#)" útil para la resolución de problemas, incluyendo:
 - `broadcast-err.log`
 - `broadcast.log`
 - `jaeger.log`
 - `nms.log` (Solo nodos de administración)
 - `prometheus.log`
 - `raft.log`

▪ `hagroups.log`

- **Enviar registros de acceso:** Envía los registros de acceso HTTP correspondientes a las solicitudes externas dirigidas a Grid Manager, Tenant Manager, los puntos finales del equilibrador de carga configurados y las solicitudes de federación de grid procedentes de sistemas remotos.

2. Utiliza los menús desplegables para seleccionar la gravedad y la facilidad (tipo de mensaje) para cada categoría de información de auditoría que quieras enviar.

Establecer los valores de gravedad y de facility puede ayudarte a agrupar los registros de forma personalizada para facilitar su análisis.

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

Si seleccionas un valor, este se aplicará a todos los mensajes de este tipo. Se perderá la información sobre las diferentes gravedades si sustituyes gravedad por un valor fijo.

Gravedad	Descripción
Passthrough	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 los genera la distribución de Linux en los nodos. • En el caso de los registros de la aplicación, la gravedad varía entre "info" y "notice", dependiendo del tipo de incidencia. Por ejemplo, añadir un servidor NTP y configurar un grupo HA da un valor de "info", mientras que detener intencionadamente el servicio SSM o RSM da un valor de "notice". • Para los registros de acceso, la gravedad es "info".
0	Emergencia: el sistema no funciona
1	Aviso: es necesario 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 **Facility**, selecciona **Passthrough** o selecciona un valor de instalación entre 0 y 23.

Si seleccionas un valor, se aplicará a todos los mensajes de este tipo. La información sobre las diferentes facilities se perderá si sustituyes facility por un valor fijo.

Instalación	Descripción
Passthrough	Cada mensaje enviado al syslog externo debe tener el mismo valor de facility que cuando se registró localmente en el nodo: • Para los registros de auditoría, la instalación enviada al servidor syslog externo es "local7". • Para los eventos de seguridad, los valores de la facility los genera la distribución de Linux en los nodos. • Para los registros de la aplicación, los registros de la aplicación que se envían al servidor syslog externo tienen los siguientes valores de facility: ◦ <code>bcast.log</code>: usuario o demonio ◦ <code>bcast-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 entidad enviada al servidor syslog externo es "local0".
0	kern (mensajes del núcleo)
1	usuario (mensajes a nivel de usuario)
2	correo
3	demonio (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 red)
8	UUCP
9	cron (demonio del reloj)

Instalación	Descripción
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
23	local7

3. Selecciona **Continuar**.

Enviar mensajes de prueba

Antes de empezar a utilizar un servidor syslog externo, debes solicitar que todos los nodos de tu grid envíen mensajes de prueba al servidor syslog externo. Debes utilizar estos mensajes de prueba para validar toda tu infraestructura de recopilación de registros antes de comprometerte a enviar datos al servidor syslog externo.



No utilices la configuración del servidor syslog externo hasta que hayas comprobado que el servidor syslog externo recibió un mensaje de prueba de cada nodo de tu grid y que el mensaje se procesó como esperabas.

Pasos

1. Si no deseas enviar mensajes de prueba porque estás seguro de que tu servidor syslog externo está configurado correctamente y puede recibir información de auditoría de todos los nodos de tu grid, selecciona **Omitir y finalizar**.

Una barra verde indica que la configuración se ha guardado.

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

Los resultados de la prueba se van mostrando continuamente en la página hasta que detienes la prueba. Mientras la prueba está en curso, tus mensajes de auditoría siguen enviándose a los destinos que configuraste previamente.

3. Si aparece algún error durante la configuración del servidor syslog o en tiempo de ejecución, corrígelos y vuelve a seleccionar **Enviar mensajes de prueba**.

Consulta "[Solucionar problemas en un servidor syslog externo](#)" para ayudarte a resolver cualquier error.

4. Espera hasta que veas un banner verde que indique que todos los nodos han superado las pruebas.
5. Comprueba tu servidor syslog para verificar si los mensajes de prueba se reciben y se procesan como esperas.



Si utilizas UDP, comprueba toda tu infraestructura de recopilación de registros. El protocolo UDP no permite una detección de errores tan rigurosa como la de otros protocolos.

6. Selecciona **Detener y finalizar**.

Volverás a la página **Audit and syslog server**. 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 selecciones un destino que incluya el servidor syslog externo.

Selecciona la ubicación del registro

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

StorageGRID utiliza de forma predeterminada los destinos de auditoría de los nodos locales y almacena la información de auditoría en `/var/local/log/localaudit.log`.



Al utilizar `/var/local/log/localaudit.log`, es posible que las entradas del registro de auditoría de Grid Manager y Tenant Manager se envíen a un nodo de almacenamiento. Puedes averiguar qué nodo tiene las entradas más recientes usando el comando `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"`.

Algunos destinos solo están disponibles si has configurado un servidor syslog externo.

Pasos

1. Selecciona **Ubicación del registro > Nodo local y servidor externo**.
2. Para cambiar la ubicación de los registros para los tipos de registro, selecciona otra opción.



Solo los nodos locales y el servidor syslog externo suelen ofrecer un mejor rendimiento.

Opción	Descripción
Solo nodos locales (por defecto)	Los mensajes de auditoría, los registros de eventos de seguridad y los registros de aplicaciones no se envían a los nodos de administración. En su lugar, 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 mediante un sistema de 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 número 22 del archivo de registro, se elimina el archivo de registro más antiguo. De media, se almacenan unos 20 GB de datos de registro en cada nodo. Para almacenar los registros durante un periodo de tiempo prolongado, utiliza un tenant y un bucket para el almacenamiento de registros.
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 (primarios y no primarios): <code>/var/local/audit/export/audit.log</code> • Todos los nodos: El archivo <code>/var/local/log/localaudit.log</code> suele estar vacío o no existir. Podría contener información secundaria, como una copia adicional de algunos mensajes.
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 hayas configurado el servidor syslog externo. Esta opción solo se activa después de haber configurado un servidor syslog externo.
Nodos 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 hayas configurado el servidor syslog externo. Esta opción solo se activa después de haber configurado un servidor syslog externo.

3. Selecciona **Guardar**.

Aparece un mensaje de advertencia.

4. Selecciona **Aceptar** para confirmar que deseas cambiar la ubicación de destino de la información de auditoría.

Los nuevos registros se envían a los destinos que hayas seleccionado. Los registros existentes permanecen en su ubicación actual.

Usa un bucket

Los registros se renuevan periódicamente. Utiliza un bucket de S3 en la misma grid para almacenar los registros durante un periodo de tiempo prolongado.

1. Selecciona **Ubicación de los registros > Usar un bucket**.
2. Marca la casilla **Habilitar registros de archivo**.
3. Si el tenant y el bucket que aparecen en la lista no son los que deseas usar, selecciona **Cambiar tenant y bucket** y luego selecciona **Crear tenant y bucket** o **Seleccionar tenant y bucket**.

Crear inquilino y bucket

- a. Introduce un nuevo nombre de inquilino.
- b. Introduce y confirma una contraseña para el nuevo tenant.
- c. Introduce un nuevo nombre de bucket.
- d. Selecciona **Crear y activar**.

Selecciona el tenant y el bucket

- a. Selecciona un nombre de inquilino en el menú desplegable.
- b. Selecciona un bucket en el menú desplegable.
- c. Selecciona **Seleccionar y activar**.

4. Selecciona **Guardar**.

Los registros se almacenarán en el tenant y el bucket que hayas especificado. El nombre de la clave del objeto para los registros tiene este formato:

```
system-logs/{node_hostname}/{absolute_path_to_log_file_on_node}--  
{last_modified_time}.gz
```

Por ejemplo:

```
system-logs/DC1-SN1/var/local/log/localaudit.log--2025-05-12_13:41:44.gz
```

Usa la supervisión SNMP

Usa la monitorización SNMP en StorageGRID

Si quieres supervisar StorageGRID usando el Protocolo simple de gestión de redes

(SNMP), debes configurar el agente SNMP que viene incluido con StorageGRID.

- ["Configura el agente SNMP"](#)
- ["Actualizar el agente SNMP"](#)

Capacidades

Cada nodo de 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 descriptiva del sistema, como la plataforma y el número de modelo de cada nodo. Cada nodo de StorageGRID también es compatible con un subconjunto de objetos MIB-II.



Consulta ["Accede a los archivos MIB"](#) si quieres descargar los archivos MIB en los nodos de tu grid.

Inicialmente, SNMP está desactivado en todos los nodos. Cuando configuras el agente SNMP, todos los nodos de StorageGRID reciben la misma configuración.

El agente SNMP de StorageGRID es compatible con las tres versiones del protocolo SNMP. Ofrece acceso a la MIB en modo de solo lectura para consultas y puede enviar dos tipos de notificaciones basadas en eventos a un sistema de gestión:

Trampas

Las traps son notificaciones enviadas por el agente SNMP que no requieren confirmación por parte del sistema de gestión. Las traps sirven para notificar al sistema de gestión que algo ha ocurrido dentro de StorageGRID, como que se haya activado una alerta.

Las trampas son compatibles con las tres versiones de SNMP.

Informa

Los «informs» son similares a las «traps», pero requieren una confirmación por parte del sistema de gestión. Si el agente SNMP no recibe una confirmación en un plazo determinado, reenvía el «inform» hasta que se reciba una confirmación o se alcance el número máximo de reintentos.

Los mensajes «inform» son compatibles con SNMPv2c y SNMPv3.

Las notificaciones de trap e inform se envían en los siguientes casos:

- Se activa una alerta predeterminada o personalizada en cualquier nivel de gravedad. Para desactivar las notificaciones SNMP de una alerta, debes ["configurar un silencio"](#) para la alerta. Las notificaciones de alerta las envía el ["Remitente preferido Admin Node"](#).

Cada alerta se asigna a uno de los tres tipos de trap según el nivel de gravedad de la alerta: activeMinorAlert, activeMajorAlert y activeCriticalAlert. Para ver la lista de alertas que pueden activar estos trap, consulta el ["Referencia de alertas"](#).

Compatibilidad con las versiones de SNMP

La tabla ofrece un resumen a grandes rasgos de lo que es compatible con 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 de comunidad	Cadena de comunidad	Usuario del modelo de seguridad basado en usuario (USM)
Notificaciones (TRAP e INFORM)	Solo traps	Atrapa e informa	Atrapa e informa
Autenticación de notificaciones	Comunidad de trampas predeterminada o una cadena de comunidad personalizada para cada destino de trampa	Comunidad de trampas predeterminada o una cadena de comunidad personalizada para cada destino de trampa	Usuario USM para cada destino de trampa

Limitaciones

- StorageGRID admite el acceso a la MIB en modo de solo lectura. No se admite el acceso en modo de lectura/escritura.
- Todos los nodos de la red reciben la misma configuración.
- SNMPv3: StorageGRID no es compatible con el modo de soporte de transporte (TSM).
- SNMPv3: el único protocolo de autenticación compatible es SHA (HMAC-SHA-96).
- SNMPv3: el único protocolo de privacidad compatible es AES.

Configura el agente SNMP en StorageGRID

Puedes configurar el agente SNMP de StorageGRID para que utilice un sistema de gestión SNMP de terceros para acceso de solo lectura a las MIB y notificaciones.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).

Acerca de esta tarea

El agente SNMP de StorageGRID es compatible con SNMPv1, SNMPv2c y SNMPv3. Puedes configurar el agente para una o varias versiones. Para SNMPv3, solo se admite la autenticación mediante User Security Model (USM).

Todos los nodos de la red utilizan la misma configuración SNMP.

Especifica la configuración básica

Como primer paso, activa el agente SNMP de StorageGRID e introduce la información básica.

Pasos

1. Selecciona **Configuración > Supervisión > Agente SNMP**.

Aparece la página del agente SNMP.

2. Para activar el agente SNMP en todos los nodos de la red, marca la casilla **Enable SNMP**.
3. Introduce la siguiente información en la sección Basic configuration.

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 suele ser una dirección de correo electrónico. Este valor se aplica a todos los nodos del sistema StorageGRID. El contacto del sistema puede tener un máximo de 255 caracteres.
Ubicación del sistema	Opcional. La ubicación del sistema StorageGRID, que se devuelve en los mensajes SNMP como sysLocation. La ubicación del sistema puede ser cualquier información que sea útil para identificar dónde se encuentra tu sistema StorageGRID. Por ejemplo, podrías usar la dirección de la calle de una instalación. Este valor se aplica a todos los nodos del sistema StorageGRID. Ubicación del sistema puede tener un máximo de 255 caracteres.
Habilita las notificaciones del agente SNMP	• Si seleccionas esta opción, el agente SNMP de StorageGRID envía notificaciones de trap e inform. • Si no se selecciona, el agente SNMP admite el acceso a la MIB en modo de solo lectura, pero no envía ninguna notificación SNMP.
Habilita las alertas de autenticación	Si seleccionas esta opción, el agente SNMP de StorageGRID envía traps de autenticación si recibe mensajes de protocolo autenticados de forma incorrecta.

Introduce las cadenas de la comunidad

Si utilizas SNMPv1 o SNMPv2c, completa la sección Cadenas de comunidad.

Cuando el sistema de gestión 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 gestión.

Pasos

1. Para **Comunidad de solo lectura**, opcionalmente introduce una cadena de comunidad para permitir el acceso de solo lectura a la MIB en las direcciones de los agentes IPv4 e IPv6.



Para garantizar la seguridad de tu sistema StorageGRID, no utilices "public" como cadena de comunidad. Si dejas este campo en blanco, el agente SNMP usa el grid ID de tu sistema StorageGRID como cadena de comunidad.

Cada cadena de comunidad puede tener un máximo de 32 caracteres y no puede contener caracteres de espacio en blanco.

2. Selecciona **Add another community string** para añadir cadenas adicionales.

Se permiten hasta cinco cadenas.

Crear destinos de trap

Utiliza la pestaña «Destinos de trap» de la sección «Otras configuraciones» para definir uno o varios destinos para las notificaciones de trap o inform de StorageGRID. Al habilitar el agente SNMP y seleccionar **Guardar**, StorageGRID envía notificaciones a cada destino definido cuando se activan las alertas. También se envían notificaciones estándar para las entidades MIB-II compatibles (por ejemplo, ifDown y coldStart).

Pasos

1. En el campo **Comunidad de traps predeterminada**, opcionalmente introduce la cadena de comunidad predeterminada que quieras usar para los destinos de traps SNMPv1 o SNMPv2.

Si es necesario, puedes indicar una cadena de comunidad diferente («personalizada») al definir un destino de trap específico.

Comunidad de trampa predeterminada puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

2. Para añadir un destino de captura, selecciona **Crear**.
3. Selecciona qué versión de SNMP se usará para este destino de trap.
4. Rellena el formulario «Crear destino de trampa» para la versión que seleccionaste.

SNMPv1

Si seleccionaste SNMPv1 como versión, completa estos campos.

Campo	Descripción
Tipo	Debe ser Trap para SNMPv1.
Host	Una dirección IPv4 o IPv6 o un nombre de dominio completo (FQDN) para recibir la trampa.
Puerto	Utiliza 162, que es el puerto estándar para las alertas SNMP, a menos que tengas que usar otro valor.
Protocolo	Utiliza UDP, que es el protocolo estándar para las trampas SNMP, a menos que necesites usar TCP.
Cadena de comunidad	Usa la comunidad de trap predeterminada, si se especificó alguna, o ingresa una cadena de comunidad personalizada para este destino de trap. La cadena personalizada de la comunidad puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

SNMPv2c

Si seleccionaste SNMPv2c como versión, completa estos campos.

Campo	Descripción
Tipo	Si el destino se utilizará para traps o informs.
Host	Una dirección IPv4 o IPv6 o un FQDN para recibir la trampa.
Puerto	Utiliza 162, que es el puerto estándar para las alertas SNMP, a menos que tengas que usar otro valor.
Protocolo	Utiliza UDP, que es el protocolo estándar para las trampas SNMP, a menos que necesites usar TCP.
Cadena de comunidad	Usa la comunidad de trap predeterminada, si se especificó alguna, o ingresa una cadena de comunidad personalizada para este destino de trap. La cadena personalizada de la comunidad puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.

SNMPv3

Si has seleccionado SNMPv3 como versión, rellena estos campos.

Campo	Descripción
Tipo	Si el destino se utilizará para traps o informs.
Host	Una dirección IPv4 o IPv6 o un FQDN para recibir la trampa.
Puerto	Utiliza 162, que es el puerto estándar para las alertas SNMP, a menos que tengas que usar otro valor.
Protocolo	Utiliza UDP, que es el protocolo estándar para las trampas SNMP, a menos que necesites usar TCP.
Usuario de USM	El usuario de USM que se utilizará para la autenticación. • Si seleccionaste Trap, solo se muestran los usuarios de USM que no tienen IDs de motor autorizados. • Si seleccionaste Inform, solo se muestran los usuarios de USM con IDs de motor autorizados. • Si no aparece ningún usuario: i. Crea y guarda el destino de la trampa. ii. Entra en Crear usuarios de USM y crea el usuario. iii. Vuelve a la pestaña «Destinos de la trampa», selecciona el destino guardado en la tabla y selecciona Editar. iv. Selecciona el usuario.

5. Selecciona **Crear**.

Se crea el destino de la trampa y se añade a la tabla.

Crear direcciones de agentes

Si lo deseas, utiliza la pestaña «Direcciones del agente» de la sección «Otras configuraciones» para especificar una o varias «direcciones de escucha». Estas son las direcciones de StorageGRID en las que el agente SNMP puede recibir consultas.

Si no configuras una dirección de agente, la dirección de escucha predeterminada es el puerto UDP 161 en todas las redes StorageGRID.

Pasos

1. Selecciona **Crear**.
2. Introduce la siguiente información.

Campo	Descripción
Protocolo de Internet	Si esta dirección utilizará IPv4 o IPv6. Por defecto, SNMP utiliza IPv4.
Protocolo de transporte	Si esta dirección usará UDP o TCP. Por defecto, SNMP utiliza UDP.
Red de StorageGRID	En qué red de StorageGRID estará a la escucha el agente. • Redes Grid, Admin y Client: el agente SNMP estará a la escucha de consultas en las tres redes. • Red de grid • Red de administración • Red de clientes Nota: Si utilizas la red de clientes para datos no seguros y creas una dirección de agente para la red de clientes, ten 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 puedes introducir cualquier número de puerto que no esté en uso. Nota: Al guardar el agente SNMP, StorageGRID abre automáticamente los puertos de la dirección del agente en el cortafuegos interno. Debes asegurarte de que cualquier cortafuegos externo permita el acceso a estos puertos.

3. Selecciona **Crear**.

Se crea la dirección del agente y se añade a la tabla.

Crear usuarios de USM

Si utilizas SNMPv3, usa la pestaña «Usuarios de USM» en la sección «Otras configuraciones» para definir los usuarios de USM que están autorizados a consultar la MIB o a recibir traps e informs.



Para los destinos de *trap* de SNMPv3, se recomienda crear un usuario de USM para cada nodo de administración. Si cada nodo de administración no tiene un usuario de USM, tu sistema de gestión podría dejar de recibir notificaciones si el nodo de administración principal deja de funcionar.



Los destinos *inform* de SNMPv3 deben tener usuarios con ID de motor. Los destinos *trap* de SNMPv3 no pueden tener usuarios con ID de motor.

Estos pasos no aplican si solo usas SNMPv1 o SNMPv2c.

Pasos

1. Selecciona **Crear**.
2. Introduce 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 después de crear el usuario.
Acceso de solo lectura a la MIB	Si se selecciona, este usuario debería tener acceso de solo lectura a la MIB.
ID de motor autorizado	Si este usuario se va a usar en un destino inform, el ID de motor de autoridad para este usuario. Introduce entre 10 y 64 caracteres hexadecimales (5 a 32 bytes) sin espacios. Este valor es obligatorio para los usuarios de USM que se seleccionarán en los destinos de trap para informs. Este valor no está permitido para los usuarios de USM que se seleccionarán en los destinos de trap para traps. Nota: Este campo no aparece si has seleccionado Acceso a la MIB de solo lectura porque los usuarios de USM con acceso a la MIB de solo lectura no pueden tener ID de motor.
Nivel de seguridad	El nivel de seguridad del usuario USM: • authPriv: Este usuario se comunica mediante autenticación y privacidad (encriptación). Debes especificar un protocolo de autenticación y una contraseña, así como un protocolo de privacidad y una contraseña. • authNoPriv: Este usuario se comunica con autenticación y sin privacidad (sin cifrado). Debes especificar un protocolo de autenticación y una contraseña.
Protocolo de autenticación	Configúralo siempre en SHA, que es el único protocolo compatible (HMAC-SHA-96).
Password	La contraseña que utilizará este usuario para autenticarse.
Protocolo de privacidad	Solo se muestra si seleccionaste authPriv y siempre está configurado en AES, que es el único protocolo de privacidad compatible.

Campo	Descripción
Password	Se muestra únicamente si has seleccionado authPriv . La contraseña que este usuario usará para privacidad.

3. Selecciona **Crear**.

Se crea el usuario USM y se añade a la tabla.

4. Cuando hayas terminado de configurar el agente SNMP, selecciona **Guardar**.

La nueva configuración del agente SNMP se activa.

Actualiza el agente SNMP de StorageGRID

Puedes desactivar las notificaciones SNMP, actualizar las cadenas de comunidad o añadir o eliminar direcciones de agentes, usuarios de USM y destinos de traps.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).

Acerca de esta tarea

Consulta ["Configura el agente SNMP"](#) para obtener más información sobre cada campo de la página del agente SNMP. Debes seleccionar **Guardar** en la parte inferior de la página para aplicar los cambios que realices en cada pestaña.

Pasos

1. Selecciona **Configuración > Supervisión > Agente SNMP**.

Aparece la página del agente SNMP.

2. Para desactivar el agente SNMP en todos los nodos de la red, desmarca la casilla **Habilitar SNMP** y selecciona **Guardar**.

Si vuelves a activar el agente SNMP, se conservarán todos los ajustes de configuración SNMP anteriores.

3. Opcionalmente, actualiza la información en la sección de configuración básica:

- Según sea necesario, actualiza **System contact** y **System location**.
- Si lo deseas, marca o desmarca la casilla **Habilitar notificaciones del agente SNMP** para controlar si el agente SNMP de StorageGRID envía notificaciones de tipo trap e inform.

Cuando esta casilla no está marcada, el agente SNMP admite el acceso a la MIB en modo de solo lectura, pero no envía notificaciones SNMP.

- Si lo deseas, marca o desmarca la casilla **Habilitar traps de autenticación** para controlar si el agente SNMP de StorageGRID envía traps de autenticación cuando recibe mensajes de protocolo autenticados de forma incorrecta.

4. Si utilizas SNMPv1 o SNMPv2c, puedes actualizar o añadir una **comunidad de solo lectura** en la sección Cadenas de comunidad.

5. Para actualizar los destinos de captura, selecciona la pestaña Destinos de captura en la sección Otras configuraciones.

Utiliza esta pestaña para definir uno o varios destinos para las notificaciones de trap o inform de StorageGRID. Cuando actives el agente SNMP y selecciones **Guardar**, StorageGRID envía notificaciones a cada destino definido cuando se activan las alertas. También se envían notificaciones estándar para las entidades MIB-II compatibles (por ejemplo, ifDown y coldStart).

Para obtener más información sobre qué datos hay que introducir, consulta ["Crear destinos de trap"](#).

- Opcionalmente, actualiza o elimina la comunidad de trap predeterminada.

Si eliminas la comunidad de trampa predeterminada, primero debes asegurarte de que cualquier destino de trampa existente utilice una cadena de comunidad personalizada.

- Para añadir un destino de captura, selecciona **Crear**.
- Para editar un destino de trampa, selecciona el botón de opción y selecciona **Editar**.
- Para eliminar un destino de trampa, selecciona el botón de opción y selecciona **Eliminar**.
- Para guardar los cambios, selecciona **Guardar** en la parte inferior de la página.

6. Para actualizar las direcciones de los agentes, selecciona la pestaña Direcciones de los agentes en la sección Otras configuraciones.

Utiliza esta pestaña para especificar una o varias «direcciones de escucha». Estas son las direcciones de StorageGRID en las que el agente SNMP puede recibir consultas.

Para obtener más información sobre qué datos hay que introducir, consulta ["Crear direcciones de agentes"](#).

- Para añadir la dirección de un agente, selecciona **Create**.
- Para editar la dirección de un agente, selecciona el botón de opción y selecciona **Editar**.
- Para eliminar la dirección de un agente, selecciona el botón de opción y selecciona **Eliminar**.
- Para guardar los cambios, selecciona **Guardar** en la parte inferior de la página.

7. Para actualizar los usuarios de USM, selecciona la pestaña Usuarios de USM en la sección Otras configuraciones.

Utiliza esta pestaña para definir los usuarios de USM que están autorizados a consultar el MIB o a recibir traps e informs.

Para obtener más información sobre qué datos hay que introducir, consulta ["Crear usuarios de USM"](#).

- Para añadir un usuario de USM, selecciona **Create**.
- Para editar un usuario de USM, selecciona el botón de opción y selecciona **Editar**.

No se puede cambiar el nombre de usuario de un usuario existente de USM. Si necesitas cambiar un nombre de usuario, debes eliminar el usuario y crear uno nuevo.



Si añades o eliminas el ID de motor autoritativo de un usuario y dicho usuario está seleccionado actualmente para un destino, debes editar o eliminar el destino. De lo contrario, se producirá un error de validación al guardar la configuración del agente SNMP.

- Para eliminar un usuario de USM, selecciona el botón de opción y selecciona **Eliminar**.



Si el usuario que has eliminado está seleccionado actualmente como destino de una trampa, debes modificar o eliminar dicho destino. De lo contrario, se produce un error de validación al guardar la configuración del agente SNMP.

- Para guardar los cambios, selecciona **Guardar** en la parte inferior de la página.

8. Cuando hayas actualizado la configuración del agente SNMP, selecciona **Guardar**.

Accede a los archivos MIB de StorageGRID

Los archivos MIB contienen definiciones e información sobre las propiedades de los recursos y servicios gestionados de los nodos en tu grid. Puedes acceder a los archivos MIB que definen los objetos y las notificaciones para StorageGRID. Estos archivos pueden ser útiles para supervisar tu grid.

Consulta ["Usa la supervisión SNMP"](#) para obtener más información sobre SNMP y los archivos MIB.

Accede a los archivos MIB

Sigue estos pasos para acceder a los archivos MIB.

Pasos

1. Selecciona **Configuración > Supervisión > Agente SNMP**.
2. En la página del agente SNMP, selecciona el archivo que quieras descargar:
 - **NETAPP-STORAGEGRID-MIB.txt**: Define la tabla de alertas y las notificaciones (traps) a las que se puede acceder desde todos los nodos de administración.
 - **ES-NETAPP-06-MIB.mib**: Define objetos y notificaciones para los dispositivos basados en E-Series.
 - **MIB_1_10.zip**: Define objetos y notificaciones para dispositivos con interfaz BMC.



También puedes acceder a los archivos MIB en la siguiente ubicación en cualquier nodo de StorageGRID: `/usr/share/snmp/mibs`

3. Para extraer los OID de StorageGRID del archivo MIB:

- a. Obtén el OID de la raíz de la MIB de StorageGRID:

```
root@user-adm1:~ # snmptranslate -On -IR storagegrid
```

Resultado: `.1.3.6.1.4.1.789.28669` (28669 siempre es el OID de StorageGRID)

- b. Busca el OID de StorageGRID en todo el árbol (utilizando `paste` para unir las líneas):

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



El comando `snmptranslate` tiene muchas opciones que son útiles para explorar el MIB. Este comando está disponible en cualquier nodo de StorageGRID.

Contenido del archivo MIB

Todos los objetos están bajo el OID de StorageGRID.

Nombre del objeto	Identificador de objeto (OID)	Descripción
		El módulo MIB para las entidades StorageGRID de NetApp.

Objetos MIB

Nombre del objeto	Identificador de objeto (OID)	Tipo	Acceso	Módulo MIB	Descripción
activeAlertCount		Integer32	Solo lectura	NETAPP-STORAGEGRID-MIB	El número de alertas activas en la activeAlertTable.
activeAlertTable		Secuencia de ActiveAlertEntry	No accesible	NETAPP-STORAGEGRID-MIB	Una tabla con las alertas activas en StorageGRID.
activeAlertEntry		Secuencia	No accesible	NETAPP-STORAGEGRID-MIB	Una única alerta de StorageGRID, indexada por ID de alerta.
activeAlertId		Cadena de octetos	Solo lectura	NETAPP-STORAGEGRID-MIB	El identificador de la alerta. Único solo dentro del conjunto actual de alertas activas.
activeAlertName		Cadena de octetos	Solo lectura	NETAPP-STORAGEGRID-MIB	El nombre de la alerta.
activeAlertInstance		Cadena de octetos	Solo lectura	NETAPP-STORAGEGRID-MIB	El nombre de la entidad que generó la alerta, normalmente el nombre de nodo.
activeAlertSeverity		Cadena de octetos	Solo lectura	NETAPP-STORAGEGRID-MIB	La gravedad de la alerta.
activeAlertStartTime		Fecha y hora	Solo lectura	NETAPP-STORAGEGRID-MIB	La hora en la que se activó la alerta.

Recopila datos adicionales de StorageGRID

Supervisa el rendimiento de PUT y GET en StorageGRID

Puedes supervisar el rendimiento de determinadas operaciones, como el almacén de objetos y la recuperación, para ayudar a identificar cambios que puedan requerir una investigación más detallada.

Acerca de esta tarea

Para supervisar el rendimiento de las operaciones PUT y GET, puedes ejecutar comandos S3 directamente desde una estación de trabajo o usando la aplicación de código abierto S3tester. Usar estos métodos te permite evaluar el rendimiento independientemente de factores que son externos a StorageGRID, como problemas con una aplicación cliente o con una red externa.

Al realizar pruebas de operaciones PUT y GET, sigue estas directrices:

- Utiliza tamaños de objetos comparables a los que sueles incorporar a tu grid.
- Realiza operaciones tanto en sitios locales como remotos.

Los mensajes en la "[registro de auditoría](#)" indican el tiempo total necesario para ejecutar ciertas operaciones. Por ejemplo, para determinar el tiempo total de procesamiento de una solicitud S3 GET, puedes revisar el valor del atributo TIME en el mensaje de auditoría SGET. También puedes 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, fíjate en el tiempo medio necesario para atender una solicitud, así como en el rendimiento global que puedes alcanzar. Repite las mismas pruebas con regularidad y anota los resultados, para que puedas identificar tendencias que puedan requerir investigación.

- Puedes "[Descarga S3tester desde GitHub](#)".

Supervisa las operaciones de verificación de objetos en StorageGRID

El sistema StorageGRID puede verificar la integridad de los datos de objetos en los nodos de almacenamiento, comprobando si hay objetos dañados o que faltan.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "[navegador web compatible](#)".
- Tienes el "[Permiso de mantenimiento o acceso de usuario raíz](#)".

Acerca de esta tarea

Dos "[procesos de verificación](#)" trabajan juntos para garantizar la integridad de los datos:

- La **verificación de antecedentes** se ejecuta automáticamente y comprueba de forma continua la corrección de los datos de los objetos.

La verificación en segundo plano comprueba de forma automática y continua todos los nodos de almacenamiento para determinar si hay copias dañadas de datos de objetos replicados y con código de borrado. Si se detectan problemas, el sistema StorageGRID intenta automáticamente sustituir los datos de objetos dañados por copias almacenadas en otras partes del sistema. La verificación en segundo plano no se ejecuta en los objetos de un Cloud Storage Pool.



La alerta **Se ha detectado un objeto dañado no identificado** se activa si el sistema detecta un objeto dañado que no se puede corregir automáticamente.

- **La comprobación de la existencia de objetos** puede ser activada por un usuario para verificar más rápido la existencia (aunque no la corrección) de los datos de un objeto.

La comprobación de la existencia de objetos verifica si todas las copias replicadas de los objetos y los fragmentos con código de borrado esperados existen en un Storage Node. La comprobación de la existencia de objetos ofrece una forma de verificar la integridad de los dispositivos de almacenamiento, especialmente si un problema reciente de hardware pudo haber afectado la integridad de los datos.

Debes revisar periódicamente los resultados de las verificaciones de antecedentes y de la existencia de objetos. Investiga inmediatamente cualquier caso de datos de objetos dañados o que falten para determinar la causa raíz.

Pasos

1. Revisa los resultados de las comprobaciones de antecedentes:
 - a. Selecciona **Nodos > Storage Node > Objetos**.
 - b. Comprueba los resultados de la verificación:
 - Para comprobar la verificación de los datos de los objetos replicados, consulta los atributos de la sección Verificación.

Verification		
Status: ?	No errors	
Percent complete: ?	0.00%	
Average stat time: ?	0.00 microseconds	
Objects verified: ?	0	
Object verification rate: ?	0.00 objects / second	
Data verified: ?	0 bytes	
Data verification rate: ?	0.00 bytes / second	
Missing objects: ?	0	
Corrupt objects: ?	0	
Corrupt objects unidentified: ?	0	
Quarantined objects: ?	0	

- Para comprobar la verificación de fragmentos con código de borrado, selecciona **Storage Node > ILM** y consulta los atributos en la sección de 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	

Selecciona el signo de interrogación (?) junto al nombre de un atributo para mostrar el texto de ayuda.

2. Revisa los resultados de los trabajos de comprobación de la existencia de objetos:
 - a. Selecciona **Mantenimiento > Comprobación de existencia de objetos > Historial de trabajos**.
 - b. Revisa la columna «Copias de objetos perdidas detectadas». Si algún trabajo ha dado como resultado 100 o más copias de objetos perdidas y se ha activado la alerta **Objetos potencialmente perdidos**, ponte en contacto con 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

☐	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

Revisa los mensajes de auditoría de StorageGRID

Los mensajes de auditoría pueden ayudarte a comprender mejor el funcionamiento detallado de tu sistema StorageGRID. Puedes utilizar los registros de auditoría para resolver problemas y evaluar el rendimiento.

Durante el funcionamiento normal del sistema, todos los servicios de StorageGRID generan mensajes de auditoría, como sigue:

- Los mensajes de auditoría del sistema se refieren al propio sistema de auditoría, a los estados de los nodos de grid, a la actividad de tareas en todo el sistema y a las operaciones de copia de seguridad de servicios.
- Los mensajes de auditoría del almacenamiento de objetos están relacionados con el almacenamiento y la gestión de objetos dentro de StorageGRID, lo que incluye el almacenamiento y la recuperación de objetos, las transferencias entre nodos de la red y las verificaciones.
- Los mensajes de auditoría de lectura y escritura del cliente se registran cuando una aplicación cliente de S3 hace una solicitud para crear, modificar o recuperar un objeto.
- Los mensajes de auditoría de gestión registran las solicitudes de los usuarios a la Management API.

Cada nodo de administración almacena los mensajes de auditoría en archivos de texto. El recurso compartido de auditoría contiene el archivo activo (audit.log) así como los registros de auditoría comprimidos de días anteriores. Cada nodo de la red también almacena una copia de la información de auditoría generada en el propio nodo.

Puedes acceder a los archivos de auditoría directamente desde la línea de comandos del Admin Node.

StorageGRID puede enviar información de auditoría de forma predeterminada, o puedes cambiar el destino:

- StorageGRID utiliza de forma predeterminada los destinos de auditoría de los nodos locales.
- Las entradas del registro de auditoría de Grid Manager y Tenant Manager podrían enviarse a un nodo de almacenamiento.
- Si lo deseas, puedes cambiar la ubicación de los registros de auditoría y enviar la información de auditoría a un servidor syslog externo. Los registros locales de auditoría se siguen generando y almacenando cuando se configura un servidor syslog externo.
- ["Infórmate sobre cómo configurar la gestión de registros"](#).

Para obtener más información sobre el archivo de auditoría, el formato de los mensajes de auditoría, los tipos de mensajes de auditoría y las herramientas disponibles para analizarlos, consulta ["Revisar los registros de auditoría"](#).

Recopila archivos de registro de StorageGRID y datos del sistema

Puedes recuperar los archivos de registro y los datos del sistema de StorageGRID, incluidos los datos de configuración, y enviarlos al soporte técnico.

Antes de empezar

- Has iniciado sesión en el Grid Manager en cualquier nodo de administración usando una ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).
- Tienes la frase de contraseña de aprovisionamiento.

Acerca de esta tarea

Utiliza el Grid Manager para recopilar "[archivos de registro](#)", datos del sistema y datos de configuración de cualquier nodo de la red durante el periodo de tiempo que elijas. Los datos se recopilan y archivan en un archivo `.tar.gz` que luego puedes descargar en tu ordenador local o enviar al soporte técnico.

Si lo deseas, puedes cambiar la ubicación de destino de los registros de auditoría y enviar la información de auditoría a un servidor syslog externo. Los registros locales de auditoría se siguen generando y almacenando cuando se configura un servidor syslog externo. Consulta "[Configura la gestión de registros y el servidor syslog externo](#)".

Pasos

1. Selecciona **Soporte > Herramientas > Recopilación de registros**. Se muestra una tabla con los nodos.
2. Selecciona los nodos de la grid de los que deseas recopilar los archivos de registro.

Puedes ordenar por nombre de nodo, sitio y tipo de nodo. Las columnas Site y Node type contienen filtros para seleccionar por sitios y tipos de nodo individuales.

3. Selecciona **Continuar**.
4. Selecciona el intervalo de fechas y horas de los datos que se incluirán en los archivos de registro.

Si seleccionas un periodo de tiempo muy largo o recopilas registros de todos los nodos en una grid grande, el archivo de registros podría llegar a ser demasiado grande para almacenarse en un nodo o demasiado grande para que un Admin Node lo recopile para su descarga. Si ocurre cualquiera de estos escenarios, reinicia la recopilación de registros con un conjunto de datos más pequeño.

5. Selecciona los tipos de registros que deseas recopilar.
 - **Registros de aplicaciones:** registros específicos de cada aplicación que el soporte técnico utiliza con mayor frecuencia para la resolución de 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 usados para la depuración de red.
 - **Base de datos Prometheus:** métricas de series temporales de los servicios en todos los nodos.
6. Si lo deseas, puedes utilizar el cuadro de texto **Notas** para introducir notas sobre los archivos de registro que estás recopilando.

Puedes utilizar estas notas para proporcionar información de soporte técnico sobre el problema que te llevó a recopilar los archivos de registro. Tus notas se añaden a un archivo llamado `info.txt`, junto con otra información sobre la recopilación de archivos de registro. El archivo `info.txt` se guarda en el paquete de archivo de los archivos de registro.

7. En el cuadro de texto **Contraseña de aprovisionamiento**, introduce la contraseña de aprovisionamiento de tu sistema StorageGRID.
8. Selecciona **Recopilar registros**.

Puedes utilizar la página de recopilación de logs para supervisar el progreso de la recopilación de archivos de log de cada nodo de grid.

Si recibes un mensaje de error sobre el tamaño de los registros, intenta recopilar los registros durante un periodo de tiempo más corto o para menos nodos.

9. Si falla la recopilación de registros:

- Si aparece el mensaje «Error en la recopilación de registros», puedes volver a intentar la recopilación de registros o finalizar la sesión sin volver a intentarlo.
- Si aparece el mensaje «La recopilación de registros ha fallado parcialmente», puedes volver a intentar la recopilación de registros, finalizar la sesión, descargar el archivo de registro parcial o enviar dicho archivo a AutoSupport.

10. Una vez finalizada la recopilación de los archivos de registro:

- Selecciona **Descargar** para descargar el archivo `.tar.gz`.
- Selecciona **Enviar a AutoSupport** para enviar el archivo `.tar.gz` al soporte técnico.

El `.tar.gz` archivo contiene todos los archivos de registro de todos los nodos de la grid donde la recopilación de registros fue exitosa. El archivo combinado `.tar.gz` contiene un archivo de registro archivado por cada nodo de la grid.

El asunto del paquete AutoSupport es `USER_TRIGGERED_SUPPORT_BUNDLE`.

11. Selecciona **Finalizar**.



El archivo `.tar.gz` se elimina al seleccionar **Finalizar**. Asegúrate de descargar o enviar el archivo primero.

Activar manualmente un paquete de StorageGRID AutoSupport

Para ayudar al soporte técnico a solucionar problemas con tu sistema StorageGRID, puedes activar manualmente el envío de un paquete de AutoSupport.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes acceso Root u otro permiso de configuración de grid.

Pasos

1. Selecciona **Soporte > Herramientas > AutoSupport**.
2. En la pestaña **Acciones**, selecciona **Enviar AutoSupport activado por el usuario**.

StorageGRID intenta enviar un paquete de AutoSupport al sitio de soporte de NetApp. Si el intento tiene éxito, se actualizan los valores de **Resultado más reciente** y **Hora del último éxito** en la pestaña **Resultados**. Si hay algún problema, el valor de **Resultado más reciente** se actualiza a "Fallido" y StorageGRID no vuelve a intentar enviar el paquete de AutoSupport.

3. Después de 1 minuto, actualiza la página AutoSupport en tu navegador para acceder a los resultados más recientes.



Además, puedes ["recopilar archivos de registro y datos del sistema más exhaustivos"](#) y enviarlos al sitio de soporte de NetApp.

Revisa las métricas de soporte de StorageGRID

A la hora de resolver un problema, puedes colaborar con el soporte técnico para revisar métricas y gráficos detallados de tu sistema StorageGRID.

Antes de empezar

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

Acerca de esta tarea

La página «Métricas» te 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 de Métricas están destinadas al soporte técnico. Algunas funciones y opciones de menú dentro de estas herramientas no están operativas de forma intencionada y están sujetas a cambios. Consulta la lista de ["Métricas de Prometheus más utilizadas"](#).

Pasos

1. Siguiendo las instrucciones del soporte técnico, selecciona **Support > Tools > Metrics**.

Aquí tienes un ejemplo de la página de Métricas:

Metrics

Access charts and metrics to help troubleshoot issues.

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

Prometheus is an open-source toolkit for collecting metrics. The Prometheus interface allows you to query the current values of metrics and to view charts of the values over time. Access the Prometheus interface using the link below. You must be signed in to the Grid Manager.

[https://](#)

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values. Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

ADE	Cloud Storage Pool Overview	Platform Services Processing
Account Service Overview	Decommission	Replicated Read Path Overview
Alertmanager	Erasure Coding - ADE	S3 - Node
Appliance Hardware Status	Erasure Coding - Overview	S3 Control
Audit Overview	Grid	S3 Overview
Bucket Cache	ILM	S3 Select
Cache Service	Identity Service Overview	Site
Cassandra Cluster Overview	Ingests	Support
Cassandra Network Overview	Node	SSD - Warranty
Cassandra Node Overview	Node (Internal Use)	Traces
Cassandra Table Cleanup	Object Chunk Leak Overview	Traffic Classification Policy
Chunk - Operations Overview	Object Serialization Mapping	Usage Processing
Chunk - Filesystem Latency Overview	OSL - AsyncIO	Virtual Memory (vmstat)
Chunk - Filesystem Latency Details	Platform Services Commits	
Cross Grid Replication	Platform Services Overview	

2. Para consultar los valores actuales de las métricas de StorageGRID y ver gráficos de la evolución de

dichos valores a lo largo del tiempo, haz clic en el enlace de la sección Prometheus.

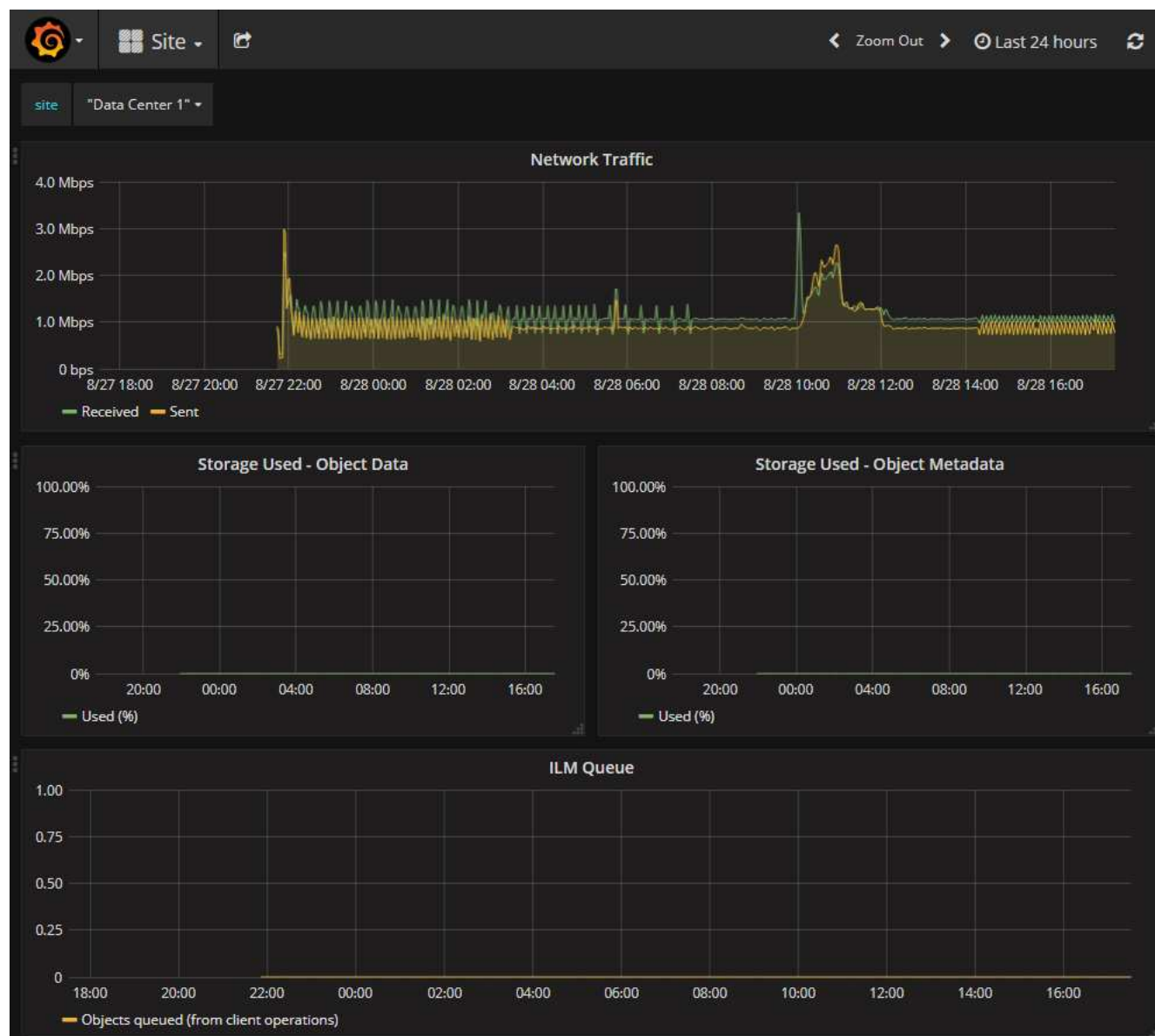
Aparece la interfaz de Prometheus. Puedes utilizar esta interfaz para ejecutar consultas sobre las métricas disponibles de StorageGRID y para representar gráficamente las métricas de StorageGRID a lo largo del tiempo.



Las métricas que incluyen *private* en su nombre están destinadas exclusivamente a uso interno y pueden cambiar entre versiones de StorageGRID sin previo aviso.

3. Para acceder a los paneles ya creados que contienen gráficos de las métricas de StorageGRID a lo largo del tiempo, haz clic en los enlaces de la sección Grafana.

Aparece la interfaz de Grafana para el enlace que seleccionaste.



Cambiar la priorización de I/O en StorageGRID

La priorización de entrada/salida (E/S) te permite cambiar las prioridades relativas de las operaciones de E/S en el grid.

De forma predeterminada, el tráfico de E/S PUT y GET de los clientes tiene la máxima prioridad frente a actividades en segundo plano como la purga de datos con código de borrado (EC) y la reparación de EC. Al aumentar la prioridad de la purga de datos con código de borrado (EC) y las actividades de reparación de EC, estas tareas pueden completarse más rápido. La eficacia de los cambios en la priorización de E/S se ve afectada por la tasa de solicitudes de los clientes, las fluctuaciones del tráfico de red y otras tareas de red en curso.

Antes de empezar

- Consulta la página sobre la priorización de E/S para determinar qué opciones podrían afectar a tu grid.
- Evalúa si el tráfico actual de clientes puede manejar de forma segura tiempos de espera más largos o timeouts de los clientes.
- Prepárate para supervisar el efecto del cambio en las prioridades y realizar los ajustes necesarios. Estos cambios se aplican rápidamente, pero es posible que su efecto tarde unas horas en hacerse visible.

Pasos

1. Selecciona **Support > Priorización de E/S**.
2. (Opcional) Cambia la prioridad de purga y reparación de EC, para las operaciones en segundo plano que purgan datos de EC, desde sus valores predeterminados.



Utiliza la prioridad predeterminada de purga y reparación de EC baja para grids que tienen nodos basados en RAID.

3. Selecciona **Guardar**.
4. Supervisa el **"métricas"** para evaluar el efecto de los cambios en la priorización.

Ejecuta diagnósticos en StorageGRID

Al solucionar un problema, puedes trabajar con el soporte técnico para ejecutar diagnósticos en tu sistema StorageGRID y revisar los resultados.

- ["Revisar las métricas de soporte"](#)
- ["Métricas de Prometheus más utilizadas"](#)

Antes de empezar

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

Acerca de esta tarea

La página «Diagnósticos» realiza una serie de comprobaciones de diagnóstico sobre el estado actual de la grid. Cada comprobación de diagnóstico puede tener uno de tres estados:

- **Normal:** Todos los valores están dentro del rango normal.
- **Atención:** uno o varios de los valores se encuentran fuera del rango normal.
- **Precaución:** Uno o varios de los valores están significativamente fuera del rango normal.

Los estados de diagnóstico son independientes de las alertas actuales y pueden no indicar problemas operativos con el grid. Por ejemplo, una comprobación de diagnóstico puede mostrar el estado Precaución

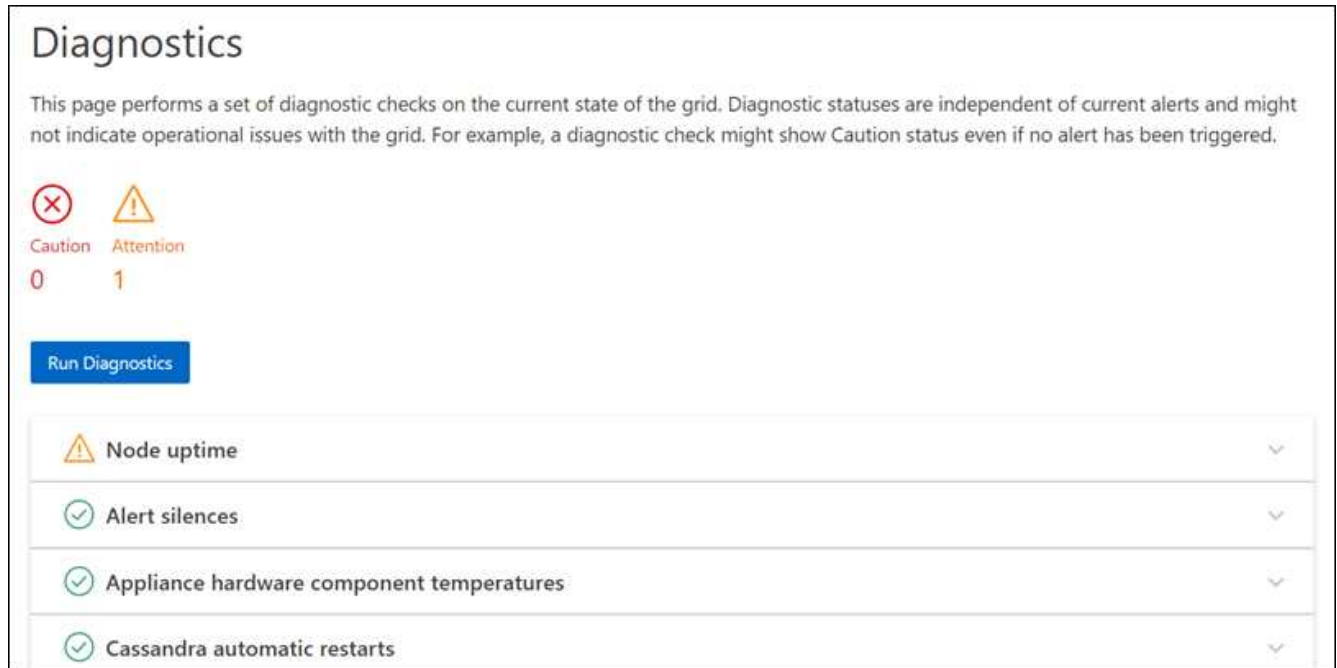
aunque no se haya activado ninguna alerta.

Pasos

1. Selecciona **Soporte > Herramientas > Diagnóstico**.

Aparece la página de Diagnósticos y se muestran los resultados de cada comprobación de diagnóstico. Los resultados se ordenan por gravedad (Precaución, Atención y luego Normal). Dentro de cada gravedad, los resultados se ordenan alfabéticamente.

En este ejemplo, un diagnóstico tiene el estado Atención y tres diagnósticos tienen el estado Normal.



2. Para obtener más información sobre un diagnóstico concreto, haz clic en cualquier parte de la fila.

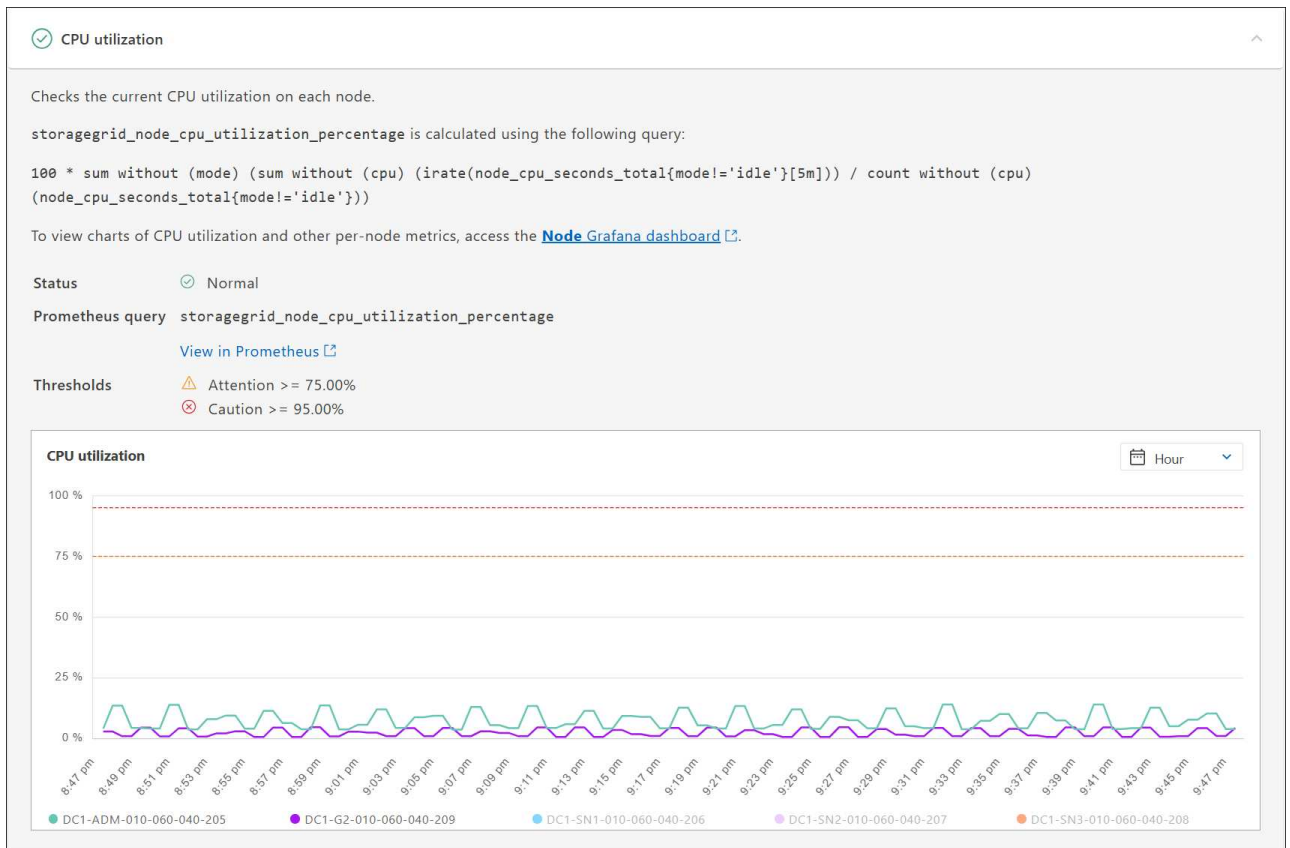
Aparecen los detalles sobre el diagnóstico y sus resultados actuales. Se muestran los siguientes detalles:

- **Estado:** El estado actual de este diagnóstico: Normal, Atención o Precaución.
- **Consulta de Prometheus:** si se ha utilizado para el diagnóstico, la expresión de Prometheus que se empleó para generar los valores de estado. (No se utiliza una expresión de Prometheus en todos los diagnósticos.)
- **Umbrales:** si están disponibles para el diagnóstico, los umbrales definidos por el sistema para cada estado de diagnóstico anómalo. (Los valores de umbral no se utilizan en todos los diagnósticos.)



No puedes cambiar estos umbrales.

- **Valores de estado:** Un gráfico y una tabla (la tabla no aparece en la captura de pantalla) que muestran el estado y el valor del diagnóstico en todo el sistema StorageGRID. En este ejemplo, la utilización de CPU actual para cada nodo de un sistema StorageGRID se muestra. Todos los valores de los nodos están por debajo de los umbrales de Atención y Precaución, así que el estado general del diagnóstico es Normal.



3. **Opcional:** Para ver los gráficos de Grafana relacionados con este diagnóstico, selecciona **Grafana dashboard**.

Este enlace no aparece en todos los diagnósticos.

Aparece el panel de Grafana correspondiente. En este ejemplo, aparece el panel del nodo mostrando la utilización de CPU a lo largo del tiempo para este nodo, así como otros gráficos de Grafana para el nodo.



También puedes acceder a los paneles de Grafana ya creados 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, haz clic en **Ver en Prometheus**.

Aparece un gráfico de Prometheus con 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))
```

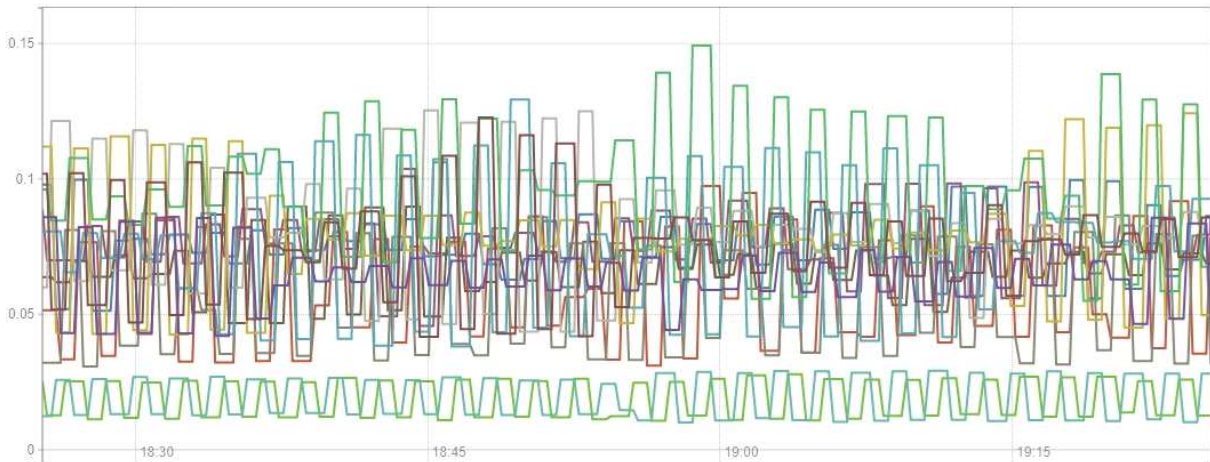
Load time: 547ms
Resolution: 14s
Total time series: 13

Execute

- insert metric at cursor - ▾

Graph Console

1h ⏪ Until ⏩ Res. (s) ☐ stacked



Remove Graph

Add Graph

Crea aplicaciones de supervisión personalizadas para StorageGRID

Puedes crear aplicaciones de supervisión y paneles personalizados utilizando las métricas de StorageGRID disponibles desde la API de gestión de la red.

Si deseas supervisar métricas que no aparecen en ninguna de las páginas existentes de Grid Manager, o si quieres crear paneles personalizados para StorageGRID, puedes utilizar la Grid Management API para consultar las métricas de StorageGRID.

También puedes acceder directamente a las métricas de Prometheus mediante una herramienta de monitorización externa, como Grafana. El uso de una herramienta externa requiere que subas o generes un certificado de cliente administrativo para que StorageGRID pueda autenticar la herramienta por motivos de seguridad. Consulta la ["Instrucciones para la administración de StorageGRID"](#).

Para consultar las operaciones de la API de métricas, incluida la lista completa de las métricas disponibles, accede al Grid Manager. En la parte superior de la página, selecciona el icono de ayuda y selecciona **API documentation > metrics**.

GET

`/grid/metric-labels/{label}/values` Lists the values for a metric label

GET

`/grid/metric-names` Lists all available metric names

GET

`/grid/metric-query` Performs an instant metric query at a single point in time

GET

`/grid/metric-query-range` Performs a metric query over a range of time

Los detalles sobre cómo implementar una aplicación de supervisión personalizada quedan fuera del alcance de esta documentación.

Soluciona problemas del sistema StorageGRID

Soluciona problemas en un sistema StorageGRID

Si tienes algún problema al utilizar un sistema StorageGRID, consulta los consejos y las directrices de esta sección para obtener ayuda a la hora de identificar y resolver el problema.

A menudo, puedes resolver problemas por tu cuenta; sin embargo, es posible que tengas que escalar algunas incidencias al soporte técnico.

Definir el problema

El primer paso para resolver un problema es definirlo con claridad.

En esta tabla se ofrecen ejemplos de los tipos de información que podrías recopilar para definir un problema:

Pregunta	Ejemplo de respuesta
¿Qué está haciendo o dejando de hacer el sistema StorageGRID? ¿Cuáles son sus síntomas?	Las aplicaciones de los clientes indican que no es posible incorporar objetos a StorageGRID.
¿Cuándo empezó el problema?	La incorporación del objeto fue rechazada por primera vez alrededor de las 14:50 del 8 de enero de 2020.
¿Cómo notaste el problema por primera vez?	Notificado por la aplicación cliente. También recibiste notificaciones de alerta por correo electrónico.
¿El problema se produce siempre o solo de vez en cuando?	El problema sigue.

Pregunta	Ejemplo de respuesta
Si el problema ocurre regularmente, ¿qué pasos lo causan?	El problema ocurre cada vez que un cliente intenta ingerir un objeto.
Si el problema se produce de forma intermitente, ¿cuándo ocurre? Anota las horas de cada incidente del que tengas constancia.	El problema no es intermitente.
¿Has visto este problema antes? ¿Con qué frecuencia has tenido este problema en el pasado?	Es la primera vez que me encuentro con este problema.

Evalúa el riesgo y el impacto en el sistema

Una vez que hayas definido el problema, evalúa su riesgo e impacto en el sistema StorageGRID. Por ejemplo, la presencia de alertas críticas no significa necesariamente que el sistema no esté ofreciendo servicios principales.

Esta tabla resume el impacto que el problema de ejemplo está teniendo en el funcionamiento del sistema:

Pregunta	Ejemplo de respuesta
¿Puede el sistema StorageGRID incorporar contenido?	No.
¿Pueden las aplicaciones cliente recuperar contenido?	Algunos objetos se pueden recuperar y otros no.
¿Están los datos en peligro?	No.
¿La capacidad para desarrollar la actividad empresarial está gravemente afectada?	Sí, porque las aplicaciones cliente no pueden almacenar objetos en el sistema StorageGRID y los datos no se pueden recuperar de forma coherente.

Recopilar datos

Una vez que hayas definido el problema y evaluado su riesgo e impacto, recopila datos para su análisis. El tipo de datos que resulta más útil recopilar depende de la naturaleza del problema.

Tipo de datos que se van a recopilar	Por qué recopilamos estos datos	Instrucciones
Crear una cronología de los cambios recientes	Los cambios en tu sistema StorageGRID, en su configuración o en su entorno pueden provocar un comportamiento nuevo.	• Crea una cronología de los cambios recientes

Tipo de datos que se van a recopilar	Por qué recopilamos estos datos	Instrucciones
Revisar alertas	Las alertas pueden ayudarte a determinar rápidamente la causa raíz de un problema al proporcionarte pistas importantes sobre los problemas subyacentes que podrían estar causándolo. Consulta la lista de alertas actuales para ver si StorageGRID ha identificado la causa raíz de un problema por ti. Revisa las alertas que se activaron en el pasado para obtener información adicional.	• "Ver alertas actuales y resueltas"
Establece puntos de referencia	Recopila información sobre los niveles normales de diversos valores operativos. Estos valores de referencia, y las desviaciones de estas líneas base, pueden proporcionar pistas valiosas.	• Establece puntos de referencia
Realiza pruebas de importación y recuperación	Para solucionar problemas de rendimiento relacionados con la importación y la recuperación, utiliza una estación de trabajo para almacenar y recuperar objetos. Compara los resultados con los obtenidos al utilizar la aplicación cliente.	• "Supervisa el rendimiento de las operaciones PUT y GET"
Revisar los mensajes de auditoría	Revisa los mensajes de auditoría para realizar un seguimiento detallado de las operaciones de StorageGRID. La información detallada de los mensajes de auditoría puede ser útil para solucionar muchos tipos de problemas, incluidos los problemas de rendimiento.	• "Revisar los mensajes de auditoría"
Comprobar la ubicación de los objetos y la integridad del almacenamiento	Si tienes problemas de almacenamiento, verifica que los objetos se estén colocando donde esperas. Verifica la integridad de los datos de los objetos en un Storage Node.	• "Supervisar las operaciones de verificación de objetos" • "Confirma las ubicaciones de los datos de los objetos" • "Verifica la integridad del objeto"

Tipo de datos que se van a recopilar	Por qué recopilamos estos datos	Instrucciones
Recopilar datos para el soporte técnico	Es posible que el soporte técnico te pida que recopiles datos o revises información concreta para ayudar a resolver problemas.	• "Recopilar archivos de registro y datos del sistema" • "Activar manualmente un paquete de AutoSupport" • "Revisar las métricas de soporte"

Crear una cronología de los cambios recientes

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

- Los cambios en tu sistema StorageGRID, en su configuración o en su entorno pueden provocar un comportamiento nuevo.
- Una cronología de los cambios puede ayudarte a identificar qué cambios podrían ser los responsables de un problema y cómo cada cambio podría haber influido en su desarrollo.

Elabora una tabla con los cambios recientes realizados en tu sistema que incluya información sobre cuándo se produjo cada cambio y cualquier detalle relevante al respecto, como por ejemplo qué más estaba ocurriendo mientras se llevaba a cabo el cambio:

Tiempo de cambio	Tipo de cambio	Detalles
Por ejemplo: • ¿Cuándo iniciaste la recuperación del nodo? • ¿Cuándo se completó la actualización del software? • ¿Interrumpiste el proceso?	¿Qué ha pasado? ¿Qué has hecho?	Documenta cualquier detalle relevante sobre el cambio. Por ejemplo: • Detalles de los cambios en la red. • Qué corrección urgente se instaló. • Cómo han cambiado las cargas de trabajo de los clientes. Asegúrate de anotar si se estaba realizando más de un cambio al mismo tiempo. Por ejemplo, ¿se hizo este cambio mientras había una actualización en curso?

Ejemplos de cambios recientes significativos

Aquí tienes algunos ejemplos de cambios que podrían ser significativos:

- ¿Se ha instalado, ampliado o recuperado recientemente el sistema StorageGRID?
- ¿Se ha actualizado el sistema recientemente? ¿Se aplicó una corrección urgente?
- ¿Has reparado o cambiado algún componente de 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?
- ¿Has cambiado los equilibradores de carga o has añadido o eliminado un grupo de alta disponibilidad de Admin Nodes o Gateway Nodes?
- ¿Has iniciado alguna tarea que pueda tardar mucho en completarse? Por ejemplo:
 - Recuperación de un nodo de almacenamiento que ha fallado
 - Decomisionamiento de Storage Node
- ¿Has hecho algún cambio en la autenticación de usuarios, como añadir un tenant o modificar la configuración de LDAP?
- ¿Se está llevando a cabo la migración de datos?
- ¿Se habilitaron o cambiaron recientemente los servicios de plataforma?
- ¿Activaste recientemente la función de cumplimiento normativo?
- ¿Se han añadido o eliminado Cloud Storage Pools?
- ¿Se han hecho cambios en la compresión o el cifrado del almacenamiento?
- ¿Se ha producido algún cambio en la infraestructura de red? Por ejemplo, VLANs, routers o DNS.
- ¿Has hecho algún cambio en las fuentes NTP?
- ¿Has hecho algún cambio en las interfaces de red Grid, Admin o Client Network?
- ¿Has hecho algún otro cambio en el sistema StorageGRID o en su entorno?

Establece puntos de referencia

Puedes establecer valores de referencia para tu sistema registrando los niveles normales de varios valores operativos. En el futuro, puedes comparar los valores actuales con estos valores de referencia para ayudar a detectar y resolver valores anómalos.

Propiedad	Valor	Cómo obtenerlo
Consumo medio de almacenamiento	GB consumidos al día Porcentaje consumido al día	Accede al Grid Manager. En la página «Nodes», selecciona toda la grid o un sitio y ve a la pestaña «Storage». En el gráfico Storage Used - Object Data, busca un periodo en el que la línea sea bastante estable. Coloca el cursor sobre el gráfico para estimar cuánto almacenamiento se consume cada día Puedes recopilar esta información para todo el sistema o para un centro de datos específico.

Propiedad	Valor	Cómo obtenerlo
Consumo medio de metadatos	GB consumidos al día Porcentaje consumido al día	Accede al Grid Manager. En la página «Nodes», selecciona toda la grid o un sitio y ve a la pestaña «Storage». En el gráfico «Almacenamiento utilizado: metadatos de objetos», busca un periodo en el que la línea se mantenga bastante estable. Coloca el cursor sobre el gráfico para calcular cuánto almacenamiento de metadatos se consume cada día. Puedes recopilar esta información para todo el sistema o para un centro de datos específico.
Índice de operaciones de S3	Operaciones por segundo	En el panel de control de Grid Manager, selecciona Rendimiento > Operaciones S3 para Storage Nodes. Para ver las tasas y los recuentos de ingesta y recuperación de un sitio o nodo específico, selecciona Nodos > sitio o nodo de almacenamiento > Objetos. Coloca el cursor sobre el gráfico de ingesta y recuperación de S3.
Tasa de evaluación del ILM	Objetos por segundo	En la página «Nodos», selecciona grid > ILM. En el gráfico de la cola de ILM, busca un periodo en el que la línea sea bastante estable. Coloca el cursor sobre el gráfico para estimar un valor de referencia para la tasa de evaluación de tu sistema.
Velocidad de exploración del ILM	Objetos por segundo	Selecciona Nodos > grid > ILM. En el gráfico ILM Queue, busca un periodo en el que la línea sea bastante estable. Coloca el cursor sobre el gráfico para estimar un valor de referencia para Scan rate en tu sistema.
Objetos en cola procedentes de operaciones del cliente	Objetos por segundo	Selecciona Nodos > grid > ILM. En el gráfico «ILM Queue», busca un periodo en el que la línea se mantenga bastante estable. Coloca el cursor sobre el gráfico para calcular un valor de referencia para Objetos en cola (from client operations) en tu sistema.
Latencia media de las consultas	Milisegundos	Selecciona Nodos > Storage Node > Objects . En la tabla de consultas, consulta el valor de latencia media.

Analizar datos

Utiliza la información que recopiles para determinar la causa del problema y las posibles soluciones.

El análisis depende del problema, pero en general:

- Localiza los puntos de fallo y los cuellos de botella usando las alertas.
- Reconstruye el historial del problema utilizando el historial de alertas y los gráficos.
- Utiliza los gráficos para detectar anomalías y comparar la situación problemática con el funcionamiento normal.

Lista de comprobación de la información de escalación

Si no puedes resolver el problema por tu cuenta, ponte en contacto con soporte técnico. Antes de ponerte en contacto con soporte técnico, recopila la información que se indica en la siguiente tabla para facilitar la resolución del problema.

	Artículo	Notas
	Planteamiento del problema	¿Cuáles son los síntomas del problema? ¿Cuándo empezó el problema? ¿Ocurre de forma constante o intermitente? Si es intermitente, ¿en qué momentos ha ocurrido? Define el problema
	Evaluación de impacto	¿Cuál es la gravedad del problema? ¿Cuál es el impacto en la aplicación cliente? • ¿El cliente se ha conectado correctamente antes? • ¿Puede el cliente ingerir, recuperar y eliminar datos?
	ID del sistema StorageGRID	Selecciona Mantenimiento > Sistema > Licencia . El ID del sistema de StorageGRID se muestra como parte de la licencia actual.
	Versión del software	En la parte superior del Grid Manager, selecciona el icono de ayuda y selecciona Acerca de para ver la versión de StorageGRID.
	Personalización	Resume cómo está configurado tu sistema StorageGRID. Por ejemplo, indica lo siguiente: • ¿La grid utiliza compresión de almacenamiento, cifrado de almacenamiento o cumplimiento? • ¿Crea ILM objetos replicados o con código de borrado? ¿Garantiza ILM la redundancia entre sitios? ¿Utilizan las reglas de ILM los comportamientos de ingesta «Equilibrado», «Estricto» o «Compromiso dual»?

	Artículo	Notas
	Archivos de registro y datos del sistema	Recopila los archivos de registro y los datos del sistema para tu sistema. Selecciona Soporte > Herramientas > Recopilación de registros. Puedes recopilar registros de toda la grid o de los nodos seleccionados. Si solo vas a recopilar registros de determinados nodos, asegúrate de incluir al menos un nodo de almacenamiento que cuente con el servicio ADC. Los tres primeros nodos de almacenamiento instalados en una sede incluyen el servicio ADC.
	Información inicial	Recopila información de referencia sobre las operaciones de ingesta, las operaciones de recuperación y el consumo de almacenamiento. Establece puntos de referencia
	Cronología de los cambios recientes	Elabora una cronología que resuma los cambios recientes en el sistema o en su entorno. Crea una cronología de los cambios recientes
	Historial de las medidas adoptadas para diagnosticar el problema	Si has tomado medidas para diagnosticar o solucionar el problema por tu cuenta, asegúrate de anotar los pasos que has seguido y el resultado.

Soluciona problemas de objetos y almacenamiento

Confirma las ubicaciones de los datos de objetos en StorageGRID

Según el problema, es posible que quieras "[confirma dónde se almacenan los datos del objeto](#)". Por ejemplo, es posible que quieras verificar que la política de ILM funciona como se espera y que los datos de objetos se están almacenando donde corresponde.

Antes de empezar

- Debes disponer de un identificador de objeto, que puede ser uno de los siguientes:
 - **UUID**: el identificador único universal del objeto. Introduce el UUID completamente en mayúsculas.
 - **CBID**: el identificador único del objeto dentro de StorageGRID. Puedes obtener el CBID de un objeto a partir del registro de auditoría. Introduce el CBID todo en mayúsculas.
 - **Depósito S3 y clave de objeto**: Cuando se importa un objeto a través de "[Interfaz S3](#)", la aplicación cliente utiliza una combinación de depósito y clave de objeto para almacenar e identificar el objeto.

Pasos

1. Selecciona **ILM > Búsqueda de metadatos de objetos**.

2. Escribe el identificador del objeto en el campo **Identificador**.

Puedes introducir un UUID, un CBID o un bucket/clave de objeto de S3.

3. Si quieres buscar una versión concreta del objeto, introduce el identificador de la versión (opcional).



4. Selecciona **Buscar**.

Los "[resultados de la búsqueda de metadatos del objeto](#)" aparecen. Esta página muestra los siguientes tipos de información:

- Metadatos del sistema, incluyendo el identificador del objeto (UUID), el identificador de la versión (opcional), el nombre del objeto, el nombre del contenedor, el nombre o el identificador 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 por última vez.
- Cualquier par clave-valor de metadatos de usuario personalizados asociados al objeto.
- Para los objetos de S3, cualquier par clave-valor de etiquetas asociado con el objeto.
- En el caso de las copias replicadas de objetos, la ubicación de almacenamiento actual de cada copia.
- En el caso de las copias de objetos con código de borrado, la ubicación actual de almacenamiento de cada fragmento.
- Para las copias de objetos en un Cloud Storage Pool, la ubicación del objeto, incluyendo el nombre del bucket externo y el identificador único del objeto.
- En el caso de los objetos segmentados y los objetos compuestos, una lista de los segmentos del objeto que incluye los identificadores de los segmentos y los tamaños de los datos. Para los objetos con más de 100 segmentos, solo se muestran los primeros 100 segmentos.
- Todos los metadatos de los objetos en el formato de almacenamiento interno sin procesar. Estos metadatos sin procesar incluyen metadatos internos del sistema cuya persistencia no está garantizada de una versión a otra.

El siguiente ejemplo muestra los resultados de la consulta de metadatos de un objeto de prueba de S3 almacenado en 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",

```

Conoce los fallos del almacén de objetos para volúmenes de almacenamiento en StorageGRID

El almacenamiento subyacente de un nodo de almacenamiento se divide en almacenes de objetos. Los almacenes de objetos también se conocen como volúmenes de almacenamiento.

Puedes ver la información del almacén de objetos de cada nodo de almacenamiento. Selecciona **Nodos** > **Nodo de almacenamiento** > **Almacenamiento**.

Disk devices

Name ? ⇅	World Wide Name ? ⇅	I/O load ? ⇅	Read rate ? ⇅	Write rate ? ⇅
sd(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB 	Enabled

Object stores

ID ? ⇅	Size ? ⇅	Available ? ⇅	Replicated data ? ⇅	EC data ? ⇅	Object data (%) ? ⇅	Health ? ⇅
0000	107.32 GB	96.44 GB 	1.55 MB 	0 bytes 	0.00%	No Errors
0001	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0002	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0003	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0004	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors

Dependiendo de la naturaleza del fallo, los fallos en un volumen de almacenamiento podrían reflejarse en "[alertas de volumen de almacenamiento](#)". Si un volumen de almacenamiento falla, debes reparar el volumen de almacenamiento fallido para restaurar el Storage Node a su funcionalidad completa lo antes posible. Si es necesario, puedes ir a la pestaña **Configuration** y "[Coloca el nodo de almacenamiento en estado de solo lectura](#)" para que el sistema StorageGRID pueda usarlo para la recuperación de datos mientras te preparas para una recuperación completa del servidor.

Verifica la integridad de los datos de objetos en StorageGRID

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

Hay dos procesos de verificación: la verificación en segundo plano y la comprobación de existencia de objetos (anteriormente llamada verificación en primer plano). Trabajan juntos para garantizar la integridad de los datos. La verificación en segundo plano se ejecuta automáticamente y comprueba de forma continua la corrección de los datos de los objetos. Puedes activar la comprobación de existencia de objetos para verificar más rápidamente la existencia (aunque no la corrección) de los objetos.

¿Qué es la verificación de antecedentes?

El proceso de verificación de fondo comprueba de forma automática y continua los nodos de almacenamiento en busca de copias dañadas de los datos de los objetos e intenta reparar automáticamente cualquier problema que detecte.

La verificación de antecedentes comprueba la integridad de los objetos replicados y de los objetos con código de borrado, como sigue:

- **Objetos replicados:** Si el proceso de verificación en segundo plano detecta un objeto replicado que está dañado, la copia dañada se elimina de su ubicación y se pone en cuarentena en otra parte del Storage Node. Luego, se genera una nueva copia sin daños y se coloca para cumplir con las políticas de ILM activas. Es posible que la nueva copia no se coloque en el Storage Node que se usó para la copia original.



Los datos de objetos dañados se ponen en cuarentena en lugar de eliminarse del sistema, para que aún puedas acceder a ellos. Para obtener más información sobre cómo acceder a los datos de objetos en cuarentena, ponte en contacto 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 que falta in situ en el mismo nodo de almacenamiento, utilizando los datos restantes y los fragmentos de paridad. Si no es posible reconstruir el fragmento dañado, se intenta recuperar otra copia del objeto. Si la recuperación se realiza con éxito, se lleva a cabo una evaluación de ILM para crear una copia de sustitución del objeto con código de borrado.

El proceso de verificación en segundo plano solo comprueba los objetos en los nodos de almacenamiento. No comprueba los objetos en un Cloud Storage Pool. Los objetos deben tener más de cuatro días de antigüedad para ser aptos para la verificación en segundo plano.

La verificación en segundo plano se ejecuta a un ritmo continuo diseñado para no interferir con las actividades habituales del sistema. La verificación en segundo plano no se puede detener. Sin embargo, puedes aumentar la velocidad de verificación en segundo plano para verificar más rápidamente el contenido de un nodo de almacenamiento si sospechas que hay algún problema.

Alertas relacionadas con la verificación en segundo plano

Si el sistema detecta un objeto dañado que no puede corregir automáticamente (porque el daño impide identificar el objeto), se activa la alerta **Unidentified corrupt object detected**.

Si la verificación en segundo plano no puede sustituir un objeto dañado porque no encuentra otra copia, se activa la alerta **Objetos potencialmente perdidos**.

¿Qué es la comprobación de existencia de un objeto?

La comprobación de existencia de objetos verifica si todas las copias replicadas esperadas de los objetos y los fragmentos con codificación de borrado existen en un nodo de almacenamiento. La comprobación de existencia de objetos no verifica los datos del objeto en sí (de eso se encarga la verificación en segundo plano); en su lugar, proporciona una forma de verificar la integridad de los dispositivos de almacenamiento, especialmente si un problema de hardware reciente pudiera haber afectado a la integridad de los datos.

A diferencia de la verificación en segundo plano, que ocurre automáticamente, debes iniciar manualmente una tarea de comprobación de la existencia de un objeto.

La comprobación de la existencia de objetos lee los metadatos de cada objeto almacenado en StorageGRID y verifica la existencia tanto de las copias replicadas de los objetos como de los fragmentos de objetos con código de borrado. Los datos que falten se gestionan de la siguiente manera:

- **Copias replicadas:** Si falta una copia de los datos de un objeto replicado, StorageGRID intenta automáticamente sustituirla por una copia almacenada en otra ubicación del sistema. El nodo de almacenamiento somete la copia existente a una evaluación de ILM, que determinará que ya no se cumple la política de ILM actual para este objeto porque falta otra copia. Se genera una nueva copia y se coloca para cumplir con las políticas de ILM activas del sistema. Es posible que esta nueva copia no se coloque en la misma ubicación en la que estaba almacenada la copia que falta.
- **Fragmentos con código de borrado:** Si falta un fragmento de un objeto con código de borrado, StorageGRID intenta automáticamente reconstruir el fragmento que falta in situ en el mismo nodo de almacenamiento utilizando los fragmentos restantes. Si no es posible reconstruir el fragmento que falta (porque se han perdido demasiados fragmentos), ILM intenta encontrar otra copia del objeto, que pueda utilizar para generar un nuevo fragmento con código de borrado.

Ejecuta la comprobación de existencia del objeto

Creas y ejecutas un solo trabajo de comprobación de existencia de objetos a la vez. Cuando creas un trabajo, seleccionas los nodos de almacenamiento y los volúmenes que quieres verificar. También seleccionas la consistencia para el trabajo.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- Te has asegurado de que los Storage Nodes que quieres comprobar estén en línea. Selecciona **Nodes** para ver la tabla de nodos. Asegúrate de que no aparezca ningún icono de alerta junto al nombre de nodo de los nodos que quieres comprobar.
- Te has asegurado de que los siguientes procedimientos **no** se estén ejecutando en los nodos que deseas comprobar:
 - Ampliación de la red para añadir un nodo de almacenamiento
 - Decomisionar Storage Node
 - Recuperación de un volumen de almacenamiento con error

- Recuperación de un nodo de almacenamiento con una unidad del sistema con error
- Reequilibrio de EC
- Clon de nodo de appliance

La comprobación de la existencia de un objeto no proporciona información útil mientras estos procedimientos están en curso.

Acerca de esta tarea

Un trabajo de comprobación de existencia de objetos puede tardar días o semanas en completarse, según el número de objetos del grid, los nodos de almacenamiento y volúmenes seleccionados, y la consistencia seleccionada. Solo puedes ejecutar un trabajo a la vez, pero puedes seleccionar varios nodos de almacenamiento y volúmenes al mismo tiempo.

Pasos

1. Selecciona **Mantenimiento > Tareas > Comprobación de existencia de objetos**.
2. Selecciona **Crear trabajo**. Aparece el asistente Crear un trabajo de comprobación de existencia de objeto.
3. Selecciona los nodos que contienen los volúmenes que quieres verificar. Para seleccionar todos los nodos en línea, selecciona la casilla de verificación **Nombre de nodo** en el encabezado de la columna.

Puedes buscar por nombre de nodo o sitio.

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

4. Selecciona **Continuar**.
5. Selecciona uno o más volúmenes para cada nodo de la lista. Puedes buscar volúmenes usando el número de volumen de almacenamiento o el nombre de nodo.

Para seleccionar todos los volúmenes de cada nodo que seleccionaste, marca la casilla **Storage volume** en el encabezado de la columna.

6. Selecciona **Continuar**.
7. Selecciona la consistencia para el trabajo.

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

- **Sitio principal**: Dos copias de metadatos en un único sitio.
- **Strong-global**: Dos copias de metadatos en cada sitio.
- **Todas** (por defecto): las tres copias de los metadatos en cada sitio.

Para obtener más información sobre la coherencia, consulta las descripciones que aparecen en el asistente.

8. Selecciona **Continuar**.
9. Revisa y verifica tus selecciones. Puedes seleccionar **Anterior** para volver a un paso anterior del asistente y actualizar tus selecciones.

Se genera una tarea de comprobación de la existencia de un objeto y se ejecuta hasta que ocurra una de las siguientes situaciones:

- La tarea se completa.
- Puedes pausar o cancelar el trabajo. Puedes reanudar un trabajo que hayas pausado, pero no puedes reanudar un trabajo que hayas cancelado.
- El trabajo se ha bloqueado. Se activa la alerta **Comprobación de existencia del objeto bloqueada**. Sigue las medidas correctivas especificadas para la alerta.
- La tarea falla. Se activa la alerta **Fallo en la comprobación de existencia del objeto**. Sigue las acciones correctivas especificadas para la alerta.
- Aparece el mensaje «Servicio no disponible» o «Error interno del servidor». Después de un minuto, actualiza la página para seguir supervisando el trabajo.



Si lo necesitas, puedes salir de la página de comprobación de la existencia del objeto y volver para seguir supervisando el trabajo.

10. Mientras se ejecuta el trabajo, consulta la pestaña **Trabajo activo** y toma nota del valor de Copias de objetos que faltan detectadas.

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

Si el número de copias de objetos perdidos detectadas es superior a 100, es posible que haya un problema con el almacenamiento del Storage Node.

11. Una vez finalizado el trabajo, realiza cualquier acción adicional que sea necesaria:

- Si el valor de Missing object copies detected es cero, entonces no se encontraron problemas. No es necesario realizar ninguna acción.
- Si el valor de «Copias de objetos perdidos detectadas» es mayor que cero y no se ha activado la alerta **Objetos potencialmente perdidos**, entonces el sistema reparó todas las copias perdidas. Verifica que cualquier problema de hardware se haya corregido para evitar daños futuros en las copias de los objetos.
- Si el valor de «Copias de objetos perdidos detectadas» es superior a cero y se ha activado la alerta **Objetos potencialmente perdidos**, la integridad de los datos podría verse afectada. Ponte en contacto con el soporte técnico.
- Puedes investigar posibles copias de objetos perdidas utilizando grep para extraer los mensajes de auditoría de LLST: `grep LLST audit_file_name`.

Este procedimiento es similar al de "[investigando objetos que puedan haberse perdido](#)", aunque para las copias de objetos buscas LLST en vez de OLST.

12. Si seleccionaste la consistencia strong-site o strong-global para el trabajo, espera aproximadamente tres semanas para la consistencia de los metadatos y luego vuelve a ejecutar el trabajo en los mismos volúmenes.

Cuando StorageGRID haya tenido tiempo de lograr la coherencia de los metadatos de los nodos y volúmenes incluidos en el trabajo, volver a ejecutar el trabajo podría eliminar las copias de objetos que se habían señalado erróneamente como faltantes o hacer que se comprueben copias adicionales de objetos en caso de que se hubieran pasado por alto.

- a. Selecciona **Mantenimiento > Comprobación de existencia de objetos > Historial de trabajos**.
- b. Determina qué trabajos están listos para volver a ejecutarse:

- i. Fíjate en la columna **Hora de finalización** para determinar qué trabajos se ejecutaron hace más de tres semanas.
- ii. Para esos trabajos, revisa la columna Control de consistencia para ver si aparece strong-site o strong-global.
- c. Marca la casilla de cada trabajo que quieras volver a ejecutar y, a continuación, selecciona **Rerun**.
- d. En el asistente de reejecución de tareas, revisa los nodos y volúmenes seleccionados y la consistencia.
- e. Cuando estés listo para volver a ejecutar los trabajos, selecciona **Rerun**.

Aparece la pestaña «Tareas activas». Todas las tareas que seleccionaste se vuelven a ejecutar como una sola tarea con una consistencia de strong-site. Un campo **Tareas relacionadas** en la sección Detalles muestra los ID de las tareas originales.

Resuelve la alerta S3 PUT object size too large en StorageGRID

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

Antes de empezar

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

Determina qué inquilinos usan objetos que son mayores de 5 GiB, así puedes notificárselos.

Pasos

1. Ve a **Configuración > Supervisión > Servidor de auditoría y syslog**.
2. Si las operaciones de escritura del cliente son normales, accede al registro de auditoría:
 - a. Introduce `ssh admin@primary_Admin_Node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

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

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

Opción	Destino
Nodos locales (predeterminado)	<code>/var/local/log/localaudit.log</code>

Opción	Destino
Nodos de administración/nodos locales	- Nodos de administración (primarios y no primarios): /var/local/audit/export/audit.log - Todos los nodos: El archivo /var/local/log/localaudit.log suele estar vacío o faltar en este modo.
Servidor syslog externo	/var/local/log/localaudit.log

Según tu configuración de destino de auditoría, introduce: `cd /var/local/log o /var/local/audit/export/`

Para saber más, consulta ["Selecciona la ubicación del registro"](#).

f. Identifica qué tenants están utilizando objetos de más de 5 GiB.

- Introduce `zgrep SPUT * | egrep "CSIZ\ (UI64\): ([5-9] | [1-9] [0-9]+) [0-9]{9}"`
- Para cada mensaje de auditoría en los resultados, consulta el campo `S3AI` para determinar el ID de la cuenta del inquilino. Utiliza los demás campos del mensaje para determinar qué dirección IP usó el cliente, el bucket y el objeto:

Código	Descripción
SAIP	IP de origen
S3AI	ID de inquilino
S3BK	Bucket
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 operaciones de escritura del cliente no son normales, utiliza el tenant ID de la alerta para identificar al tenant:

- a. Ve a **Soporte > Herramientas > Recopilación de registros**. Recopila los registros de la aplicación para el Storage Node en la alerta. Especifica 15 minutos antes y después de la alerta. Consulta ["Recopilar archivos de registro y datos del sistema"](#).
- b. Descomprime el archivo y entra en `bycast.log`:

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

- c. Busca en el registro `method=PUT` e identifica al cliente en el campo `clientIP`.

Ejemplo de `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=
```

4. Informa a los inquilinos que el tamaño máximo de `PutObject` es de 5 GiB y que deben usar cargas multiparte para objetos mayores de 5 GiB.
5. Ignora la alerta durante una semana si la aplicación ha sido cambiada.

Soluciona problemas de datos de objetos perdidos o faltantes

Conoce la pérdida y la ausencia de datos de objetos en StorageGRID

Los objetos pueden recuperarse por varios motivos, como las solicitudes de lectura de una aplicación cliente, las verificaciones en segundo plano de los datos de objetos replicados, las reevaluaciones de ILM y la restauración de los datos de objetos durante la recuperación de un Storage Node.

El sistema StorageGRID utiliza la información de ubicación en los metadatos de un objeto para determinar de 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 de otro lugar del sistema, asumiendo que la política de ILM

contiene una regla para realizar dos o más copias del objeto.

Si esta recuperación se realiza con éxito, el sistema StorageGRID sustituye la copia perdida del objeto. De lo contrario, se activa la alerta **Objetos potencialmente perdidos** de la siguiente manera:

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

Debes investigar inmediatamente todas las alertas de **Objetos potencialmente perdidos** para determinar la causa principal de la pérdida y comprobar si el objeto podría seguir existiendo en algún nodo de almacenamiento fuera de línea o que, por cualquier otro motivo, no esté disponible en ese momento. Consulta ["Investiga los objetos que puedan haberse perdido"](#). Las alertas de objetos perdidos pueden activarse por error como medida de precaución.

En caso de que se pierdan datos de objetos sin copias, no hay ninguna solución de recuperación. Sin embargo, debes ["reiniciar el contador de objetos que podrían haberse perdido"](#) para evitar que los objetos perdidos conocidos oculten nuevos objetos perdidos.

Resuelve la alerta de objetos potencialmente perdidos en StorageGRID

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

Antes de empezar

- Debes haber iniciado sesión en Grid Manager usando una ["navegador web compatible"](#).
- Tienes ["permisos de acceso específicos"](#).
- Debes tener el archivo `Passwords.txt`.

Acerca de esta tarea

La alerta **Objetos potencialmente perdidos** indica que, según la información disponible en StorageGRID, no hay copias de un objeto en el grid. Es posible que los datos se hayan perdido de forma permanente.

Investiga de inmediato las alertas de objetos perdidos. Es posible que debas tomar medidas para evitar una mayor pérdida de datos. En algunos casos, es posible que puedas restaurar un objeto perdido si actúas rápidamente.



Si se notifican más de 10 objetos perdidos, ponte en contacto con el soporte técnico. No realices este procedimiento por tu cuenta.

Pasos

1. Selecciona **Nodos**.
2. Selecciona **Storage Node > Objetos**.
3. Revisa el número de objetos perdidos que aparece en la tabla de recuento de objetos.

Este número indica el número total de objetos que este nodo de la grid detecta como perdidos en todo el sistema StorageGRID. El valor es la suma de los contadores de objetos perdidos del componente Data store 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 potencialmente perdidos**:

- a. Inicia sesión en el nodo de la grid:
 - i. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - iii. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - iv. Introduce la contraseña que figura en el archivo `Passwords.txt`. Cuando hayas iniciado sesión como root, el indicador de comandos cambia de `$` a `#`.
- b. Accede al directorio donde se encuentran los registros de auditoría.

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

Opción	Destino
Nodos locales (predeterminado)	<code>/var/local/log/localaudit.log</code>
Nodos de administración/nodos locales	• Nodos de administración (primarios y no primarios): <code>/var/local/audit/export/audit.log</code> • Todos los nodos: El archivo <code>/var/local/log/localaudit.log</code> suele estar vacío o faltar en este modo.
Servidor syslog externo	<code>/var/local/log/localaudit.log</code>

Según tu configuración de destino de auditoría, introduce: `cd /var/local/log o /var/local/audit/export/`

Para saber más, consulta "[Selecciona la ubicación del registro](#)".

- c. Utiliza `grep` para extraer los mensajes de auditoría de Object Lost (OLST). Escribe: `grep OLST audit_file_name`
- d. Toma nota del valor UUID que figura 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] [VOL1(UI64):3222345986]
[RSLT(FC32):NONE] [AVER(UI32):10]
[ATIM(UI64):1581535134780426] [ATYP(FC32):OLST] [ANID(UI32):12448208] [AMID(FC32):ILMX] [ATID(UI64):7729403978647354233]]
```

5. Busca los metadatos del objeto perdido utilizando el UUID:

- a. Selecciona **ILM > Búsqueda de metadatos de objetos**.
- b. Introduce el UUID y selecciona **Buscar**.
- c. Revisa las ubicaciones en los metadatos y toma 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, reiniciar el contador de objetos que podrían haberse perdido para borrar la alerta. La falta de un objeto indica que el objeto se eliminó intencionadamente.
Ubicaciones > 0	Si en el resultado aparecen ubicaciones, es posible que la alerta Objetos que podrían haberse perdido sea un falso positivo. Confirma que los objetos existen. Usa el Node ID y la ruta de archivo que aparecen en la salida para confirmar que el archivo de objeto está en la ubicación indicada. Si los objetos existen, reiniciar el contador de objetos que podrían haberse perdido para eliminar la alerta.
Ubicaciones = 0	Si en el resultado no aparece ninguna ubicación, es posible que falte el objeto. Ponte en contacto con el soporte técnico. El soporte técnico podría pedirte que determines si hay un procedimiento de recuperación de almacenamiento en curso. Consulta la información sobre "restaurar datos de objetos usando Grid Manager" y "restaurar datos de objetos en un volumen de almacenamiento".

6. Después de solucionar los problemas de objetos perdidos, restablece el contador de Objetos potencialmente perdidos para asegurarte de que las alertas no sean falsos positivos:
 - a. Selecciona **Nodos**.
 - b. Selecciona **Nodo de almacenamiento > Tareas**.
 - c. En la sección «Restablecer el contador de objetos potencialmente perdidos», selecciona **Reset**.

Resuelve la alerta de bajo almacenamiento de datos de objetos en StorageGRID

La alerta **Espacio de almacenamiento de datos de objetos insuficiente** supervisa cuánto espacio hay disponible para almacenar datos de objetos en cada Storage Node.

Antes de empezar

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

Acerca de esta tarea

La alerta **Bajo nivel de almacenamiento de datos de objetos** se activa cuando la cantidad total de datos de objetos replicados y con código de borrado en un nodo de almacenamiento cumple una de las condiciones

configuradas en la regla de alerta.

Por defecto, se activa una alerta grave cuando esta condición se cumple:

```
(storagegrid_storage_utilization_data_bytes/  
(storagegrid_storage_utilization_data_bytes +  
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

En esta situación:

- `storagegrid_storage_utilization_data_bytes` es una estimación del tamaño total de los datos de objetos replicados y codificados con código de borrado para un Storage Node.
- `storagegrid_storage_utilization_usable_space_bytes` es la cantidad total de espacio de almacenamiento de objetos que le queda a un nodo de almacenamiento.

Si se activa una alerta grave o leve de **Low object data storage**, debes llevar a cabo un procedimiento de ampliación lo antes posible.

Pasos

1. Selecciona **Alertas > Actuales**.

Aparece la página Alerts.

2. En la tabla de alertas, despliega el grupo de alertas **Low object data storage**, si es necesario, y selecciona la alerta que quieras ver.



Selecciona la alerta, no el encabezado de un grupo de alertas.

3. Revisa los detalles en el cuadro de diálogo y ten en cuenta lo siguiente:

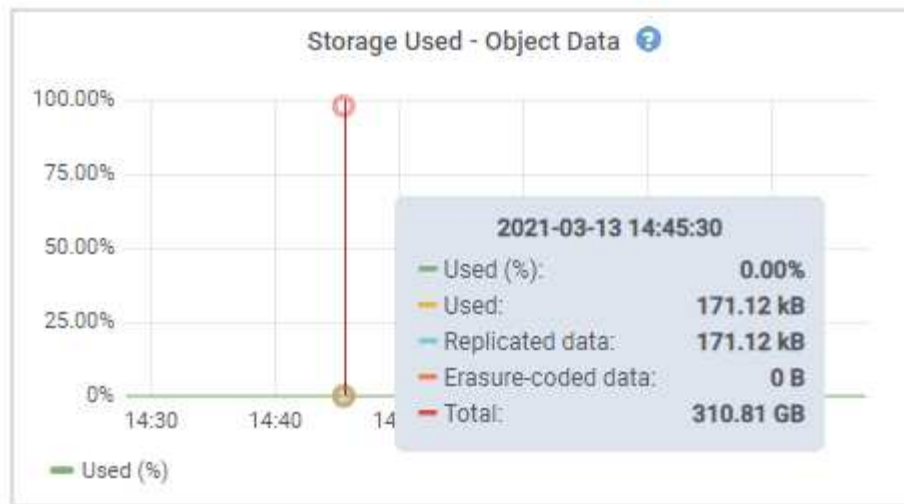
- Activado por tiempo
- El nombre del sitio y del nodo
- Los valores actuales de las métricas para esta alerta

4. Selecciona **Nodos > Storage Node or Site > Almacenamiento**.

5. Coloca el cursor sobre el gráfico Almacenamiento utilizado - datos de objetos.

Se muestran los siguientes valores:

- **Utilizado (%)**: el porcentaje del espacio total utilizable que se ha utilizado para datos de objetos.
- **Utilizado**: La cantidad del espacio total utilizable que se ha usado para los datos de objetos.
- **Datos replicados**: una estimación de la cantidad de datos de objetos replicados en este nodo, sitio o grid.
- **Datos con código de borrado**: Una estimación de la cantidad de datos de objetos con código de borrado en este nodo, sitio o grid.
- **Total**: La cantidad total de espacio utilizable en este nodo, sitio o grid. El valor Used es la métrica `storagegrid_storage_utilization_data_bytes`.



6. Selecciona los controles de tiempo situados encima del gráfico para ver el uso del almacenamiento a lo largo de diferentes periodos de tiempo.

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

7. En cuanto sea posible, ["aumentar la capacidad de almacenamiento"](#) a tu grid.

Puedes añadir volúmenes de almacenamiento (LUN) a los nodos de almacenamiento existentes o puedes añadir nuevos nodos de almacenamiento.



Para más información, consulta ["Gestiona todos los nodos de almacenamiento"](#).

Resuelve la alerta de anulación de marca de agua en StorageGRID

Si utilizas valores personalizados para las marcas de agua del volumen de almacenamiento, es posible que tengas que resolver la alerta **Anulación de marca de agua de solo lectura baja**. Si es posible, deberías actualizar tu sistema para empezar a usar los valores optimizados.

En versiones anteriores, los tres ["marcas de nivel de agua en el volumen de almacenamiento"](#) eran ajustes globales: los mismos valores se aplicaban a todos los volúmenes de almacenamiento en cada Storage Node. A partir de StorageGRID 11.6, el software puede optimizar estos watermarks para cada volumen de almacenamiento, según el tamaño del Storage Node y la capacidad relativa del volumen.

Al actualizar a StorageGRID 11.6 o una versión posterior, se aplican automáticamente marcas de agua optimizadas de solo lectura y de lectura/escritura a todos los volúmenes de almacenamiento, salvo que se dé alguna de las siguientes circunstancias:

- Tu sistema está casi al límite de su capacidad y no podría aceptar nuevos datos si se aplicaran marcas de agua optimizadas. StorageGRID no cambiará la configuración de las marcas de agua en este caso.
- Anteriormente configuraste alguna de las marcas de agua del volumen de almacenamiento con un valor personalizado. StorageGRID no anulará la configuración de las marcas de agua personalizadas con valores optimizados. Sin embargo, StorageGRID podría activar la alerta **Anulación de marca de agua de solo lectura baja** si tu valor personalizado para la marca de agua de solo lectura flexible del volumen de

almacenamiento es demasiado bajo.

Entiende la alerta

Si utilizas valores personalizados para los umbrales de volumen de almacenamiento, es posible que se active la alerta **Low read-only watermark override** en uno o varios Storage Nodes.

Cada aparición de la alerta indica que el valor personalizado del umbral de solo lectura del volumen de almacenamiento es inferior al valor mínimo optimizado para ese Storage Node. Si sigues utilizando la configuración personalizada, el Storage Node podría quedarse críticamente sin espacio antes de poder pasar de forma segura al estado de solo lectura. Es posible que algunos volúmenes de almacenamiento dejen de estar accesibles (se desmonten automáticamente) cuando el nodo alcance su capacidad.

Por ejemplo, supón que anteriormente configuraste el watermark de solo lectura suave del volumen de almacenamiento en 5 GB. Ahora supón que StorageGRID ha calculado los siguientes valores optimizados para los cuatro volúmenes de almacenamiento en Storage Node A:

Volumen 0	12 GB
Volumen 1	12 GB
Volumen 2	11 GB
Volumen 3	15 GB

La alerta **Anulación de marca de agua baja de solo lectura** se activa para el nodo de almacenamiento A porque tu marca de agua personalizada (5 GB) es inferior al valor mínimo optimizado para todos los volúmenes de ese nodo (11 GB). Si sigues utilizando la configuración personalizada, es posible que el nodo se quede con un nivel de espacio críticamente bajo antes de que pueda realizar la transición de forma segura al estado de solo lectura.

Resolver la alerta

Sigue estos pasos si se ha activado una o más alertas de **Anulación de marca de agua de solo lectura baja**. También puedes seguir estas instrucciones si actualmente usas una configuración personalizada de marcas de agua y quieres empezar a usar una configuración optimizada aunque no se haya activado ninguna alerta.

Antes de empezar

- Has completado la actualización a StorageGRID 11.6 o una versión posterior.
- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso raíz"](#).

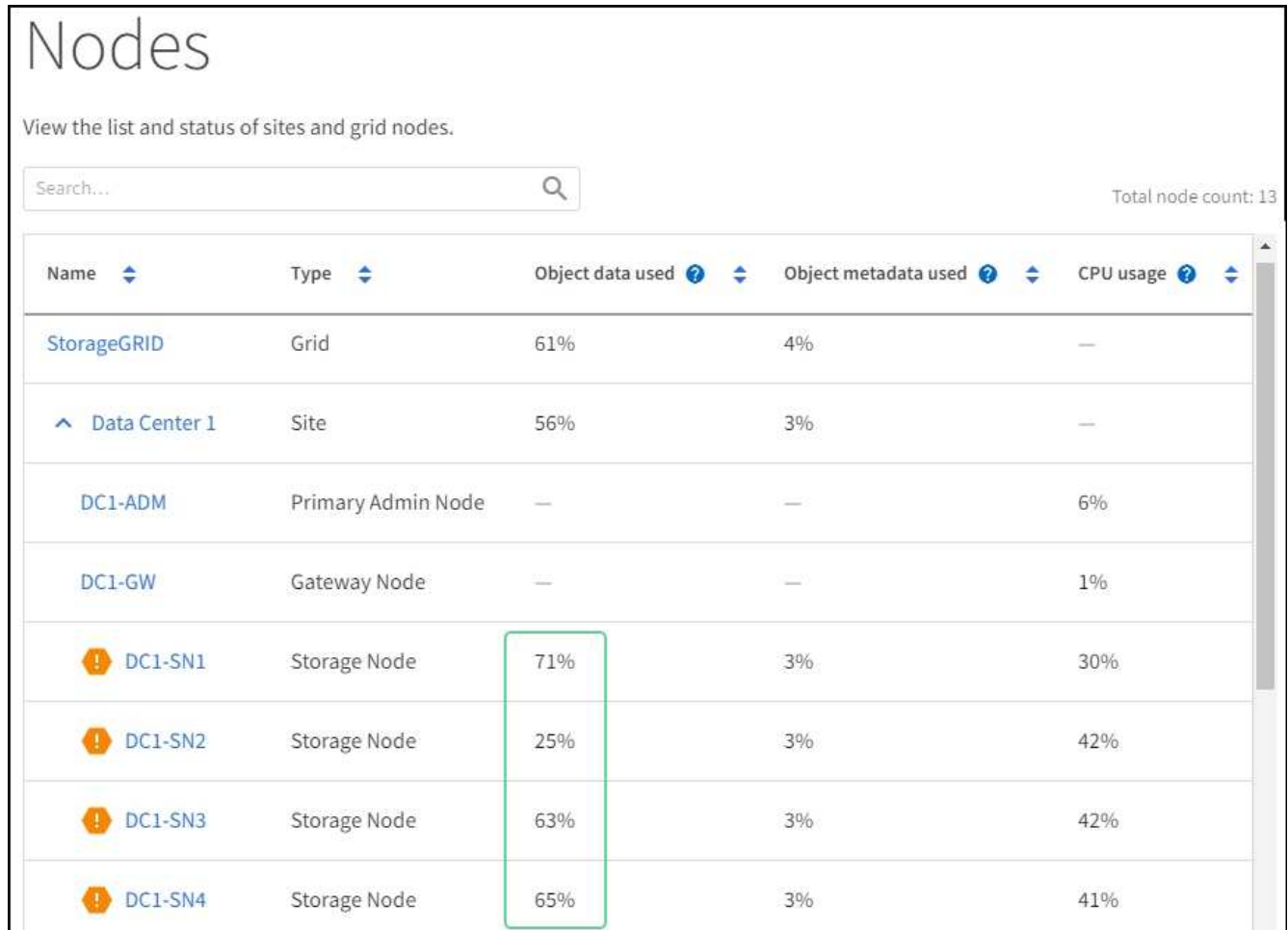
Acerca de esta tarea

Puedes resolver la alerta **Low read-only watermark override** actualizando la configuración de las marcas de agua personalizadas con las nuevas anulaciones de marca de agua. Sin embargo, si uno o varios Storage Nodes están a punto de llenarse o tienes requisitos especiales de ILM, primero debes consultar las marcas de agua de almacenamiento optimizadas y determinar si es seguro utilizarlas.

Evalúa el uso de datos de objetos en toda la grid

Pasos

1. Selecciona **Nodos**.
2. Para cada sitio en la grid, despliega la lista de nodos.
3. Revisa los valores porcentuales que aparecen en la columna **Object data used** para cada Storage Node 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. Sigue el paso correspondiente:
 - a. Si ninguno de los nodos de almacenamiento está a punto de llenarse (por ejemplo, todos los valores de **Datos de objeto utilizados** son inferiores al 80 %), puedes empezar a utilizar la configuración de anulación. Ve a [Utiliza marcas de agua optimizadas](#).
 - b. Si las reglas de ILM utilizan el comportamiento de ingesta estricto o si determinados grupos de almacenamiento están a punto de llenarse, realiza los pasos en [Ver marcas de agua de almacenamiento optimizadas](#) y [Comprueba si puedes utilizar marcas de agua optimizadas](#).

Ver marcas de agua optimizadas para almacenamiento

StorageGRID utiliza dos métricas de Prometheus para mostrar los valores optimizados que ha calculado para el umbral de solo lectura (soft) del volumen de almacenamiento. Puedes consultar los valores optimizados mínimos y máximos para cada Storage Node en tu grid.

Pasos

1. Selecciona **Soporte > Herramientas > Métricas**.
2. En la sección Prometheus, selecciona el enlace para acceder a la interfaz de usuario de Prometheus.
3. Para ver la marca de agua mínima recomendada de solo lectura, introduce la siguiente métrica de Prometheus y selecciona **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 flexible para todos los volúmenes de almacenamiento de cada Storage Node. Si este valor es mayor que el ajuste personalizado de la marca de agua de solo lectura flexible del volumen de almacenamiento, se activa la alerta **Low read-only watermark override** para el Storage Node.

4. Para ver el límite máximo recomendado de marcas de agua soft de solo lectura, introduce la siguiente métrica de Prometheus y selecciona **Execute**:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

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

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

Averigua si puedes utilizar marcas de agua optimizadas

Pasos

1. Selecciona **Nodos**.
2. Repite estos pasos para cada nodo de almacenamiento en línea:
 - a. Selecciona **Nodo de almacenamiento > Almacenamiento**.
 - b. Desplázate hacia abajo hasta la tabla de almacenes de objetos.
 - c. Compara el valor **Disponible** de cada almacén de objetos (volumen) con el nivel máximo optimizado que anotaste para ese Storage Node.
3. Si al menos un volumen de cada nodo de almacenamiento en línea tiene más espacio disponible que el umbral máximo optimizado para ese nodo, ve a [Utiliza marcas de agua optimizadas](#) para empezar a usar los umbrales optimizados.

De lo contrario, amplía la grid lo antes posible. O bien ["añadir volúmenes de almacenamiento"](#) a un nodo existente o ["agrega nuevos nodos de almacenamiento"](#). Luego, ve a [Utiliza marcas de agua optimizadas](#) para actualizar la configuración de la marca de agua.

4. Si necesitas seguir utilizando valores personalizados para los umbrales del volumen de almacenamiento, ["silencio"](#) o ["desactivar"](#) la alerta **Anulación del umbral bajo de solo lectura**.



Se aplican los mismos valores de marca de agua personalizados a todos los volúmenes de almacenamiento de cada Storage Node. El uso de valores inferiores a los recomendados para las marcas de agua de los volúmenes de almacenamiento podría provocar que algunos volúmenes de almacenamiento quedaran inaccesibles (se desmontaran automáticamente) cuando el nodo alcance su capacidad.

Usa marcas de agua optimizadas

Pasos

1. Ve a **Support > Other > Storage watermarks**.
2. Marca la casilla **Usar valores optimizados**.
3. Selecciona **Guardar**.

Ya están en vigor los ajustes optimizados de los límites máximos de los volúmenes de almacenamiento para cada volumen, en función del tamaño del Storage Node y de la capacidad relativa del volumen.

Soluciona problemas de metadatos en StorageGRID

Si se producen problemas con los metadatos, las alertas te informarán sobre el origen de los problemas y las acciones recomendadas que debes realizar. En particular, debes añadir nuevos nodos de almacenamiento si se activa la alerta Low metadata storage.

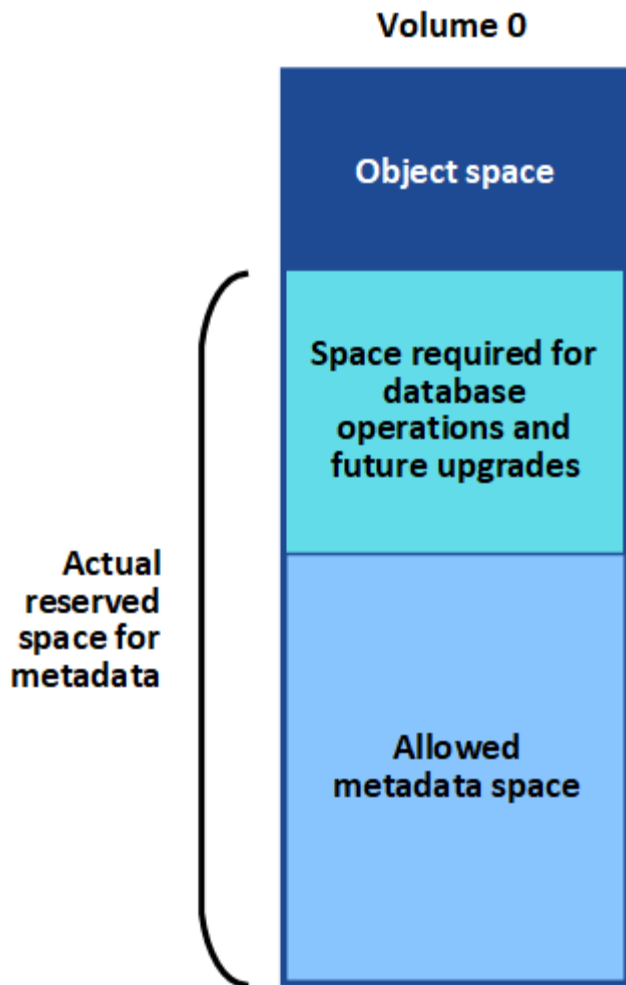
Antes de empezar

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

Acerca de esta tarea

Sigue las acciones recomendadas para cada alerta relacionada con los metadatos que se active. Si se activa la alerta **Low metadata storage**, debes añadir nuevos Storage Nodes.

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



Si los metadatos de los objetos ocupan más del 100% del espacio asignado a los metadatos, las operaciones de la base de datos no pueden ejecutarse de forma eficiente y se producirán errores.

Puedes ["supervisar la capacidad de metadatos de los objetos para cada Storage Node"](#) para ayudarte a anticipar errores y corregirlos antes de que ocurran.

StorageGRID utiliza la siguiente métrica de Prometheus para medir el nivel de ocupación del espacio de metadatos permitido:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

Cuando esta expresión de Prometheus alcanza determinados umbrales, se activa la alerta **Low metadata storage**.

- **Menor:** los metadatos de objetos están utilizando el 70 % o más del espacio de metadatos permitido. Deberías añadir nuevos Storage Nodes lo antes posible.
- **Grave:** Los metadatos de los objetos ocupan el 90 % o más del espacio permitido para metadatos. Debes añadir nuevos Storage Nodes inmediatamente.



Cuando los metadatos de los objetos ocupan el 90 % o más del espacio permitido para metadatos, aparece una advertencia en el panel de control. Si aparece esta advertencia, debes añadir nuevos Storage Nodes inmediatamente. Nunca debes permitir que los metadatos de los objetos ocupen más del 100 % del espacio permitido.

- **Crítico:** los metadatos de objetos están utilizando el 100 % o más del espacio de metadatos permitido y están empezando a consumir el espacio necesario para las operaciones esenciales de la base de datos. Debes detener la ingesta de nuevos objetos y debes añadir nuevos Storage Nodes de inmediato.



Si el tamaño del volumen 0 es menor que la opción de almacenamiento Metadata Reserved Space (por ejemplo, en un entorno que no sea de producción), el cálculo de la alerta **Low metadata storage** podría ser inexacto.

Pasos

1. Selecciona **Alertas > Actuales**.
2. En la tabla de alertas, despliega el grupo de alertas **Bajo almacenamiento de metadatos**, si es necesario, y selecciona la alerta concreta que quieras ver.
3. Revisa los detalles en el cuadro de diálogo de alerta.
4. Si se ha activado una alerta importante o crítica de **Low metadata storage**, realiza una ampliación para añadir Storage Nodes de inmediato.



Dado que StorageGRID conserva copias completas de todos los metadatos de los objetos en cada sitio, la capacidad de metadatos de toda la red viene limitada por la capacidad de metadatos del sitio más pequeño. Si necesitas aumentar la capacidad de metadatos de un sitio, también debes "[ampliar cualquier otro sitio](#)" en el mismo número de nodos de almacenamiento.

Después de que realices la expansión, StorageGRID redistribuye los metadatos de objetos existentes a los nuevos nodos, lo que aumenta la capacidad general de metadatos del grid. No es necesario que realices ninguna acción. La alerta **Low metadata storage** se desactiva.

Soluciona errores de certificado en StorageGRID

Si detectas algún problema de seguridad o relacionado con el certificado al intentar conectarte a StorageGRID mediante un navegador web, un cliente S3 o una herramienta de supervisión externa, debes comprobar el certificado.

Acerca de esta tarea

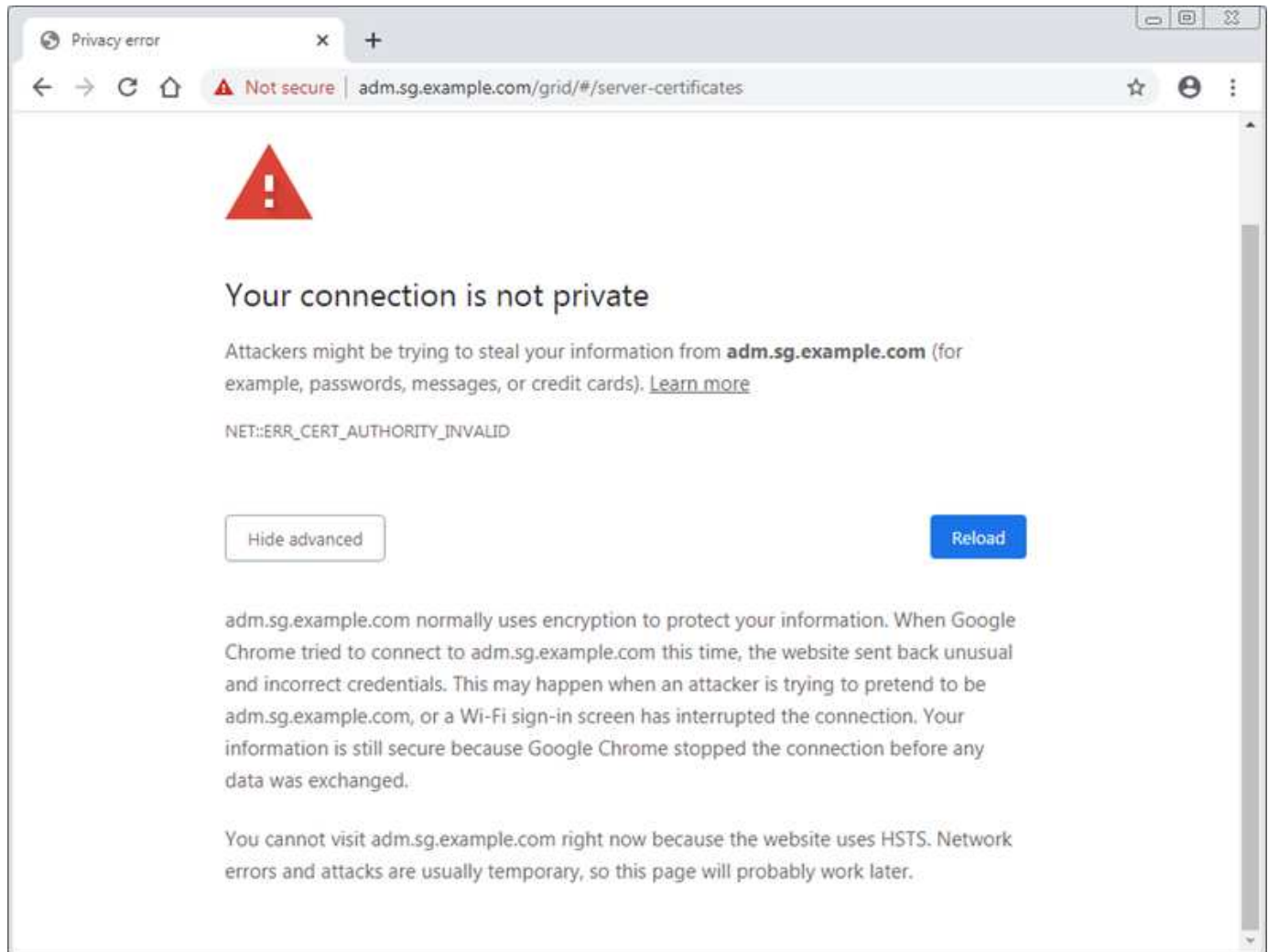
Los errores de certificado pueden causar problemas cuando intentas conectarte a StorageGRID mediante el Grid Manager, la Grid Management API, el Tenant Manager o la Tenant Management API. Los errores de certificado también pueden ocurrir cuando intentas conectarte con un cliente S3 o una herramienta de monitoreo externa.

Si accedes al Grid Manager o al Tenant Manager utilizando un nombre de dominio en lugar de una dirección IP, el navegador muestra un error de certificado sin opción de ignorarlo si se da alguna de las siguientes situaciones:

- El certificado de tu interfaz de gestión personalizada caduca.
- Vuelves de un certificado personalizado de la interfaz de administración al certificado predeterminado del

servidor.

El siguiente ejemplo muestra un error de certificado cuando ha caducado el certificado de la interfaz de gestión personalizada:



Para garantizar que las operaciones no se vean interrumpidas por un fallo en el certificado del servidor, se activa la alerta **Caducidad del certificado del servidor para la interfaz de gestión** cuando el certificado del servidor está a punto de caducar.

Cuando se utilizan certificados de cliente para la integración externa con Prometheus, los errores de certificado pueden deberse al certificado de la interfaz de gestión de StorageGRID o a los certificados de cliente. La alerta **Caducidad de los certificados de cliente configurados en la página Certificados** se activa cuando un certificado de cliente está a punto de caducar.

Pasos

Si has recibido una notificación de alerta sobre un certificado caducado, accede a los detalles del certificado: . Selecciona **Configuración > Seguridad > Certificados** y luego "[Selecciona la pestaña del certificado correspondiente](#)".

1. Comprueba el periodo de validez del certificado. + Algunos navegadores web y clientes S3 no aceptan certificados con un periodo de validez superior a 398 días.
2. Si el certificado ha caducado o va a caducar pronto, sube o genera un nuevo certificado.

- Para un certificado de servidor, consulta los pasos para ["configurar un certificado de servidor personalizado para Grid Manager y Tenant Manager"](#).
 - Para un certificado de cliente, consulta los pasos para ["configuración de un certificado de cliente"](#).
3. Para errores de certificado del servidor, prueba una o ambas de las siguientes opciones:
- Asegúrate de que el Nombre alternativo del sujeto (SAN) del certificado esté relleno y de que dicho SAN coincida con la dirección IP o el nombre de host del nodo al que te estás conectando.
 - Si intentas conectarte a StorageGRID utilizando un nombre de dominio:
 - i. Introduce la dirección IP del nodo de administración en lugar del nombre de dominio para evitar el error de conexión y acceder al Grid Manager.
 - ii. Desde el Grid Manager, selecciona **Configuración > Seguridad > Certificados** y luego ["Selecciona la pestaña del certificado correspondiente"](#) para instalar un nuevo certificado personalizado o continuar con el certificado predeterminado.
 - iii. En las instrucciones para administrar StorageGRID, consulta los pasos para ["configurar un certificado de servidor personalizado para Grid Manager y Tenant Manager"](#).

Soluciona problemas del nodo de administración y de la interfaz de usuario en StorageGRID

Puedes realizar varias tareas que te ayudarán 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 experimentas un error al iniciar sesión en un nodo de administración de StorageGRID, es posible que tu sistema tenga un problema con un ["redes"](#) o ["hardware"](#), un problema con ["Servicios del nodo de administración"](#) o un ["problema con la base de datos Cassandra"](#) en los nodos de almacenamiento conectados.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el archivo `Passwords.txt`.
- Tienes ["permisos de acceso específicos"](#).

Acerca de esta tarea

Sigue estas instrucciones de resolución de problemas si ves 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. Espera 10 minutos e intenta iniciar sesión de nuevo.

Si el error no se soluciona automáticamente, pasa al siguiente paso.

2. Si tu sistema StorageGRID tiene más de un nodo de administración, intenta iniciar sesión en Grid Manager desde otro nodo de administración para comprobar el estado de un nodo de administración que no está disponible.
 - Si puedes iniciar sesión, puedes utilizar las opciones **Panel de control**, **Nodos**, **Alertas** y **Soporte** para ayudarte a determinar la causa del error.
 - Si solo tienes un nodo de administración o sigues sin poder iniciar sesión, pasa al siguiente paso.
3. Comprueba si el hardware del nodo está desconectado.
4. Si el inicio de sesión único (SSO) está habilitado en tu sistema StorageGRID, consulta los pasos para ["configuración del inicio de sesión único"](#).

Es posible que tengas que desactivar y volver a activar temporalmente el inicio de sesión único en un único nodo de administración para resolver cualquier problema.



Si el inicio de sesión único (SSO) está activado, no puedes iniciar sesión utilizando un puerto restringido. Debes utilizar el puerto 443.

5. Comprueba si la cuenta que estás utilizando pertenece a un usuario federado.

Si la cuenta de usuario federada no funciona, intenta iniciar sesión en Grid Manager como usuario local, como root.

- Si el usuario local puede iniciar sesión:
 - i. Revisa las alertas.
 - ii. Selecciona **Configuración > Control de acceso > Federación de identidades**.
 - iii. Haz clic en **Probar conexión** para validar la configuración de tu conexión con el servidor LDAP.
 - iv. Si la prueba falla, soluciona cualquier error de configuración.
- Si el usuario local no puede iniciar sesión y estás seguro de que las credenciales son correctas, pasa al siguiente paso.

6. Utiliza Secure Shell (SSH) para iniciar sesión en el nodo de administración:

- a. Introduce el siguiente comando: `ssh admin@Admin_Node_IP`
- b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
- d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

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

Asegúrate de que los servicios nms, mi, nginx y mgmt api estén todos en funcionamiento.

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. Comprueba que el servicio nginx-gw esté en funcionamiento # `service nginx-gw status`

9. Usa Lumberjack para recopilar registros: # `/usr/local/sbin/lumberjack.rb`

Si el error de autenticación se produjo en el pasado, puedes utilizar las opciones `--start` y `--end` del script Lumberjack para especificar el intervalo de tiempo correspondiente. Utiliza `lumberjack -h` para obtener más información sobre estas opciones.

La salida en la terminal indica dónde se ha copiado el archivo de registro.

10. Revisa los siguientes registros:

- ° `/var/local/log/bycast.log`
- ° `/var/local/log/bycast-err.log`
- ° `/var/local/log/nms.log`

◦ `**/*commands.txt`

11. Si no has podido detectar ningún problema con el nodo de administración, ejecuta cualquiera de los siguientes comandos para determinar las direcciones IP de los tres nodos de almacenamiento que ejecutan el servicio ADC en tu sitio. Normalmente, se trata de los tres primeros nodos de almacenamiento que se instalaron 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, utiliza ssh para iniciar sesión en cada uno de los nodos de almacenamiento ADC, usando las direcciones IP que identificaste.
13. Ver el estado de todos los servicios que se están ejecutando en el nodo de la red: `storagegrid-status`

Asegúrate de que los servicios idnt, acct, nginx y cassandra estén todos en funcionamiento.

14. Repite los pasos [Usa Lumberjack para recopilar registros](#) y [Revisar los registros](#) para revisar los registros en los Storage Nodes.
15. Si no consigues resolver el problema, ponte en contacto con el soporte técnico.

Envía los registros que hayas recopilado al soporte técnico. Consulta también ["Referencia de los archivos de registro"](#).

Problemas con la interfaz de usuario

Es posible que la interfaz de usuario de Grid Manager o Tenant Manager no responda como se espera después de actualizar el software StorageGRID.

Pasos

1. Asegúrate de que estás utilizando un ["navegador web compatible"](#).
2. Borra la caché de tu navegador web.

Al vaciar la caché se eliminan los recursos obsoletos utilizados por la versión anterior del software StorageGRID, y permite que la interfaz de usuario vuelva a funcionar correctamente. Para obtener instrucciones, consulta la documentación de tu navegador web.

Soluciona problemas de red, hardware y plataforma en StorageGRID

Hay varias tareas que puedes realizar para ayudar a determinar el origen de los problemas relacionados con la red, el hardware y la plataforma de StorageGRID.

[[422-unprocessable-entity-errors]]
== Errores "422: Entidad no procesable"

El error 422: «Entidad no procesable» puede producirse por diferentes motivos. Consulta el mensaje de error

para determinar cuál es la causa de tu problema.

Si ves uno de los mensajes de error que aparecen en la lista, realiza la acción recomendada.

Mensaje de error	Causa raíz y medidas correctivas
<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 seleccionas la opción No utilizar TLS para Transport Layer Security (TLS) al configurar la federación de identidades mediante Windows Active Directory (AD). El uso de la opción Do not use TLS no es compatible con los servidores de AD que exigen la firma de LDAP. Debes seleccionar la opción Use STARTTLS o la opción Use LDAPS para TLS.
<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 intentas utilizar un cifrado no compatible para establecer una conexión TLS (Transport Layer Security) desde StorageGRID a un sistema externo utilizado para la federación de identidades o Cloud Storage Pools. Comprueba los algoritmos de cifrado que ofrece el sistema externo. El sistema debe usar uno de los "algoritmos de cifrado compatibles con StorageGRID" para las conexiones TLS salientes, como se muestra en las instrucciones para administrar StorageGRID.

Alerta de discrepancia de MTU en la Grid Network

La alerta **Discrepancia en la MTU de la red Grid** se activa cuando la configuración de la unidad máxima de transmisión (MTU) de la interfaz de red Grid (eth0) varía de forma significativa entre los nodos de la grid.

Acerca de esta tarea

Las diferencias en la configuración de la MTU podrían indicar que algunas, pero no todas, las redes eth0 están configuradas para tramas jumbo. Una discrepancia en el tamaño de la MTU superior a 1000 podría causar problemas de rendimiento en la red.

Pasos

1. El acceso externo por SSH está bloqueado de forma predeterminada. Si es necesario, ["permitir el acceso de forma temporal"](#).
2. Indica los parámetros de MTU de eth0 en todos los nodos.
 - Utiliza la consulta proporcionada en el Grid Manager.
 - Accede a *primary Admin Node IP address/metrics/graph* e introduce la siguiente consulta:
`node_network_mtu_bytes{device="eth0"}`
3. ["Modificar la configuración de MTU"](#) según sea necesario para asegurarte de que sean iguales para la interfaz de la red de grid (eth0) en todos los nodos.
 - Para nodos basados en Linux y VMware, usa el siguiente comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

Ejemplo: `change-ip.py -n node 1500 grid admin`

Nota: en los nodos basados en Linux, si el valor de MTU deseado para la red en el contenedor supera el valor ya configurado en la interfaz del host, primero debes configurar la interfaz del host para que tenga el valor de MTU deseado y luego usar el script `change-ip.py` para cambiar el valor de MTU de la red en el contenedor.

Utiliza los siguientes argumentos para modificar el MTU en nodos basados en Linux o VMware.

Argumentos posicionales	Descripción
mtu	La MTU que vas a configurar. Debe estar en el rango de 1280 a 9216.
network	Las redes a las que se aplicará el MTU. Incluye uno o más de los siguientes tipos de red: • grid • administrador • cliente

+

Argumentos opcionales	Descripción
-h, - help	Mostrar el mensaje de ayuda y salir.

Argumentos opcionales	Descripción
<code>-n node, --node node</code>	El nodo. El valor predeterminado es el nodo local.

- Si has permitido el acceso SSH externo, "[bloquear el acceso](#)" cuando hayas terminado la tarea.

Alerta de error en la trama de recepción de la red de nodos

Las alertas de **Node network reception frame error** pueden deberse a problemas de conectividad entre StorageGRID y tu hardware de red. Esta alerta se borra sola después de que se resuelve el problema subyacente.

Acerca de esta tarea

Las alertas de «**Error en la trama de recepción de la red del nodo**» pueden deberse a los siguientes problemas relacionados con el hardware de red que se conecta a StorageGRID:

- Se requiere la corrección de errores hacia adelante (FEC) y no está en uso
- Incompatibilidad entre el puerto del switch y la MTU de la NIC
- Altas tasas de error en los enlaces
- Desbordamiento del búfer circular de la NIC

Pasos

- Sigue los pasos de resolución de problemas para todas las posibles causas de esta alerta según la configuración de tu red.
- Sigue los siguientes pasos en función de la causa del error:

Desajuste de FEC



Estos pasos solo son aplicables a las alertas de **Error de trama de recepción de red del nodo** provocadas por una discrepancia de FEC en los dispositivos StorageGRID.

- a. Comprueba el estado FEC del puerto en el switch conectado a tu dispositivo StorageGRID.
- b. Comprueba la integridad física de los cables que van desde el dispositivo hasta el conmutador.
- c. Si quieres cambiar los parámetros de FEC para intentar resolver la alerta, primero asegúrate de que el dispositivo esté configurado en modo **Auto** en la página de Configuración de enlace del StorageGRID Appliance Installer (consulta las instrucciones para tu dispositivo):
 - "SG6160"
 - "SGF6112"
 - "SG6000"
 - "SG5800"
 - "SG5700"
 - "SG110 y SG1100"
 - "SG100 y SG1000"
- d. Cambia la configuración de FEC en los puertos del switch. Los puertos del dispositivo StorageGRID ajustarán su configuración de FEC para que coincida, si es posible.

No puedes configurar los parámetros de FEC en los dispositivos StorageGRID. En su lugar, los dispositivos intentan detectar y replicar los parámetros de FEC de los puertos del switch a los que están conectados. Si se fuerzan los enlaces a velocidades de red de 25 GbE o 100 GbE, es posible que el switch y la NIC no logren negociar un parámetro de FEC común. Sin una configuración FEC común, la red pasará al modo "sin FEC". Cuando la FEC no está habilitada, las conexiones son más susceptibles a errores causados por el ruido eléctrico.



Los dispositivos StorageGRID admiten Firecode (FC) y Reed Solomon (RS) FEC, así como sin FEC.

Incompatibilidad entre el puerto del switch y la MTU de la NIC

Si la alerta se debe a una discrepancia entre el puerto del switch y el tamaño de MTU de la NIC, comprueba que el tamaño de MTU configurado en el nodo sea el mismo que la configuración de MTU del puerto del switch.

El tamaño de MTU configurado en el nodo podría ser menor que el ajuste en el puerto del switch al que está conectado el nodo. Si un nodo de StorageGRID recibe una trama de Ethernet mayor que su MTU, lo cual es posible con esta configuración, podría informarse de la alerta **Error de trama de recepción de red de nodo**. Si crees que esto es lo que está pasando, cambia la MTU del puerto del switch para que coincida con la MTU de la interfaz de red de StorageGRID, o bien cambia la MTU de la interfaz de red de StorageGRID para que coincida con la del puerto del switch, según tus 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 **Desajuste de MTU de la red Grid** se activa si existe una diferencia significativa en la configuración de MTU de la red Grid en los distintos nodos. No es necesario que los valores de MTU sean iguales para todos los tipos de red. Consulta [Soluciona la alerta de discrepancia de MTU en la red Grid](#) para más información.



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

Altas tasas de error en los enlaces

- Activa FEC, si aún no está activada.
- Comprueba que el cableado de red sea de buena calidad y que no esté dañado ni mal conectado.
- Si los cables no parecen ser el problema, ponte en contacto con soporte técnico.



Es posible que observes unas tasas de error elevadas en un entorno con mucho ruido eléctrico.

Desbordamiento del búfer circular de la NIC

Si el error se debe a un desbordamiento del búfer circular de la tarjeta de red, ponte en contacto con soporte técnico.

El búfer circular puede saturarse cuando el sistema StorageGRID está sobrecargado y no puede procesar los eventos de red a tiempo.

- Supervisa el problema y ponte en contacto con el soporte técnico si la alerta no se resuelve.

Errores de sincronización horaria

Es posible que detectes problemas de sincronización horaria en tu grid.

Si tienes problemas de sincronización horaria, verifica que hayas especificado al menos cuatro fuentes NTP externas, que cada una proporcione una referencia Stratum 3 o mejor, y que todas las fuentes NTP externas estén funcionando normalmente y sean accesibles por tus nodos de StorageGRID.



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

Linux: Problemas de conectividad de red

Es posible que veas problemas de conectividad de red en los nodos de StorageGRID alojados en hosts Linux.

Clonación de direcciones MAC

En algunos casos, puedes resolver los problemas de red usando la clonación de direcciones MAC. Si usas hosts virtuales, establece el valor de la clave de clonación de direcciones MAC para cada una de tus redes en "true" en tu archivo de configuración del nodo. Esta configuración hace que la dirección MAC del contenedor

de StorageGRID use la dirección MAC del host. Consulta las instrucciones para ["crear archivos de configuración de nodos"](#).



Crea interfaces de red virtuales independientes para que las use el sistema operativo host de Linux. Si usas las mismas interfaces de red para el sistema operativo host de Linux y el contenedor de StorageGRID, el sistema operativo host podría quedar inaccesible si no has habilitado el modo promiscuo en el hipervisor.

Para obtener más información, consulta las instrucciones de ["activar la clonación de direcciones MAC"](#).

Modo promiscuo

Si no deseas utilizar la clonación de direcciones MAC y prefieres permitir que todas las interfaces reciban y transmitan datos para direcciones MAC distintas de las asignadas por el hipervisor, asegúrate de que las propiedades de seguridad a nivel de conmutador virtual y de grupo de puertos estén configuradas en **Aceptar** para el modo promiscuo, los cambios de dirección MAC y las transmisiones falsificadas. Los valores configurados en el conmutador virtual pueden ser anulados por los valores a nivel de grupo de puertos, así que asegúrate de que la configuración sea la misma en ambos lugares.

Para obtener más información sobre cómo utilizar el modo promiscuo, consulta las instrucciones para ["Cómo configurar la red del host"](#).

Linux: el estado del nodo es «huérfano»

Un nodo de Linux en estado «huérfano» suele indicar que, o bien el servicio storagegrid o bien el demonio del nodo StorageGRID que controla el contenedor del nodo se ha detenido de forma inesperada.

Acerca de esta tarea

Si un nodo de Linux indica que se encuentra en estado huérfano, debes:

- Comprueba los registros en busca de errores y mensajes.
- Intenta volver a iniciar el nodo.
- Si es necesario, utiliza los comandos del motor de contenedores para detener el contenedor del nodo existente.
- Reinicia el nodo.

Pasos

1. Comprueba los registros tanto del demonio del servicio como del nodo huérfano para detectar errores evidentes o mensajes sobre salidas inesperadas.
2. Inicia sesión en el host como root o usando una cuenta con permisos sudo.
3. Intenta volver a iniciar el nodo ejecutando el siguiente comando: `$ sudo storagegrid node start node-name`

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

Si el nodo queda huérfano, la respuesta es

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. En Linux, detén el motor de contenedores y cualquier proceso storagegrid-node que esté controlando. Por ejemplo: `sudo docker stop --time secondscontainer-name`

En `seconds`, introduce el número de segundos que quieres esperar a que se detenga el contenedor (normalmente 15 minutos o menos). Por ejemplo:

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

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

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

Linux: Soluciona problemas de compatibilidad con IPv6

Es posible que tengas que habilitar la compatibilidad con IPv6 en el kernel si has instalado nodos de StorageGRID en hosts Linux y notas que no se han asignado direcciones IPv6 a los contenedores de los nodos como esperabas.

Acerca de esta tarea

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

1. Selecciona **Nodos** y elige el nodo.
2. Selecciona **Mostrar direcciones IP adicionales** junto a **Direcciones IP** en la pestaña **Resumen**.

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

Pasos

1. Inicia sesión en el host como root o usando una cuenta con permisos sudo.
2. Ejecuta el siguiente comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

El resultado debería ser 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```



Si el resultado no es 0, consulta la documentación de tu sistema operativo para cambiar la configuración de `sysctl`. Luego, cambia el valor a 0 antes de continuar.

3. Accede al contenedor del nodo de StorageGRID: `storagegrid node enter node-name`
4. Ejecuta 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 es aplicable. Ponte en contacto con el soporte técnico.

5. Sal del contenedor: `exit`

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

6. Como root, edita el siguiente archivo: `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Localiza las siguientes dos líneas y elimina las etiquetas de comentario. A continuación, guarda y cierra el archivo.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Ejecuta estos comandos para reiniciar el contenedor de StorageGRID:

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

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

Soluciona los mensajes de error del servidor syslog externo para StorageGRID

La siguiente tabla describe los mensajes de error que podrían estar relacionados con el uso de un servidor syslog externo y enumera las medidas correctivas.

El asistente para configurar el servidor syslog externo muestra estos errores si tienes problemas a la hora de enviar mensajes de prueba para comprobar que el servidor syslog externo está configurado correctamente.

Los problemas que surjan durante la ejecución pueden notificarse mediante la alerta "[Error de reenvío del servidor syslog externo](#)". Si recibes esta alerta, sigue las instrucciones en la alerta para reenviar los mensajes de prueba y así poder obtener mensajes de error detallados.

Para obtener más información sobre cómo enviar información de auditoría a un servidor syslog externo, consulta:

- "[Aspectos a tener en cuenta al utilizar un servidor syslog externo](#)"
- "[Configura la gestión de registros y el servidor syslog externo](#)"

Mensaje de error	Descripción y acciones recomendadas
No se puede resolver el nombre de host	El FQDN que introdujiste para el servidor syslog no se pudo resolver en una dirección IP. 1. Comprueba el nombre de host que has introducido. Si has introducido una dirección IP, asegúrate de que sea una dirección IP válida en notación W.X.Y.Z ("decimal con puntos"). 2. Comprueba que los servidores DNS estén configurados correctamente. 3. Confirma que cada nodo pueda acceder a las direcciones IP del servidor DNS.
Conexión rechazada	Se ha rechazado una conexión TCP o TLS con el 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. Comprueba que has introducido correctamente el FQDN o la dirección IP, el puerto y el protocolo del servidor syslog. 2. Comprueba que el servidor del servicio syslog esté ejecutando un demonio syslog que esté a la escucha en el puerto especificado. 3. Comprueba que ningún cortafuegos esté bloqueando el acceso a las conexiones TCP/TLS desde los nodos hacia la dirección IP y el puerto del servidor syslog.
No se puede acceder a la red	El servidor syslog no se encuentra en una subred conectada directamente. Un router devolvió un mensaje de error ICMP para indicar que no pudo reenviar los mensajes de prueba desde los nodos indicados al servidor syslog. 1. Comprueba que hayas introducido el FQDN o la dirección IP correctos para el servidor syslog. 2. Para cada nodo de la lista, comprueba la lista de subredes de la red Grid, las listas de subredes de las redes de administración y las puertas de enlace de la red de clientes. Confirma que estén configuradas para enrutar el tráfico hacia el servidor syslog a través de la interfaz de red y la puerta de enlace previstas (Grid, Admin o Client).

Mensaje de error	Descripción y acciones recomendadas
Host inalcanzable	El servidor syslog está en una subred conectada directamente (la subred que usan los nodos indicados para sus direcciones IP de Grid, Admin o de cliente). Los nodos intentaron enviar mensajes de prueba, pero no recibieron respuesta a las solicitudes ARP para la dirección MAC del servidor syslog. 1. Comprueba que hayas introducido el FQDN o la dirección IP correctos para el servidor syslog. 2. Comprueba que el servidor que ejecuta el servicio syslog esté en funcionamiento.
Se agotó el tiempo de espera de la conexión	Se intentó establecer 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 el tráfico sin enviar ninguna respuesta (una configuración común). 1. Comprueba que hayas introducido el FQDN o la dirección IP correctos para el servidor syslog. 2. Para cada nodo de la lista, comprueba la lista de subredes de la red de Grid, las listas de subredes de las redes de administración y las puertas de enlace de la red de cliente. Confirma que estén configuradas para enrutar el tráfico al servidor syslog mediante la interfaz de red y la puerta de enlace (Grid, administración o cliente) a través de las cuales esperas que se acceda al servidor syslog. 3. Comprueba que ningún cortafuegos esté bloqueando el acceso a las conexiones TCP/TLS desde los nodos indicados a la dirección IP y al puerto del servidor syslog.
Conexión cerrada por el socio	Se estableció correctamente una conexión TCP con el servidor syslog, pero se cerró más tarde. Entre los motivos de esto se pueden incluir: • Es posible que el servidor syslog se haya reiniciado o reiniciado el sistema. • Es posible que el nodo y el servidor syslog tengan configuraciones TCP/TLS diferentes. • Es posible que un cortafuegos intermedio esté cerrando las conexiones TCP inactivas. • Es posible que un servidor que no sea de syslog y que esté a la escucha en el puerto del servidor de syslog haya cerrado la conexión. Para resolver este problema: 1. Comprueba que has introducido correctamente el FQDN o la dirección IP, el puerto y el protocolo del servidor syslog. 2. Si utilizas TLS, comprueba que el servidor syslog también utilice TLS. Si utilizas TCP, comprueba que el servidor syslog también utilice TCP. 3. Comprueba que no haya ningún firewall intermedio configurado para cerrar las conexiones TCP inactivas.

Mensaje de error	Descripción y acciones recomendadas
Error de certificado TLS	El certificado del servidor recibido del servidor syslog no era compatible con el paquete de certificados de la CA y el certificado de cliente que proporcionaste. 1. Comprueba que el paquete de certificados de la CA y el certificado de cliente (si lo hay) sean compatibles con el certificado del servidor syslog. 2. Comprueba que las identidades del certificado 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. Revisa los registros de depuración que acompañan a este error para intentar determinar la causa raíz.
Sesión TLS finalizada	El servidor syslog terminó la sesión TLS y StorageGRID no puede detectar el motivo. 1. Revisa los registros de depuración que acompañan a este error para intentar determinar la causa raíz. 2. Comprueba que has introducido correctamente el FQDN o la dirección IP, el puerto y el protocolo del servidor syslog. 3. Si utilizas TLS, comprueba que el servidor syslog también utilice TLS. Si utilizas TCP, comprueba que el servidor syslog también utilice TCP. 4. Comprueba que el paquete de certificados de la CA y el certificado de cliente (si lo hay) sean compatibles con el certificado del servidor syslog. 5. Comprueba que las identidades del certificado del servidor syslog incluyan los valores de IP o FQDN esperados.
Error al consultar los resultados	El nodo de administración utilizado para la configuración y las pruebas del servidor syslog no puede solicitar los resultados de las pruebas a los nodos indicados. Es posible que uno o varios nodos estén inactivos. 1. Sigue los pasos habituales de resolución de problemas para asegurarte de que los nodos estén en línea y que todos los servicios esperados estén en funcionamiento. 2. Reinicia el servicio «miscd» en los nodos indicados.

Conoce los problemas de almacenamiento en caché del equilibrador de carga en StorageGRID

Infórmate sobre los posibles problemas con el almacenamiento en caché del equilibrador de carga y cómo solucionarlos.

Determina si una solicitud fue un acierto en la caché

- El encabezado X-Cache se establece en la respuesta a las solicitudes gestionadas por el servicio de caché. Códigos posibles:

- HIT: El objeto se sirvió desde la caché
- PARTIAL-HIT: El bucket/key tenía un registro en la caché, pero no se pudo servir desde la caché todo el rango solicitado
- STALE: el bucket/key tenía un registro en la caché, pero el objeto se actualizó desde la última vez que se entregó desde la caché.
- MISS: el objeto no estaba en la caché
- El `nginx-gw/endpoint-access.log.gz` registro de la solicitud incluye "unix:/run/cache-svc/cache-svc.sock" para las solicitudes gestionadas por la caché.
- El `cache-svc/cache-svc.log` muestra un mensaje como: «Request 320390: completed successfully (cache hit)» o «Request 320375: completed successfully (cache miss)». Busca la ruta solicitada buscando otros registros con la misma cadena «Request <number>».

Baja tasa de aciertos en la caché

- Es normal que se produzcan bajas tasas de aciertos en la caché cuando se añade una nueva carga de trabajo o cuando cambia el conjunto de trabajo al que accede una carga de trabajo. En estas situaciones, se espera que la tasa de aciertos aumente con el tiempo.
- Si varias cargas de trabajo utilizan el almacenamiento en caché, considera añadir políticas de clasificación de tráfico para aislar las partes de las cargas de trabajo a las que la caché presta servicio. Las métricas de tasa de aciertos de la caché están disponibles por cada política de clasificación de tráfico. Si algunas cargas de trabajo no registran una buena tasa de aciertos de la caché, considera moverlas a otros endpoints que no tengan habilitado el almacenamiento en caché.
- Evalúa la tasa de expulsión de la caché. Si la caché es demasiado pequeña para albergar el conjunto de trabajo, experimentará altas tasas de expulsión y podría contribuir a una menor tasa de aciertos.
- Es posible que FPVR ofrezca opciones para mejorar las tasas de aciertos de determinadas cargas de trabajo.

Bajo rendimiento

- Evalúa la tasa de aciertos de la caché. Una tasa de aciertos de la caché baja puede provocar un rendimiento general bajo.
- Evalúa la tasa de desalojo de la caché. Durante el desalojo, se utilizan algunos recursos de almacenamiento para eliminar objetos existentes del disco. Si el proceso de desalojo no sigue el ritmo del acceso de nuevos objetos, el sistema podría alcanzar los umbrales de marca de agua estricta y empezar a omitir la caché.
- Comprueba los límites de red usando los diagnósticos "Network interfaces receive usage" y "Network interfaces transmit usage".

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. Puedes usar esta información para leer y analizar la pista de auditoría de la actividad del sistema.

Estas instrucciones son para los administradores responsables de generar informes sobre la actividad y el uso

del sistema que requieran el análisis de los mensajes de auditoría del sistema StorageGRID.

Para utilizar el archivo de registro de texto, debes tener acceso al recurso compartido de auditoría configurado en el Admin Node.

Para obtener información sobre cómo configurar los niveles de los mensajes de auditoría y usar un servidor syslog externo, consulta ["Configura la gestión de registros y el servidor syslog externo"](#).

Cómo los mensajes de auditoría se mueven a través del sistema StorageGRID hasta el archivo audit.log para su retención

Todos los servicios de StorageGRID generan mensajes de auditoría durante el funcionamiento normal del sistema. Deberías entender cómo estos mensajes de auditoría se mueven a través del sistema StorageGRID hasta el archivo `audit.log`.

Los siguientes flujos de trabajo para los mensajes de auditoría y la retención de mensajes de auditoría solo son aplicables si StorageGRID está configurado para **Admin Nodes/local nodes** o **Admin Node and external syslog server**. Si StorageGRID está configurado para "Local nodes only" (por defecto) o "External syslog server", los mensajes de auditoría se guardan localmente en cada nodo en el archivo `/var/local/log/localaudit.log` y no pueden ser procesados por los Admin Nodes ni por los Storage Nodes.

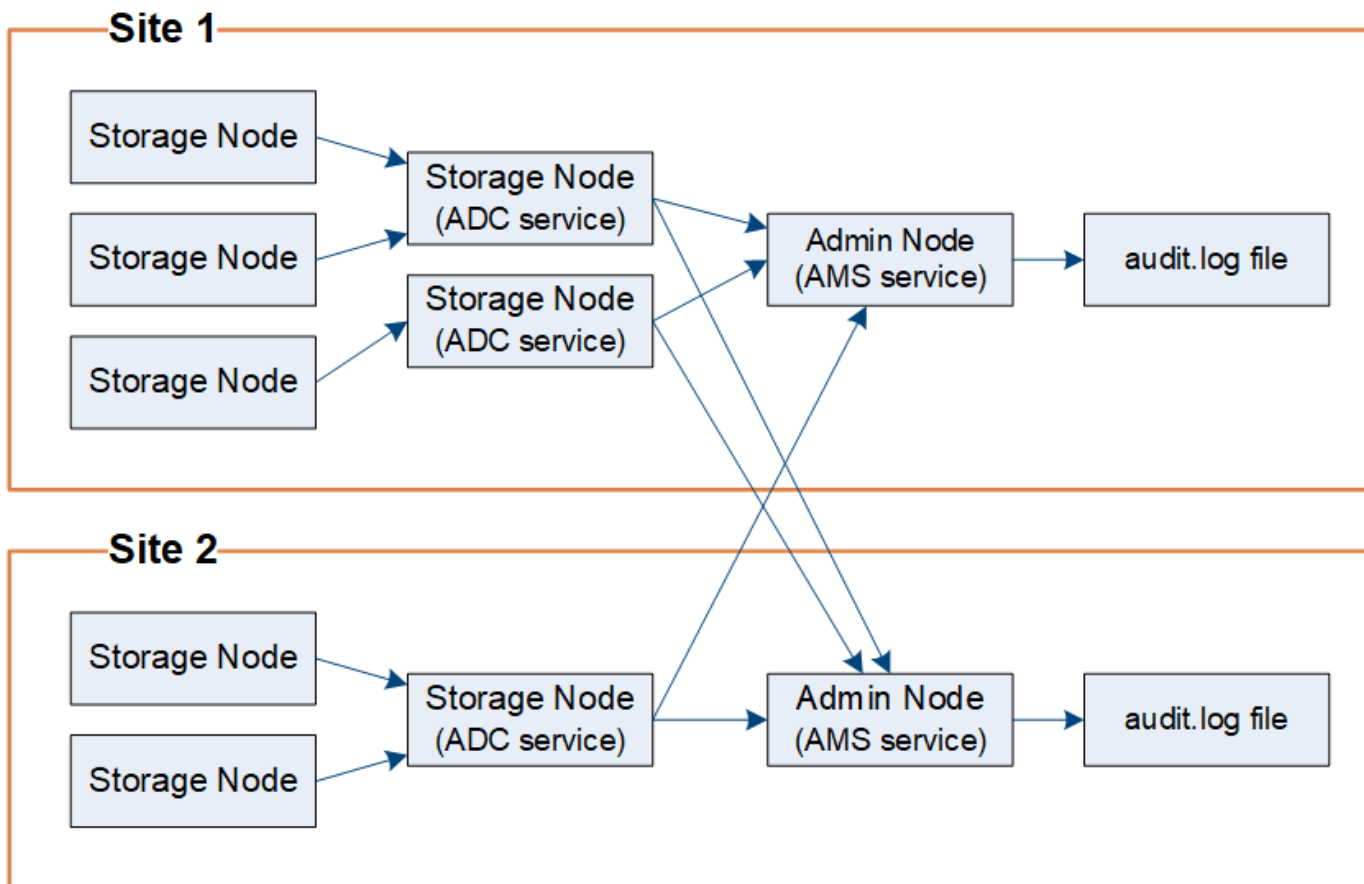
Flujo de mensajes de auditoría

Los mensajes de auditoría son procesados por los nodos de administración cuando StorageGRID está configurado para **nodos de administración/nodos locales** o **nodo de administración y servidor syslog externo** y por aquellos nodos de almacenamiento que tienen un servicio de controlador de dominio administrativo (ADC).

Como se muestra en el diagrama de flujo de mensajes de auditoría, cada nodo de 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 tres primeros nodos de almacenamiento instalados en cada sitio.

A su vez, cada servicio ADC actúa como relé y envía su conjunto de mensajes de auditoría a cada nodo de administración en el sistema StorageGRID, lo que le da a cada nodo de administración un registro completo de la actividad del sistema.

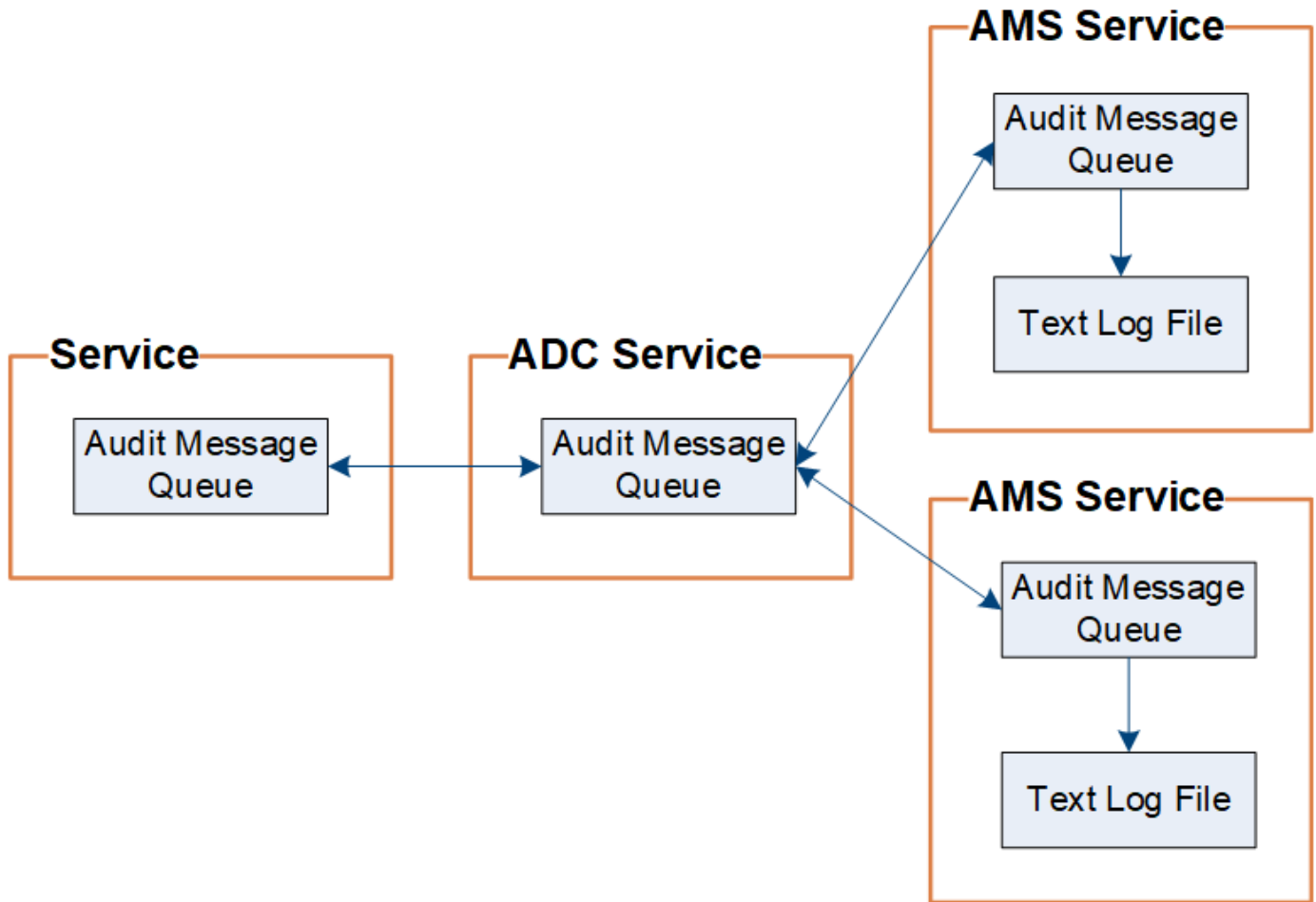
Cada nodo de administración almacena los mensajes de auditoría en archivos de registro de texto; el archivo de registro activo se llama `audit.log`.



Conservación de los mensajes de auditoría

StorageGRID utiliza un proceso de copia y eliminación para garantizar que no se pierda ningún mensaje de auditoría antes de que se pueda registrar 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 grid. Siempre se conserva 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 directorio del Admin Node `/var/local/audit/export`. 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 a una capacidad de auditoría insuficiente. A medida que las colas aumentan, consumen más espacio disponible en el directorio de cada nodo `/var/local/`. Si el problema persiste y el directorio de mensajes de auditoría de un nodo se llena demasiado, los nodos individuales priorizan procesar su trabajo pendiente y dejan de estar disponibles temporalmente para nuevos mensajes.

En concreto, es posible que observes los siguientes comportamientos:

- Si el directorio `/var/local/audit/export` que usa un nodo de administración se llena, el nodo de administración se marcará como no disponible para nuevos mensajes de auditoría hasta que el directorio deje de estar lleno. Las solicitudes de los clientes S3 no se ven afectadas. La alarma XAMS (repositorios de auditoría inaccesibles) se activa cuando un repositorio de auditoría no está accesible.
- Si el directorio `/var/local/` que utiliza un nodo de almacenamiento con el servicio ADC llega al 92 % de su capacidad, el nodo se marcará como no disponible para los mensajes de auditoría hasta que el directorio vuelva a estar al 87 % de su capacidad. Las solicitudes de clientes S3 a otros nodos no se ven afectadas. La alarma NRLY (retransmisores de auditoría disponibles) se activa cuando no se puede acceder a los retransmisores de auditoría.



Si no hay nodos de almacenamiento disponibles con el servicio ADC, los nodos de almacenamiento almacenan los mensajes de auditoría de forma local en el archivo `/var/local/log/localaudit.log`.

- Si el directorio `/var/local/` que usa un nodo de almacenamiento se llena al 85 %, el nodo empezará a rechazar las solicitudes de clientes S3 con `503 Service Unavailable`.

Los siguientes tipos de problemas pueden provocar que las colas de mensajes de auditoría alcancen un tamaño muy grande:

- La interrupción del servicio de un nodo de administración o de un nodo de almacenamiento que ejecute el servicio ADC. Si uno de los nodos del sistema está inactivo, los nodos restantes podrían acumular retrasos.
- Un ritmo de actividad sostenido que supera la capacidad de auditoría del sistema.
- El espacio `/var/local/` de un nodo de almacenamiento ADC se está llenando por razones no relacionadas con los mensajes de auditoría. Cuando esto ocurre, el nodo deja de aceptar nuevos mensajes de auditoría y prioriza su acumulación actual, lo que puede causar acumulaciones en otros nodos.

Alerta de cola de auditoría grande y alarma «Audit Messages Queued» (AMQS)

Para ayudarte a supervisar el tamaño de las colas de mensajes de auditoría a lo largo del tiempo, se activan la alerta **Large audit queue** y la alarma AMQS heredada cuando el número de mensajes en una cola de Storage Node o Admin Node alcanza ciertos umbrales.

Si se activa la alerta **Cola de auditoría grande** o la alarma AMQS heredada, empieza por comprobar la carga del sistema—si recientemente se ha producido un número significativo de transacciones, la alerta y la alarma deberían desaparecer con el tiempo y pueden ignorarse.

Si la alerta o alarma persiste y aumenta su gravedad, consulta un gráfico del tamaño de la cola. Si el número aumenta de forma constante durante horas o días, es probable que la carga de auditoría haya superado la capacidad de auditoría del sistema. Reduce la tasa de operaciones del cliente o disminuye el número de mensajes de auditoría registrados cambiando el nivel de auditoría para Client Writes y Client Reads a Error o Off. Consulta ["Configura la gestión de registros y el servidor syslog externo"](#).

Mensajes duplicados

El sistema StorageGRID adopta un enfoque conservador en caso de que se produzca un fallo en la red o en un nodo. Por este motivo, es posible que haya mensajes duplicados en el registro de auditoría.

Accede a los archivos de registro de auditoría desde la línea de comandos del nodo de administración de StorageGRID

El recurso compartido de auditoría contiene el archivo `audit.log` activo y cualquier archivo de registro de auditoría comprimido. Puedes acceder a los archivos de registro de auditoría directamente desde la línea de comandos del Admin Node.

El archivo `audit.log` permanece vacío a menos que configures StorageGRID para **Admin Nodes/local nodes** o **Admin Node and external syslog server**. Para más información, consulta ["Selecciona la ubicación del registro"](#).

Antes de empezar

- Tienes ["permisos de acceso específicos"](#).
- Debes tener el archivo `Passwords.txt`.
- Debes conocer la dirección IP de un nodo de administración.

Pasos

1. Inicia sesión en un nodo de administración:

- a. Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
- b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
- d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

2. Ve al directorio que contiene los archivos de auditoría:

```
cd /var/local/audit/export/
```

3. Consulta el archivo de auditoría actual o uno guardado, según sea necesario.

Conoce la rotación de archivos de registro de auditoría en StorageGRID

Si StorageGRID está configurado para **nodos de administración/nodos locales o nodo de administración y servidor syslog externo**, los archivos de registros de auditoría se guardan en el directorio `/var/local/audit/export/` del nodo de administración. Los archivos de registro de auditoría activos se denominan `audit.log`.



Opcionalmente, puedes cambiar el destino de los registros de auditoría y enviar la información de auditoría a un servidor syslog externo. Los registros locales de auditoría se siguen generando y almacenando cuando se configura un servidor syslog externo. Consulta ["Configura los mensajes de auditoría y el servidor syslog externo"](#).

Una vez al día, el archivo activo `audit.log` se guarda y se inicia un nuevo archivo `audit.log`. El nombre del archivo guardado indica cuándo se guardó, en el formato `yyyy-mm-dd.txt`. Si se crea más de un registro de auditoría en un solo día, los nombres de los archivos usan la fecha en que se guardó el archivo, seguida de 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 el segundo archivo de registro creados y guardados el 15 de abril de 2018.

Después de un día, el archivo guardado se comprime y se cambia de nombre, con el formato `yyyy-mm-dd.txt.gz`, que conserva la fecha original. Con el tiempo, se consume el almacenamiento del nodo de administración asignado para los registros de auditoría. Un script supervisa el consumo de espacio de los registros de auditoría y elimina los archivos de registro según sea necesario para liberar espacio en el directorio `/var/local/audit/export/`. Los registros de auditoría se eliminan en función de la fecha en la que se crearon. Los registros más antiguos se eliminan primero. Puedes supervisar las acciones del script en el siguiente archivo: `/var/local/log/manage-audit.log`.

Este ejemplo muestra el archivo activo `audit.log`, el archivo del día anterior (`2018-04-15.txt`) y el archivo comprimido del día anterior (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Formato del archivo de registro de auditoría

Conoce el formato de los archivos de registro de auditoría en StorageGRID

Los archivos de registro de auditoría se encuentran en cada nodo de administración y contienen un conjunto de mensajes de auditoría individuales.

Cada mensaje de auditoría contiene lo siguiente:

- La hora universal coordinada (UTC) del evento que desencadenó el mensaje de auditoría (ATIM) en formato ISO 8601, seguida de un espacio:

YYYY-MM-DDTHH:MM:SS.UUUUUU, donde *UUUUUU* son microsegundos.

- El propio mensaje de auditoría, entre corchetes y que comienza con `AUDT`.

El siguiente ejemplo muestra tres mensajes de auditoría en un archivo de registro de auditoría (se han añadido saltos de línea para facilitar la lectura). Estos mensajes se generaron cuando un inquilino creó un bucket de S3 y añadió dos objetos a ese bucket.

2019-08-07T18:43:30.247711

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]
```

2019-08-07T18:43:30.783597

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]
```

2019-08-07T18:43:30.784558

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

En su formato predeterminado, los mensajes de auditoría de los archivos de registro de auditoría no son fáciles de leer ni de interpretar. Puedes usar ["herramienta audit-explain"](#) para obtener resúmenes simplificados de los mensajes de auditoría en el registro de auditoría. Puedes usar ["herramienta audit-sum"](#) para resumir cuántas operaciones de escritura, lectura y eliminación se registraron y cuánto tiempo tardaron estas operaciones.

Usa la herramienta audit-explain para traducir los mensajes de auditoría de StorageGRID

Puedes usar la herramienta `audit-explain` 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 archivo `Passwords.txt`.
- Debes conocer la dirección IP del nodo de administración principal.

Acerca de esta tarea

La herramienta `audit-explain`, disponible en el Admin Node principal, proporciona resúmenes simplificados de los mensajes de auditoría en un registro de auditoría.



La herramienta `audit-explain` está pensada principalmente para que el soporte técnico la utilice durante las operaciones de resolución de problemas. Procesar consultas de `audit-explain` puede consumir una gran cantidad de potencia de CPU, lo que podría afectar las operaciones de StorageGRID.

Este ejemplo muestra el resultado típico de la `audit-explain` herramienta. Estos cuatro **"SPUT"** mensajes de auditoría se generaron cuando el inquilino de S3 con el ID de cuenta 92484777680322627870 utilizó solicitudes PUT de S3 para crear un bucket llamado "bucket1" y añadir tres objetos a ese bucket.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

La herramienta `audit-explain` puede hacer lo siguiente:

- Procesa logs de auditoría sin formato o comprimidos. Por ejemplo:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

- Procesar varios archivos a la vez. Por ejemplo:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

- Acepta datos procedentes de una tubería, lo que te permite filtrar y preprocesar los datos mediante el comando `grep` u otros métodos. Por ejemplo:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Como los registros de auditoría pueden ser muy grandes y lentos de analizar, puedes ahorrar tiempo filtrando las partes que quieres examinar y ejecutando `audit-explain` en esas partes, en lugar de en todo el archivo.



La herramienta `audit-explain` no acepta archivos comprimidos como entrada por tubería. Para procesar archivos comprimidos, proporciona sus nombres de archivo como argumentos en la línea de comandos o usa la herramienta `zcat` para descomprimir los archivos primero. Por ejemplo:

```
zcat audit.log.gz | audit-explain
```

Usa la opción `help` (`-h`) para ver las opciones disponibles. Por ejemplo:

```
$ audit-explain -h
```

Pasos

1. Inicia sesión en el nodo de administración principal:
 - a. Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Introduce el siguiente comando, donde `/var/local/audit/export/audit.log` representa el nombre y la ubicación del archivo o archivos que deseas analizar:

```
$ audit-explain /var/local/audit/export/audit.log
```

La herramienta `audit-explain` muestra interpretaciones legibles 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 quieres ver las marcas de tiempo, usa la opción de marca de tiempo (`-t`).

Usa la herramienta `audit-sum` para resumir los mensajes de auditoría de StorageGRID

Puedes usar la herramienta `audit-sum` para contar los mensajes de auditoría de escritura, lectura, head y eliminación, y para ver el tiempo (o tamaño) mínimo, máximo y promedio de cada tipo de operación.

Antes de empezar

- Tienes "[permisos de acceso específicos](#)".
- Tienes el archivo `Passwords.txt`.
- Conoces la dirección IP del nodo de administración principal.

Acerca de esta tarea

La herramienta `audit-sum`, disponible en el nodo de administración primario, resume cuántas operaciones de escritura, lectura y eliminación se registraron y cuánto tiempo tardaron estas operaciones.



La `audit-sum` herramienta está pensada principalmente para que el soporte técnico la utilice durante las operaciones de resolución de problemas. Procesar consultas de `audit-sum` puede consumir una gran cantidad de potencia de CPU, lo que podría afectar las operaciones de StorageGRID.

Este ejemplo muestra la salida típica de la herramienta `audit-sum`. Este ejemplo muestra cuánto tiempo tardaron las operaciones de protocolo.

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

La herramienta `audit-sum` proporciona recuentos y tiempos para los siguientes mensajes de auditoría de S3 e ILM en un registro de auditoría.



Los códigos de auditoría se eliminan del producto y de la documentación a medida que las funciones quedan obsoletas. Si encuentras un código de auditoría que no aparece en esta lista, consulta las versiones anteriores de este tema para versiones anteriores de StorageGRID. Por ejemplo, ["StorageGRID 11.8 Uso de la herramienta de suma de auditoría"](#).

Código	Descripción	Consulta
IDEL	Eliminación iniciada por ILM: registra cuando ILM inicia el proceso de eliminar un objeto.	"IDEL: eliminación iniciada por ILM"
SDEL	S3 DELETE: Registra una transacción realizada con éxito para eliminar un objeto o un bucket.	"SDEL: S3 DELETE"
SGET	S3 GET: Registra una transacción realizada con éxito para recuperar un objeto o mostrar la lista de objetos en un bucket.	"SGET: S3 GET"
SHEA	S3 HEAD: Registra una transacción exitosa para comprobar la existencia de un objeto o bucket.	"SHEA: S3 HEAD"

Código	Descripción	Consulta
SPUT	S3 PUT: Registra una transacción realizada con éxito para crear un nuevo objeto o bucket.	"SPUT: S3 PUT"

La herramienta `audit-sum` puede hacer lo siguiente:

- Procesa logs de auditoría sin formato o comprimidos. Por ejemplo:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

- Procesar varios archivos a la vez. Por ejemplo:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

- Acepta datos procedentes de una tubería, lo que te permite filtrar y preprocesar los datos mediante el comando `grep` u otros métodos. 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 por tubería. Para procesar archivos comprimidos, proporciona sus nombres de archivo como argumentos en la línea de comandos o usa la herramienta `zcat` para descomprimir los archivos primero. Por ejemplo:

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

Puedes usar las opciones de la línea de comandos para resumir las operaciones en los buckets por separado de las operaciones en los objetos, o para agrupar los resúmenes de mensajes por nombre de bucket, por período de tiempo o por tipo de destino. De forma predeterminada, los resúmenes muestran el tiempo de operación mínimo, máximo y promedio, pero puedes usar la opción `size` (`-s`) para ver el tamaño del objeto en su lugar.

Usa la opción `help` (`-h`) para ver las opciones disponibles. Por ejemplo:

```
$ audit-sum -h
```

Pasos

1. Inicia sesión en el nodo de administración principal:

- a. Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`

- b. Introduce la contraseña que figura en el archivo `Passwords.txt`.

c. Introduce el siguiente comando para pasar a ser usuario root: `su -`

d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Si quieres analizar todos los mensajes relacionados con las operaciones de escritura, lectura, head y eliminación, sigue estos pasos:

a. Introduce el siguiente comando, donde `/var/local/audit/export/audit.log` representa el nombre y la ubicación del archivo o archivos que deseas analizar:

```
$ audit-sum /var/local/audit/export/audit.log
```

Este ejemplo muestra la salida típica de la herramienta `audit-sum`. Este ejemplo muestra cuánto tiempo tardaron las operaciones de protocolo.

message group average (sec)	count	min (sec)	max (sec)
=====	=====	=====	=====
=====			
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

En este ejemplo, las operaciones SGET (S3 GET) son las más lentas en promedio, con 1,13 segundos, pero tanto SGET como SPUT (S3 PUT) muestran tiempos máximos de alrededor de 1.770 segundos.

b. Para mostrar las 10 operaciones de recuperación más lentas, utiliza el comando `grep` para seleccionar únicamente los mensajes SGET y añade la opción de salida extendida (`-l`) para incluir las rutas de los objetos:

```
grep SGET audit.log | audit-sum -l
```

Los resultados incluyen el tipo (objeto o bucket) y la ruta, lo que te permite buscar en el registro de auditoría otros mensajes relacionados con estos objetos concretos.

```

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 resultados, puedes ver que las tres solicitudes GET de S3 más lentas fueron para objetos de unos 5 GB de tamaño, que es mucho mayor que el de los demás objetos. El gran tamaño explica los tiempos de recuperación más lentos en el peor de los casos.

3. Si quieres determinar qué tamaños de objetos se están ingesting en tu grid y recuperando de él, usa 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 medio de objeto para SPUT es inferior a 2,5 MB, pero el tamaño medio para SGET es mucho mayor. El número de mensajes SPUT es mucho mayor que el número de mensajes SGET, lo que indica que la mayoría de los objetos nunca se recuperan.

4. Si quieres saber si ayer las recuperaciones fueron lentas:

- a. Ejecuta el comando en el registro de auditoría correspondiente y utiliza la opción group-by-time (-gt), seguida del intervalo 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 alcanzó un pico entre las 06:00 y las 07:00. Tanto el valor máximo como el promedio son considerablemente más altos durante este intervalo de tiempo, y no aumentaron de forma gradual a medida que crecía el recuento. Estas métricas sugieren que se superó la capacidad, posiblemente en la red o en la capacidad del grid para procesar las solicitudes.

- b. Para determinar qué tamaño de objetos se recuperaron cada hora ayer, añade 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 se produjeron algunas recuperaciones muy grandes cuando el tráfico global de recuperaciones estaba en su punto máximo.

- c. Para ver más detalles, usa el ["herramienta audit-explain"](#) para revisar todas las operaciones SGET durante esa hora:

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Si se prevé que el resultado del comando `grep` sea de muchas líneas, añade el comando `less` para mostrar el contenido del archivo de auditoría una página (una pantalla) a la vez.

5. Si quieres determinar si las operaciones SPUT en buckets son más lentas que las operaciones SPUT en objetos:

- a. Empieza utilizando la opción `-go`, que agrupa los mensajes de las operaciones con objetos y buckets 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 buckets presentan características de rendimiento diferentes a las de las operaciones SPUT para objetos.

- b. Para determinar qué buckets tienen las operaciones SPUT más lentas, utiliza la opción `-gb`, que agrupa los mensajes por bucket:

```
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 buckets tienen el mayor tamaño de objeto SPUT, usa tanto la opción `-gb` como la `-s`:

```
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 de mensaje de auditoría

Conoce la estructura de los mensajes de auditoría de StorageGRID

Los mensajes de auditoría intercambiados dentro del sistema StorageGRID incluyen información estándar común a todos los mensajes y contenido específico que describe el evento o la actividad que se está reportando.

Si la información resumida que proporcionan las herramientas ["audit-explain"](#) y ["suma de auditoría"](#) no es suficiente, consulta esta sección para conocer el formato general de todos los mensajes de auditoría.

A continuación se muestra un ejemplo de mensaje de auditoría tal y como podría aparecer en el archivo 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 atributo. La cadena completa está entre paréntesis ([]) y cada elemento de atributo de la cadena presenta las siguientes características:

- Entre corchetes []
- Introducido por la cadena AUDT, que indica un mensaje de auditoría
- Sin delimitadores (sin comas ni espacios) ni antes ni después
- Terminado por un carácter de salto de línea \n

Cada elemento incluye un código de atributo, un tipo de datos y un valor que se indican en este formato:

```
[ATTR(type):value] [ATTR(type):value] ...  
[ATTR(type):value]\n
```

El número de elementos de atributo en el mensaje depende del tipo de evento del mensaje. Los elementos de atributo no se enumeran en ningún orden en particular.

La siguiente lista describe los elementos de atributos:

- **ATTR** es un código de cuatro caracteres para el atributo que se está notificando. Hay algunos atributos que son comunes a todos los mensajes de auditoría y otros que son específicos de cada evento.
- **type** es un identificador de cuatro caracteres que indica el tipo de datos de programación del valor, como UI64, FC32, y así sucesivamente. El tipo va entre paréntesis ().
- **value** es el contenido del atributo, normalmente un valor numérico o de texto. Los valores siempre van después de dos puntos (:). Los valores del tipo de datos CSTR están entre comillas dobles "".

Tipos de datos en los mensajes de auditoría de StorageGRID

Se utilizan distintos 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 por 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 siguiendo estas convenciones: • La barra invertida es \. • El retorno de carro es \r. • Las comillas dobles son \". • El salto de línea (nueva línea) es \n. • Los caracteres pueden sustituirse por sus equivalentes hexadecimales (en el formato \xHH, donde HH es el valor hexadecimal que representa el carácter).

Datos específicos del evento en los mensajes de auditoría de StorageGRID

Cada mensaje de auditoría en el registro de auditoría recoge datos específicos de un evento del sistema.

Después del contenedor de apertura [AUDT: que identifica al propio mensaje, el siguiente conjunto de atributos proporciona información sobre el evento o la acción que describe el mensaje de auditoría. Estos atributos se destacan en el siguiente ejemplo:

```
2018-12-05T08:24:45.921845 [AUDT: \[RSLT\ (FC32\):SUCS\]
\[TIME\ (UI64\):11454\]\[SAIP\ (IPAD\):"10.224.0.100"\]\[S3AI\ (CSTR\):"60025
621595611246499"\]
\[SACC\ (CSTR\):"account"\]\[S3AK\ (CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dY
zKlumRsKJA=="\]
\[SUSR\ (CSTR\):"urn:sgws:identity:60025621595611246499:root"\]
\[SBAI\ (CSTR\):"60025621595611246499"\]\[SBAC\ (CSTR\):"account"\]\[S3BK\ (C
STR\):"bucket"\]
\[S3KY\ (CSTR\):"object"\]\[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] [A
MID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261\]
```

El elemento ATYP (subrayado en el ejemplo) identifica qué evento generó el mensaje. Este mensaje de ejemplo incluye el código de mensaje "SHEA" ([ATYP(FC32):SHEA]), lo que indica que se generó mediante una solicitud S3 HEAD exitosa.

Elementos comunes en los mensajes de auditoría de StorageGRID

Todos los mensajes de auditoría contienen los elementos comunes.

Código	Tipo	Descripción
AMID	FC32	ID del módulo: identificador de cuatro caracteres del módulo que generó el mensaje. Esto indica el segmento de código en el que se generó el mensaje de auditoría.
ANID	UI32	ID de nodo: el ID de nodo de grid asignado al servicio que generó el mensaje. A cada servicio se le asigna un identificador único en el momento en que se configura e instala el sistema StorageGRID. Este ID no se puede cambiar.
ASES	UI64	Identificador de sesión de auditoría: en versiones anteriores, este elemento indicaba el momento en el que se inicializaba el sistema de auditoría tras el inicio del servicio. Este valor de tiempo se medía en microsegundos desde la época del sistema operativo (00:00:00 UTC del 1 de enero de 1970). Nota: Este elemento ha quedado obsoleto y ya no aparece en los mensajes de auditoría.

Código	Tipo	Descripción
ASQN	UI64	Recuento de secuencias: en versiones anteriores, este contador se incrementaba por cada mensaje de auditoría generado en el nodo de la red (ANID) y se ponía a cero al reiniciar el servicio. Nota: Este elemento ha quedado obsoleto y ya no aparece en los mensajes de auditoría.
ATID	UI64	ID de rastreo: un identificador que es compartido por el conjunto de mensajes que fueron activados por un solo evento.
ATIM	UI64	Marca de tiempo: hora en la que se generó el evento que desencadenó el mensaje de auditoría, medida en microsegundos desde la época del sistema operativo (00:00:00 UTC del 1 de enero de 1970). Ten en cuenta que la mayoría de las herramientas disponibles para convertir la marca de tiempo a la fecha y hora locales se basan en milisegundos. Es posible que tengas que redondear o truncar la marca de hora registrada. La hora legible por humanos que aparece al principio del mensaje de auditoría en el archivo <code>audit.log</code> 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 de texto literal que indica el inicio del segmento de hora 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 rige el contenido del "payload" del mensaje: los atributos que se incluyen.
AVER	UI32	Versión: la versión del mensaje de auditoría. A medida que el software StorageGRID evoluciona, es posible que las nuevas versiones de los servicios incorporen nuevas funciones en los informes de auditoría. Este campo permite la compatibilidad con versiones anteriores en el 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 evitar que el mensaje sea filtrado accidentalmente.

Formato de mensajes de auditoría de StorageGRID y ejemplos

Puedes encontrar información detallada en cada mensaje de auditoría. Todos los mensajes de auditoría usan el mismo formato.

A continuación, se muestra un mensaje de auditoría de ejemplo tal como podría aparecer en el archivo `audit.log`:

```
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 propio mensaje de auditoría.

Para identificar qué evento se ha registrado en el mensaje de auditoría, busca 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. "SPUT" representa una transacción PUT de S3, que registra la incorporación de un objeto a un bucket.

El siguiente mensaje de auditoría también muestra el bucket 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 saber cuándo se produjo el evento PUT, fíjate en la marca de tiempo en Tiempo Universal Coordinado (UTC) que aparece al principio del mensaje de auditoría. Este valor es una versión legible para el usuario del atributo ATIM del propio mensaje de auditoría:

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, transcurrido desde el inicio de la época UNIX. En el ejemplo, el valor 1405631878959669 corresponde al jueves, 17-jul-2014 21:17:59 UTC.

Mensajes de auditoría y el ciclo de vida de los objetos

Cuando se generan mensajes de auditoría en StorageGRID

Se generan mensajes de auditoría cada vez que se ingiere, se recupera o se elimina un objeto. Puedes identificar estas transacciones en el registro de auditoría buscando los mensajes de auditoría específicos de la API de S3.

Los mensajes de auditoría se vinculan mediante identificadores específicos de cada protocolo.

Protocolo	Código
Vinculación de operaciones S3	S3BK (bucket), S3KY (key) o ambos
Vinculando las operaciones internas	CBID (identificador interno del objeto)

Momento de los mensajes de auditoría

Debido a factores como las diferencias de sincronización entre los nodos de la grid, el tamaño de los objetos y los retrasos de la red, el orden de los mensajes de auditoría generados por los distintos servicios puede diferir del que se muestra en los ejemplos de esta sección.

Mensajes de auditoría para transacciones de ingesta de objetos en StorageGRID

Puedes identificar las transacciones de carga de datos de los clientes en el registro de auditoría buscando los mensajes de auditoría específicos de la API de S3.

No todos los mensajes de auditoría generados durante una transacción de ingestión aparecen en la siguiente tabla. Solo se incluyen los mensajes necesarios para realizar el seguimiento de la transacción de ingestión.

Mensajes de auditoría de ingestión S3

Código	Nombre	Descripción	Traza	Ver
SPUT	Transacción PUT de S3	Una transacción de ingestión PUT en S3 se ha completado correctamente.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Reglas del objeto cumplidas	Se ha cumplido la política de ILM para este objeto.	CBID	"ORLM: reglas del objeto cumplidas"

Ejemplo: carga de objetos en S3

La siguiente serie de mensajes de auditoría es un ejemplo de los mensajes de auditoría que se generan y se guardan en el registro de auditoría cuando un cliente S3 introduce un objeto en un nodo de almacenamiento (servicio LDR).

En este ejemplo, la política de ILM activa incluye la regla de ILM Make 2 Copies.



No todos los mensajes de auditoría generados durante una transacción se muestran en el ejemplo de abajo. Solo se muestran los relacionados con la transacción de ingesta de S3 (SPUT).

Este ejemplo asume que ya se ha creado un bucket de S3.

SPUT: S3 PUT

El mensaje SPUT se genera para indicar que se ha iniciado una transacción PUT de S3 para crear un objeto en un bucket 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):"SGKHya1RU_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: reglas del objeto cumplidas

El mensaje de ORLM indica que se ha cumplido la política de ILM para este objeto. El mensaje incluye el CBID del objeto y el nombre de la regla de ILM que se aplicó.

En el caso de los objetos replicados, el campo LOCS incluye el identificador del nodo LDR y el identificador de volumen de las ubicaciones del objeto.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID(UI64):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

En el caso de los objetos con código de borrado, el campo LOCS incluye el identificador del perfil de código de borrado y el identificador del grupo de código de borrado

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP(FC32):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

El campo PATH incluye información del bucket S3 y la clave.

```
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]]
```

Mensajes de auditoría para transacciones de eliminación de objetos en StorageGRID

Puedes identificar las transacciones de eliminación de objetos en el registro de auditoría buscando 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 tablas siguientes. Solo se incluyen los mensajes necesarios para realizar el seguimiento de la transacción de eliminación.

Mensajes de auditoría de eliminación de S3

Código	Nombre	Descripción	Traza	Ver
SDEL	Eliminar S3	Solicitud para eliminar el objeto de un bucket.	CBID, S3KY	"SDEL: S3 DELETE"

Ejemplo: eliminación de un objeto de S3

Cuando un cliente S3 elimina un objeto de un nodo de almacenamiento (servicio LDR), se genera un mensaje de auditoría que se guarda en el registro de auditoría.



No todos los mensajes de auditoría generados durante una transacción de eliminación se muestran en el ejemplo a continuación. Solo se muestran los relacionados con la transacción de eliminación de S3 (SDEL).

SDEL: Eliminación de S3

La eliminación de un objeto comienza cuando el cliente envía una solicitud DeleteObject a un servicio LDR. El mensaje contiene el bucket del que se va a 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]]
```

Mensajes de auditoría para transacciones de recuperación de objetos en StorageGRID

Puedes identificar las transacciones de recuperación de objetos en el registro de auditoría buscando los mensajes de auditoría específicos de la API de S3.

No todos los mensajes de auditoría generados durante una transacción de recuperación figuran en la tabla siguiente. Solo se incluyen los mensajes necesarios para rastrear la transacción de recuperación.

Mensajes de auditoría de recuperación de S3

Código	Nombre	Descripción	Traza	Ver
SGET	S3 GET	Solicitud realizada para recuperar un objeto de un bucket.	CBID, S3BK, S3KY	"SGET: S3 GET"

Ejemplo: recuperación de objeto S3

Cuando un cliente S3 recupera un objeto de un nodo de almacenamiento (servicio LDR), se genera un

mensaje de auditoría que se guarda en el registro de auditoría.

Ten en cuenta que no todos los mensajes de auditoría generados durante una transacción se enumeran en el siguiente ejemplo. Solo se enumeran los relacionados con la transacción de recuperación de S3 (SGET).

SGET: S3 GET

La recuperación de objetos comienza cuando el cliente envía una solicitud GetObject a un servicio LDR. El mensaje contiene el bucket del que se va a 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 de bucket lo permite, un cliente puede recuperar objetos de forma anónima o puede recuperar objetos de un bucket que pertenezca a una cuenta de inquilino diferente. El mensaje de auditoría contiene información sobre la cuenta de inquilino del propietario del bucket para que puedas realizar el seguimiento de estas solicitudes anónimas y entre cuentas.

En el siguiente mensaje de ejemplo, el cliente envía una solicitud GetObject para un objeto almacenado en un bucket que no le pertenece. Los valores de SBAI y SBAC registran el ID y el nombre de la cuenta de inquilino del propietario del bucket, 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):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Ejemplo: selección de un objeto en S3

Cuando un cliente de S3 realiza una consulta S3 Select sobre un objeto, se generan mensajes de auditoría que se guardan en el registro de auditoría.

Ten en cuenta que no todos los mensajes de auditoría generados durante una transacción se muestran en el siguiente ejemplo. Solo se muestran aquellos relacionados con la transacción S3 Select (SelectObjectContent).

Cada consulta genera dos mensajes de auditoría: uno que lleva a cabo la autorización de la solicitud S3 Select (el campo S3SR se establece en "select") y una operación GET estándar posterior que recupera los datos del almacenamiento durante el procesamiento.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\": \"unix:\"}"]][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Mensajes de auditoría para actualizaciones de metadatos de objetos S3 en StorageGRID

Los mensajes de auditoría se generan cuando un cliente de S3 actualiza los metadatos de un objeto.

Mensajes de auditoría de actualización de metadatos de S3

Código	Nombre	Descripción	Traza	Ver
SUPD	Metadatos de S3 actualizados	Se genera cuando un cliente de S3 actualiza los metadatos de un objeto ingerido.	CBID, S3KY, HTRH	"SUPD: Metadatos de 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 de S3

El cliente S3 realiza una solicitud (SUPD) para actualizar los metadatos especificados (`x-amz-meta-*`) del objeto S3 (S3KY). En este ejemplo, los encabezados de la solicitud se incluyen en el campo HTRH porque se ha configurado como encabezado del protocolo de auditoría (`*Configuration* > Monitoring > Audit and syslog server`). Consulta ["Configura la gestión de registros y el servidor syslog externo"](#).

```
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

Conoce los tipos y códigos de mensajes de auditoría en StorageGRID

En las siguientes secciones se incluyen descripciones detalladas de los mensajes de auditoría que devuelve el sistema. Cada mensaje de auditoría aparece primero en una tabla que agrupa los mensajes relacionados según la clase de actividad que representa cada uno. Estas agrupaciones resultan útiles tanto para comprender los tipos de actividades que se auditan como para seleccionar el tipo deseado de filtrado de

mensajes de auditoría.

Los mensajes de auditoría también se enumeran por orden alfabético según sus códigos de cuatro caracteres. Esta lista alfabética te permite encontrar información sobre mensajes concretos.

Los códigos de cuatro caracteres utilizados a lo largo de este capítulo son los valores ATYP que aparecen 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 los mensajes de auditoría, cambiar los destinos de los registros y utilizar un servidor syslog externo para tu información de auditoría, consulta ["Configura la gestión de registros y el servidor syslog externo"](#)

Categorías de mensajes de auditoría

Mensajes de auditoría para eventos del sistema en StorageGRID

Los mensajes de auditoría pertenecientes a la categoría de auditoría del sistema se usan para eventos relacionados con el propio sistema de auditoría, los estados de los nodos de grid, la actividad de tareas a nivel de todo el sistema (tareas de grid) y las operaciones de copia de seguridad de servicios.

Código	Título y descripción del mensaje	Ver
ECMC	Falta un fragmento de datos con código de borrado: indica que se ha detectado un fragmento de datos con código de borrado faltante.	"ECMC: fragmento de datos con código de borrado ausente"
ECOC	Fragmento de datos con código de borrado dañado: indica que se ha detectado un fragmento de datos con código de borrado dañado.	"ECOC: fragmento de datos con código de borrado corrupto"
ETAF	Error de autenticación de seguridad: falló un intento de conexión usando Transport Layer Security (TLS).	"ETAF: Error de autenticación de seguridad"
GNRG	Registro en GNDS: un servicio actualizó o registró información sobre sí mismo en el sistema StorageGRID.	"GNRG: Inscripción en GNDS"
GNUR	Cancelación del registro de GNDS: un servicio se ha dado de baja del sistema StorageGRID.	"GNUR: Baja del GNDS"

Código	Título y descripción del mensaje	Ver
GTED	Tarea de la red finalizada: el servicio CMN terminó de procesar la tarea de la red.	"GTED: tarea de la red finalizada"
GTST	Tarea de la red iniciada: el servicio CMN comenzó a procesar la tarea de la red.	"GTST: tarea de grid iniciada"
GTSU	Tarea de grid enviada: Se envió una tarea de grid al servicio CMN.	"GTSU: tarea de red enviada"
LLST	Pérdida de ubicación: este mensaje de auditoría se genera cuando se pierde una ubicación.	"LLST: ubicación perdida"
OLST	Objeto perdido: No se puede localizar el objeto solicitado en el sistema StorageGRID.	"OLST: el sistema detectó un objeto perdido"
SADD	Desactivación de la auditoría de seguridad: se desactivó el registro de mensajes de auditoría.	"SADD: desactivación de la auditoría de seguridad"
SADE	Activación de la auditoría de seguridad: se ha restablecido el registro de mensajes de auditoría.	"SADE: activación de la auditoría de seguridad"
SVRF	Error en la verificación del almacén de objetos: un bloque de contenido no pasó las comprobaciones de verificación.	"SVRF: Fallo en la verificación del almacén de objetos"
SVRU	Verificación desconocida del almacén de objetos: se detectaron datos de objeto inesperados en el almacén de objetos.	"SVRU: verificación de almacén de objetos desconocida"
SYSD	Parada del nodo: se solicitó un apagado.	"SYSD: Parada de nodo"
SYST	Parada del nodo: un servicio inició una parada controlada.	"SYST: parada del nodo"
SYSU	Inicio del nodo: se ha iniciado un servicio; en el mensaje se indica el motivo del apagado anterior.	"SYSU: Inicio del nodo"

Mensajes de auditoría para eventos de almacén de objetos en StorageGRID

Los mensajes de auditoría pertenecientes a la categoría de auditoría de almacenamiento de objetos se utilizan para eventos relacionados con el almacenamiento y la gestión de objetos dentro del sistema StorageGRID. Estos incluyen el almacenamiento y la recuperación de objetos, las transferencias de nodo de grid a nodo de grid y las verificaciones.



Los códigos de auditoría se eliminan del producto y de la documentación a medida que las funciones quedan obsoletas. Si encuentras un código de auditoría que no aparece en esta lista, consulta las versiones anteriores de este tema para versiones anteriores de SG. Por ejemplo, "[Mensajes de auditoría del almacenamiento de objetos StorageGRID 11.8](#)".

Código	Descripción	Ver
BROR	Solicitud de solo lectura del bucket: un bucket entró o salió del modo de solo lectura.	"BROR: Solicitud de solo lectura de bucket"
CBSE	Fin del envío del objeto: la entidad de origen completó una operación de transferencia de datos de un nodo de la red a otro.	"CBSE: Fin del envío del objeto"
CBRE	Extremo receptor del objeto: la entidad de destino completó una operación de transferencia de datos de nodo de grid a nodo de grid.	"CBRE: Fin de recepción de objeto"
CGRR	Solicitud de replicación entre grids: StorageGRID intentó realizar una operación de replicación entre grids para replicar objetos entre buckets en una conexión de federación de grids.	"CGRR: Solicitud de replicación entre grids"
EBDL	Eliminación de bucket vacío: El escáner de ILM eliminó un objeto en un bucket que está eliminando todos los objetos (realizando una operación de vaciado de bucket).	"EBDL: Eliminación de cubos vacíos"
EBKR	Solicitud de Empty Bucket: un usuario envió una solicitud para activar o desactivar Empty Bucket (es decir, para eliminar los objetos del bucket o para dejar de eliminarlos).	"EBKR: Solicitud de cubo vacío"
SCMT	Confirmación del almacén de objetos: un bloque de contenido se almacenó y verificó por completo, y ahora puede solicitarse.	"SCMT: Solicitud de confirmación del almacén de objetos"
SREM	Eliminación del almacén de objetos: se eliminó un bloque de contenido de un nodo de la cuadrícula y ya no se puede solicitar directamente.	"SREM: Eliminación del Object Store"

Mensajes de auditoría para operaciones de lectura de cliente en StorageGRID

Los mensajes de auditoría de lectura del cliente se registran cuando una aplicación cliente de S3 hace una solicitud para recuperar un objeto.

Código	Descripción	Utilizado por	Ver
S3SL	Solicitud S3 Select: Registra una finalización después de que una solicitud S3 Select ha sido devuelta al cliente. El mensaje S3SL puede incluir detalles del mensaje de error y del código de error. Es posible que la solicitud no haya sido exitosa.	Cliente S3	"S3SL: solicitud S3 Select"
SGET	S3 GET: Registra una transacción realizada con éxito para recuperar un objeto o mostrar la lista de objetos en un bucket. Nota: Si la transacción se realiza sobre un subrecurso, el mensaje de auditoría incluirá el campo S3SR.	Cliente S3	"SGET: S3 GET"
SHEA	S3 HEAD: Registra una transacción exitosa para comprobar la existencia de un objeto o bucket.	Cliente S3	"SHEA: S3 HEAD"

Mensajes de auditoría para operaciones de escritura de clientes en StorageGRID

Los mensajes de auditoría de escritura del cliente se registran cuando una aplicación cliente de S3 realiza una solicitud para crear o modificar un objeto.

Código	Descripción	Utilizado por	Ver
OVWR	Sobrescritura de objeto: registra una transacción para sobrescribir un objeto con otro objeto.	Cliente S3	"OVWR: Sobrescritura de objeto"
SDEL	S3 DELETE: Registra una transacción realizada con éxito para eliminar un objeto o un bucket. Nota: Si la transacción se realiza sobre un subrecurso, el mensaje de auditoría incluirá el campo S3SR.	Cliente S3	"SDEL: S3 DELETE"
SPOS	S3 POST: Registra una transacción realizada con éxito para restaurar un objeto desde el almacenamiento de AWS Glacier a un Cloud Storage Pool.	Cliente S3	"SPOS: S3 POST"
SPUT	S3 PUT: Registra una transacción realizada con éxito para crear un nuevo objeto o bucket. Nota: Si la transacción se realiza sobre un subrecurso, el mensaje de auditoría incluirá el campo S3SR.	Cliente S3	"SPUT: S3 PUT"

Código	Descripción	Utilizado por	Ver
SUPD	Metadatos de S3 actualizados: registra una transacción exitosa para actualizar los metadatos de un objeto o bucket existente.	Cliente S3	"SUPD: Metadatos de S3 actualizados"

Mensajes de auditoría de gestión de StorageGRID

La categoría Management registra las solicitudes de usuario a la API de Management.

Código	Título y descripción del mensaje	Ver
MGAU	Mensaje de auditoría de la API de gestión: un registro de solicitudes de usuario.	"MGAU: Mensaje de auditoría de gestión"

Mensajes de auditoría de StorageGRID ILM

Los mensajes de auditoría pertenecientes 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 tal y como especifican las reglas de ILM.	"ORLM: reglas del objeto cumplidas"

Referencia del mensaje de auditoría

Mensaje de auditoría BROR para solicitudes de solo lectura de bucket en StorageGRID

El servicio LDR genera este mensaje de auditoría cuando un bucket entra o sale del modo de solo lectura. Por ejemplo, un bucket entra en modo de solo lectura mientras se eliminan todos los objetos.

Código	Campo	Descripción
BKHD	UUID del depósito	El identificador del bucket.

Código	Campo	Descripción
BROV	Valor de la solicitud de solo lectura del bucket	Si el bucket se está configurando como de solo lectura o si está dejando de estar en ese estado (1 = solo lectura, 0 = no solo lectura).
BROS	Motivo de solo lectura del bucket	El motivo por el que el bucket pasa a ser de solo lectura o sale del estado de solo lectura. Por ejemplo, emptyBucket.
S3AI	ID de cuenta de inquilino de S3	El ID de la cuenta de inquilino que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Bucket de S3	El nombre del depósito de S3.

Mensaje de auditoría CBRB para el inicio de la recepción de objeto en StorageGRID

Durante el funcionamiento normal del sistema, los bloques de contenido se transfieren continuamente entre los distintos 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 entre nodos.
CBID	Identificador del bloque de contenido	El identificador único del bloque de contenido que se está transfiriendo.
CTDR	Sentido de la transferencia	Indica si la transferencia CBID se inició mediante push o mediante pull: 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 identificador de nodo del origen (remitente) de la transferencia CBID.
CTDS	Entidad de destino	El identificador de nodo del destino (receptor) de la transferencia CBID.
CTSS	Recuento de secuencia de inicio	Indica el primer número de secuencia solicitado. Si la operación se realiza correctamente, la transferencia comienza a partir de este número de secuencia.

Código	Campo	Descripción
CTES	Conteo esperado de secuencias finales	Indica el último recuento de secuencia solicitado. Si la operación se realiza con éxito, la transferencia se considera completa cuando se ha recibido este recuento de secuencia.
RSLT	Estado de inicio de la transferencia	Estado en el momento en que se inició la transferencia: SUCS: La transferencia se inició correctamente.

Este mensaje de auditoría indica que se ha iniciado una operación de transferencia de datos de nodo a nodo sobre un único elemento de contenido, identificado mediante su Content Block Identifier. La operación solicita datos desde "Start Sequence Count" hasta "Expected End Sequence Count". Los nodos emisores y receptores se identifican mediante sus ID de nodo. Esta información puede utilizarse para realizar un seguimiento del flujo de datos del sistema y, cuando se combina con mensajes de auditoría de almacenamiento, para verificar el recuento de réplicas.

Mensaje de auditoría CBRE para el extremo de recepción de objetos en StorageGRID

Cuando finaliza 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 entre nodos.
CBID	Identificador del bloque de contenido	El identificador único del bloque de contenido que se está transfiriendo.
CTDR	Sentido de la transferencia	Indica si la transferencia CBID se inició mediante push o mediante pull: 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 identificador de nodo del origen (remitente) de la transferencia CBID.
CTDS	Entidad de destino	El identificador de nodo del destino (receptor) de la transferencia CBID.
CTSS	Recuento de secuencia de inicio	Indica el número de secuencia en el que se inició la transferencia.

Código	Campo	Descripción
CTAS	Recuento real de secuencias finales	Indica el último recuento de secuencias transferido correctamente. Si el recuento real de secuencias finales es igual al recuento de secuencias iniciales y el resultado de la transferencia no fue exitoso, no se intercambió ningún dato.
RSLT	Resultado de la transferencia	El resultado de la operación de transferencia (desde el punto de vista de la entidad remitente): SUCS: transferencia completada con éxito; se enviaron todos los recuentos de secuencias solicitados. CONL: conexión perdida durante la transferencia CTMO: tiempo de espera de conexión agotado durante el establecimiento o la transferencia UNRE: no se puede acceder al ID del nodo de destino CRPT: la transferencia terminó debido a la recepción de datos corruptos o no válidos

Este mensaje de auditoría indica que se ha completado una operación de transferencia de datos de nodo a nodo. Si el resultado de la transferencia fue satisfactorio, la operación transfirió datos desde "Start Sequence Count" hasta "Actual End Sequence Count". Los nodos emisor y receptor se identifican por sus ID de nodo. Esta información puede usarse 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 puede usarse para verificar el recuento de réplicas.

Mensaje de auditoría CBSB para el inicio del envío de objetos en StorageGRID

Durante el funcionamiento normal del sistema, los bloques de contenido se transfieren continuamente entre los distintos 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 entre nodos.
CBID	Identificador del bloque de contenido	El identificador único del bloque de contenido que se está transfiriendo.

Código	Campo	Descripción
CTDR	Sentido de la transferencia	Indica si la transferencia CBID se inició mediante push o mediante pull: 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 identificador de nodo del origen (remitente) de la transferencia CBID.
CTDS	Entidad de destino	El identificador de nodo del destino (receptor) de la transferencia CBID.
CTSS	Recuento de secuencia de inicio	Indica el primer número de secuencia solicitado. Si la operación se realiza correctamente, la transferencia comienza a partir de este número de secuencia.
CTES	Conteo esperado de secuencias finales	Indica el último recuento de secuencia solicitado. Si la operación se realiza con éxito, la transferencia se considera completa cuando se ha recibido este recuento de secuencia.
RSLT	Estado de inicio de la transferencia	Estado en el momento en que se inició la transferencia: SUCS: la transferencia se inició correctamente.

Este mensaje de auditoría indica que se ha iniciado una operación de transferencia de datos de nodo a nodo sobre un único elemento de contenido, identificado mediante su Content Block Identifier. La operación solicita datos desde "Start Sequence Count" hasta "Expected End Sequence Count". Los nodos emisores y receptores se identifican mediante sus ID de nodo. Esta información puede utilizarse para realizar un seguimiento del flujo de datos del sistema y, cuando se combina con mensajes de auditoría de almacenamiento, para verificar el recuento de réplicas.

Mensaje de auditoría CBSE para el fin del envío de objeto en StorageGRID

Cuando finaliza 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 entre nodos.
CBID	Identificador del bloque de contenido	El identificador único del bloque de contenido que se está transfiriendo.

Código	Campo	Descripción
CTDR	Sentido de la transferencia	Indica si la transferencia CBID se inició mediante push o mediante pull: 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 identificador de nodo del origen (remitente) de la transferencia CBID.
CTDS	Entidad de destino	El identificador de nodo del destino (receptor) de la transferencia CBID.
CTSS	Recuento de secuencia de inicio	Indica el número de secuencia en el que se inició la transferencia.
CTAS	Recuento real de secuencias finales	Indica el último recuento de secuencias transferido correctamente. Si el recuento real de secuencias finales es igual al recuento de secuencias iniciales y el resultado de la transferencia no fue exitoso, no se intercambió ningún dato.
RSLT	Resultado de la transferencia	El resultado de la operación de transferencia (desde el punto de vista de la entidad remitente): SUCS: Transferencia completada con éxito; se enviaron todos los recuentos de secuencias solicitados. CONL: conexión perdida durante la transferencia CTMO: tiempo de espera de conexión agotado durante el establecimiento o la transferencia UNRE: no se puede acceder al ID del nodo de destino CRPT: la transferencia terminó debido a la recepción de datos corruptos o no válidos

Este mensaje de auditoría indica que se ha completado una operación de transferencia de datos de nodo a nodo. Si el resultado de la transferencia fue satisfactorio, la operación transfirió datos desde "Start Sequence Count" hasta "Actual End Sequence Count". Los nodos emisor y receptor se identifican por sus ID de nodo. Esta información puede usarse 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 puede usarse para verificar el recuento de réplicas.

Mensaje de auditoría CGRR para solicitudes de replicación entre grids en StorageGRID

Este mensaje se genera cuando StorageGRID intenta realizar una operación de replicación entre grids para replicar objetos entre buckets en una conexión de federación

de grids.

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 grids que abarquen una actualización de StorageGRID 11.7 a 11.8 podrían tener un tamaño total de objeto inexacto.
S3AI	ID de cuenta de inquilino de S3	El ID de la cuenta de inquilino que es propietaria del bucket desde el que se está replicando el objeto.
GFID	ID de conexión de la federación de grid	El identificador de la conexión de la federación de grid que se utiliza para la replicación entre grids.
OPER	Operación de CGR	El tipo de operación de replicación entre grids que se intentó realizar: • 0 = Replicar objeto • 1 = Replicar objeto multiparte • 2 = Replicar marcador de eliminación
S3BK	Bucket de S3	El nombre del depósito de S3.
S3KY	Clave de S3	El nombre de la clave S3, sin incluir el nombre del bucket.
VSID	ID de versión	El identificador de la versión concreta de un objeto que se estaba replicando.
RSLT	Código de resultado	Devuelve éxito (SUCS) o error general (GERR).

Mensaje de auditoría EBDL para eliminaciones de objetos de bucket vacíos en StorageGRID

El escáner de ILM eliminó un objeto de un bucket que está eliminando todos los objetos (realizando una operación de vaciado de bucket).

Código	Campo	Descripción
CSIZ	Tamaño del objeto	El tamaño del objeto en bytes.
RUTA	Depósito/clave de S3	El nombre del bucket de S3 y el nombre de la clave de S3.

Código	Campo	Descripción
SEGC	UUID del contenedor	UUID del contenedor para el objeto segmentado. Este valor solo está disponible si el objeto está segmentado.
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.

Mensaje de auditoría EBKR para solicitudes de bucket vacíos en StorageGRID

Este mensaje indica que un usuario envió una solicitud para activar o desactivar el bucket vacío (es decir, para eliminar los objetos del bucket o para dejar de eliminarlos).

Código	Campo	Descripción
BUID	UUID del depósito	El identificador del bucket.
EBJS	Configuración JSON de Empty Bucket	Contiene el JSON que representa la configuración actual de Empty Bucket.
S3AI	ID de cuenta de inquilino de S3	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Bucket de S3	El nombre del depósito de S3.

Mensaje de auditoría ECMC por datos con código de borrado faltantes en StorageGRID

Este mensaje de auditoría indica que el sistema ha detectado un fragmento de datos con código de borrado que falta.

Código	Campo	Descripción
VCMC	ID de VCS	El nombre del VCS que contiene el fragmento que falta.
MCID	ID del fragmento	El identificador del fragmento con código de borrado que falta.
RSLT	Resultado	Este campo tiene el valor «NONE». RSLT es un campo obligatorio del mensaje, pero no es relevante para este mensaje en concreto. Se utiliza «NONE» en lugar de «SUCS» para que este mensaje no sea filtrado.

Mensaje de auditoría ECOC para datos con código de borrado corruptos en StorageGRID

Este mensaje de auditoría indica que el sistema ha detectado un fragmento de datos con código de borrado dañado.

Código	Campo	Descripción
VCCO	ID de VCS	El nombre del VCS que contiene el fragmento dañado.
VLID	ID de volumen	El volumen de RangeDB que contiene el fragmento con código de borrado dañado.
CCID	ID del fragmento	El identificador del fragmento con código de borrado dañado.
RSLT	Resultado	Este campo tiene el valor «NONE». RSLT es un campo obligatorio del mensaje, pero no es relevante para este mensaje en concreto. Se utiliza «NONE» en lugar de «SUCS» para que este mensaje no sea filtrado.

Mensaje de auditoría ETAF para fallos de autenticación de seguridad en StorageGRID

Este mensaje se genera cuando falla un intento de conexión usando Transport Layer Security (TLS).

Código	Campo	Descripción
CNID	Identificador de conexión	El identificador único del sistema para la conexión TCP/IP en la que falló la autenticación.
RUID	Identidad del usuario	Un identificador dependiente del servicio que representa la identidad del usuario remoto.

Código	Campo	Descripción
RSLT	Código de motivo	La causa del fallo: SCNI: No se ha podido establecer una conexión segura. CERM: faltaba el certificado. CERT: El certificado no era válido. CERE: el certificado había caducado. CERR: Se revocó el certificado. CSGN: la firma del certificado no era válida. CSGU: el firmante del certificado era desconocido. UCRM: Faltaban las 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 espera de la autenticación.

Cuando se establece una conexión con un servicio seguro que utiliza TLS, las credenciales de la entidad remota se verifican mediante el perfil TLS y la lógica adicional integrada en el servicio. Si 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 autorizados y otros problemas de conexión relacionados con la seguridad.

El mensaje podría deberse a que una entidad remota tiene una configuración incorrecta o a intentos de presentar credenciales no válidas o no permitidas al sistema. Debes supervisar este mensaje de auditoría para detectar intentos de obtener acceso no autorizado al sistema.

Mensaje de auditoría GNRG para el registro GNDS en StorageGRID

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 fallo
GNID	Nodo ID	El identificador de nodo del servicio que inició la solicitud de actualización.

Código	Campo	Descripción
GNTTP	Tipo de dispositivo	El tipo de dispositivo del nodo de la grid (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 grid en el paquete DMDL.
GNGP	Grupo	El grupo al que pertenece el nodo de la red (en el contexto de los costes de enlace y la clasificación de las consultas de servicio).
GNIA	Dirección IP	La dirección IP del nodo de la grid.

Este mensaje se genera cada vez que un nodo de grid actualiza su entrada en el Grid Nodes Bundle.

Mensaje de auditoría GNUR para la baja de GNDS en StorageGRID

El servicio CMN genera este mensaje de auditoría cuando un servicio ha dado de baja información sobre sí mismo del sistema StorageGRID.

Código	Campo	Descripción
RSLT	Resultado	El resultado de la solicitud de actualización: • SUCS: Exitoso • SUNV: Servicio no disponible • GERR: Otro fallo
GNID	Nodo ID	El identificador de nodo del servicio que inició la solicitud de actualización.

Mensaje de auditoría GTED para tareas de grid finalizadas en StorageGRID

Este mensaje de auditoría indica que el servicio CMN ha finalizado el procesamiento de la tarea de grid especificada y la ha trasladado a la tabla Historical. Si el resultado es SUCS, ABRT o ROLF, habrá un mensaje de auditoría correspondiente de Grid Task Started. Los demás resultados indican que el procesamiento de esta tarea de grid nunca se inició.

Código	Campo	Descripción
TSID	ID de la tarea	Este campo identifica de forma única una tarea de grid generada y permite gestionar dicha tarea a lo largo de su ciclo de vida. Nota: el ID de tarea se asigna en el momento en que se genera una tarea de grid, no en el momento en que se envía. Es posible que una tarea de grid 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 Submitted, Started y Ended.
RSLT	Resultado	Resultado final del estado de la tarea de la grid: • SUCS: La tarea de la red se completó con éxito. • ABRT: La tarea de la grid se terminó sin un error de reversión. • ROLF: La tarea de grid se interrumpió y no pudo completar el proceso de reversión. • CANC: El usuario canceló la tarea de la cuadrícula antes de que se iniciara. • EXPR: La tarea de grid expiró antes de que se iniciara. • IVLD: La tarea de la cuadrícula no es válida. • AUTH: la tarea de la red no estaba autorizada. • DUPL: La tarea de la cuadrícula fue rechazada por ser un duplicado.

Mensaje de auditoría GTST para tareas grid iniciadas en StorageGRID

Este mensaje de auditoría indica que el servicio CMN ha comenzado a procesar la tarea de grid especificada. El mensaje de auditoría sigue inmediatamente al mensaje Grid Task Submitted para las tareas de grid iniciadas por el servicio interno Grid Task Submission y seleccionadas para su activación automática. Para las tareas de grid enviadas a la tabla Pending, este mensaje se genera cuando inicias la tarea de grid.

Código	Campo	Descripción
TSID	ID de la tarea	Este campo identifica de forma única una tarea de grid generada y permite gestionar dicha tarea a lo largo de su ciclo de vida. Nota: el ID de tarea se asigna en el momento en que se genera una tarea de grid, no en el momento en que se envía. Es posible que una tarea de grid 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 Submitted, Started y Ended.
RSLT	Resultado	El resultado. Este campo solo tiene un valor: • SUCS: La tarea de la grid se inició correctamente.

Este mensaje de auditoría indica que se ha enviado una tarea de grid al servicio CMN.

Código	Campo	Descripción
TSID	ID de la tarea	Identifica de forma única una tarea de grid generada y permite gestionar dicha tarea a lo largo de su ciclo de vida. Nota: el ID de tarea se asigna en el momento en que se genera una tarea de grid, no en el momento en que se envía. Es posible que una tarea de grid 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 Submitted, Started y Ended.
TTYP	Tipo de tarea	El tipo de tarea de grid.
TVER	Versión de la tarea	Un número que indica la versión de la tarea de grid.
TDSC	Descripción de la tarea	Una descripción legible para humanos de la tarea de grid.
VATS	Válido después de la marca de tiempo	El momento más temprano (en microsegundos UINT64 desde el 1 de enero de 1970 - tiempo UNIX) en el que la tarea de grid es válida.
VBTS	Válido antes de la marca de tiempo	La hora más reciente (en microsegundos UINT64 desde el 1 de enero de 1970 - tiempo UNIX) en la que la tarea de grid es válida.
TSRC	Fuente	El origen de la tarea: • TXTB: La tarea de la grid se envió a través del sistema StorageGRID como un bloque de texto firmado. • GRID: La tarea de grid se envió a través del servicio interno de envío de tareas de grid.
ACTV	Tipo de activación	El tipo de activación: • AUTO: La tarea de grid se envió para activación automática. • PEND: la tarea del grid se envió a la tabla de pendientes. Esta es la única posibilidad para el origen de TXTB.
RSLT	Resultado	El resultado del envío: • SUCS: La tarea de la grid 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 buckets S3 que cumplen los requisitos:** Este mensaje se genera cuando ILM inicia el proceso de eliminación automática de un objeto porque ha vencido su periodo de retención (suponiendo que la configuración de eliminación automática esté activada y la retención legal esté desactivada).
- **Para objetos en buckets de S3 no conformes.** Este mensaje se genera cuando ILM inicia el proceso de eliminación de un objeto porque actualmente no se aplica ninguna instrucción de ubicación de las políticas de ILM activas al objeto.

Código	Campo	Descripción
CBID	Identificador del bloque de contenido	El CBID del objeto.
CMPA	Cumplimiento: eliminación automática	Solo para objetos en buckets S3 conformes. 0 (falso) o 1 (verdadero), que indica si un objeto conforme debe eliminarse automáticamente cuando termine su período de retención, a menos que el bucket esté bajo una retención legal.
CMPL	Cumplimiento normativo: retención legal	Solo para objetos en buckets de S3 conformes. 0 (falso) o 1 (verdadero), que indica si el bucket está actualmente bajo una retención legal.
CMPR	Cumplimiento normativo: plazo de conservación	Solo para objetos en buckets S3 conformes. La duración del período de retención del objeto en minutos.
CTME	Cumplimiento: tiempo de ingesta	Solo para objetos en buckets S3 compatibles. La hora de incorporación del objeto. Puedes sumar a este valor el periodo de retención en minutos para determinar cuándo se puede eliminar el objeto del bucket.
DMRK	Eliminar identificador de versión del marcador de eliminación	El identificador de versión del marcador de eliminación creado al eliminar un objeto de un bucket con control de versiones. Las operaciones en los buckets 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 del objeto dentro del sistema StorageGRID. El valor de LOCS es "" si el objeto no tiene ubicaciones (por ejemplo, si se ha eliminado). CLEC: en el caso de los objetos con código de borrado, el identificador del perfil de código de borrado y el identificador del grupo de código de borrado que se aplican a los datos del objeto. CLDI: para los 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.
RUTA	Depósito/clave de S3	El nombre del bucket de S3 y el nombre de la clave de S3.
RSLT	Resultado	El resultado de la operación ILM. SUCS: La operación de ILM se realizó correctamente.
NORMA	Etiqueta de reglas	• Si un objeto de un depósito S3 conforme se está eliminando automáticamente porque ha vencido su periodo de retención, este campo está en blanco. • Si el objeto se está eliminando porque ya no hay instrucciones de ubicación que se apliquen actualmente al objeto, este campo muestra la etiqueta legible para el usuario de la última regla de ILM que se aplicó al objeto.
SGRP	Sitio (Grupo)	Si existía, 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 versión de la versión específica de un objeto que se eliminó. Las operaciones en buckets y objetos en buckets sin versiones no incluyen este campo.

Mensaje de auditoría LKCU para la limpieza de objetos sobrescritos en StorageGRID

Este mensaje se genera cuando StorageGRID elimina un objeto sobrescrito que antes requería una limpieza para liberar espacio de almacenamiento. Un objeto se sobrescribe cuando un cliente S3 escribe un objeto en una ruta que ya contiene un objeto. El proceso de eliminación se realiza 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>Solo para uso interno.</i>
LUID	UUID del objeto eliminado	El identificador del objeto que se eliminó.
UTA	Depósito/clave de S3	El nombre del bucket de S3 y el nombre de la clave de S3.
SEGC	UUID del contenedor	UUID del contenedor para el objeto segmentado. Este valor solo está disponible si el objeto está segmentado.
UUID	Identificador único universal	El identificador del objeto que aún existe. Este valor solo está disponible si el objeto no se ha eliminado.

Mensaje de auditoría LKDM para limpieza de objetos filtrados en StorageGRID

Este mensaje se genera cuando se ha limpiado o eliminado un fragmento filtrado. Un fragmento puede formar parte de un objeto replicado o de un objeto codificado mediante borrado.

Código	Campo	Descripción
CLOC	Ubicación del fragmento	La ruta del archivo del fragmento filtrado que se eliminó.
CTYP	Tipo de fragmento	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	Hora de creación del fragmento	Hora en la que se creó el fragmento filtrado.
UUID	Identificador único universal	El identificador del objeto al que pertenece el fragmento.
CBID	Identificador del bloque de contenido	CBID del objeto al que pertenece el fragmento filtrado.
CSIZ	Tamaño del contenido	El tamaño del fragmento en bytes.

Mensaje de auditoría LLST para ubicaciones de copias de objetos perdidas en StorageGRID

Este mensaje se genera cada vez que no se encuentra una ubicación para una copia de un objeto (replicada o con código de borrado).

Código	Campo	Descripción
CBIL	CBID	El CBID afectado.
ECPR	Perfil de código de borrado	Para datos de objetos con codificación de 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 con código de 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 en el disco de los datos del objeto perdido. Solo se devuelve cuando LTyp tiene el valor CLDI (es decir, para objetos replicados). Adopta la forma <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@</code>
RSLT	Resultado	Siempre es NONE. 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 desencadenante	USUARIO: Activado por el usuario SYST: activado por el sistema
UUID	Identificador único universal	El identificador del objeto afectado en el sistema StorageGRID.

Mensaje de auditoría MGAU para solicitudes de la API de gestión en StorageGRID

La categoría Management registra las solicitudes de usuario a la API de Management. 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).
MDNA	Nombre de dominio	El nombre de dominio del host.
MPAT	PATH de solicitud	La ruta de la solicitud.

Código	Campo	Descripción
MPQP	Parámetros de consulta de la solicitud	Los parámetros de consulta de la solicitud.
MRBD	Cuerpo de la solicitud	El contenido del cuerpo de la solicitud. Aunque el cuerpo de la respuesta se registra de forma predeterminada, el cuerpo de la solicitud se registra en determinados casos cuando el cuerpo de la respuesta está vacío. Dado que la siguiente información no está disponible en el cuerpo de la respuesta, se obtiene del cuerpo de la solicitud para los siguientes métodos POST: • Nombre de usuario e ID de cuenta en POST authorize • Nueva configuración de subredes en POST /grid/grid-networks/update • Nuevos servidores NTP en POST /grid/ntp-servers/update • Identificadores de servidores decomisionados en POST /grid/servers/decommission Nota: La información confidencial se elimina (por ejemplo, una clave de acceso a S3) o se oculta con asteriscos (por ejemplo, una contraseña).
MRMD	Método de solicitud	El método de solicitud HTTP: • POST • PUT • ELIMINAR • PATCH
MRSC	Código de respuesta	El código de respuesta.
MRSP	Cuerpo de respuesta	El contenido de la respuesta (el cuerpo de la respuesta) se registra de forma predeterminada. Nota: La información confidencial se elimina (por ejemplo, una clave de acceso a S3) o se oculta con asteriscos (por ejemplo, una contraseña).
MSIP	Dirección IP de origen	La dirección IP del cliente (origen).
MUUN	URN del usuario	El URN (nombre uniforme de recurso) del usuario que envió la solicitud.
RSLT	Resultado	Devuelve «Éxito» (SUCS) o el error informado por el backend.

Mensaje de auditoría OLST para objetos detectados como perdidos por el sistema en StorageGRID

Este mensaje se genera cuando el servicio DDS no puede localizar ninguna copia de un objeto dentro del sistema StorageGRID.

Código	Campo	Descripción
CBID	Identificador del bloque de contenido	El CBID del objeto perdido.
NOID	Nodo ID	Si se dispone de ella, la última ubicación conocida, directa o near-line, del objeto perdido. Es posible disponer únicamente del Node ID sin un Volume ID si no se dispone de la información del volumen.
UTA	Depósito/clave de S3	Si están disponibles, el nombre del bucket de S3 y el nombre de la clave de S3.
RSLT	Resultado	Este campo tiene el valor NONE. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. Se usa NONE en lugar de SUCS para que este mensaje no se filtre.
UUID	Identificador único universal	El identificador del objeto perdido dentro del sistema StorageGRID.
VOLI	ID de volumen	Si está disponible, el ID de volumen del Storage Node para la última ubicación conocida del objeto perdido.

Mensaje de auditoría ORLM para reglas ILM cumplidas en StorageGRID

Este mensaje se genera cuando el objeto se almacena y se copia correctamente según lo especifican las reglas de ILM.



El mensaje ORLM no se genera cuando un objeto se almacena correctamente mediante la regla predeterminada «Make 2 Copies» si otra regla de la política utiliza el filtro avanzado «Object Size».

Código	Campo	Descripción
BUID	Encabezado de bucket	Campo «Bucket ID». Se usa para operaciones internas. Solo aparece si STAT es PRGD.
CBID	Identificador del 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 del objeto dentro del sistema StorageGRID. El valor de LOCS es "" si el objeto no tiene ubicaciones (por ejemplo, si se ha eliminado). CLEC: en el caso de los objetos con código de borrado, el identificador del perfil de código de borrado y el identificador del grupo de código de borrado que se aplican a los datos del objeto. CLDI: para los 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.
RUTA	Depósito/clave de S3	El nombre del bucket de S3 y el nombre de la clave de S3.
RSLT	Resultado	El resultado de la operación ILM. SUCS: La operación de ILM se realizó correctamente.
NORMA	Etiqueta de reglas	La etiqueta legible por el usuario asignada a la regla ILM aplicada a este objeto.
SEGC	UUID del contenedor	UUID del contenedor para el objeto segmentado. Este valor solo está disponible si el objeto está segmentado.
SGCB	CBID del contenedor	CBID del contenedor para el objeto segmentado. Este valor solo está disponible para objetos segmentados y multiparte.
ESTADÍSTICAS	Estado	El estado de la operación de ILM. HECHO: Las operaciones de ILM sobre el objeto han finalizado. DFER: El objeto se ha marcado para una futura reevaluación de ILM. PRGD: El objeto se ha eliminado del sistema StorageGRID. NLOC: Ya no se pueden encontrar los datos de los objetos en el sistema StorageGRID. Este estado podría indicar que todas las copias de los datos de los objetos faltan o están dañadas.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
VSID	ID de versión	El ID de versión de un nuevo objeto creado en un bucket con control de versiones. Las operaciones en buckets y objetos en buckets sin control de versiones no incluyen este campo.

El mensaje de auditoría ORLM se puede emitir más de una vez para un solo objeto. Por ejemplo, se emite cada vez que ocurre uno de los siguientes eventos:

- Las reglas de ILM para el objeto se cumplen para siempre.
- Se cumplen las reglas de ILM para el objeto en esta época.
- Las reglas de ILM han eliminado el objeto.
- El proceso de verificación en segundo plano detecta que una copia de los datos de un objeto replicado está dañada. El sistema StorageGRID realiza una evaluación ILM para reemplazar el objeto dañado.

Información relacionada

- ["Transacciones de incorporación de objetos"](#)
- ["Transacciones de eliminación de objetos"](#)

Mensaje de auditoría OVWR para sobrescrituras de objetos en StorageGRID

Este mensaje se genera cuando una operación externa (solicitada por el cliente) provoca que un objeto sea sobrescrito por otro objeto.

Código	Campo	Descripción
CBID	Identificador de bloque de contenido (nuevo)	El CBID del nuevo objeto.
CSIZ	Tamaño del objeto anterior	El tamaño, en bytes, del objeto que se va a sobrescribir.
OCBD	Identificador del bloque de contenido (anterior)	El CBID del objeto anterior.
UUID	Identificador único universal (nuevo)	El identificador del nuevo objeto dentro del sistema StorageGRID.
UUID	Identificador único universal (anterior)	El identificador del objeto anterior dentro del sistema StorageGRID.
RUTA	Ruta del objeto en S3	La ruta del objeto S3 utilizada tanto para el objeto anterior como para el nuevo
RSLT	Código de resultado	Resultado de la transacción «Sobrescribir objeto». El resultado es siempre: SUCS: Exitoso

Código	Campo	Descripción
SGRP	Sitio (Grupo)	Si existía, el objeto sobrescrito se eliminó en el sitio especificado, que no es el sitio donde se ingirió el objeto sobrescrito.

Mensaje de auditoría S3SL para solicitudes S3 Select en StorageGRID

Este mensaje registra la finalización después de que se haya devuelto una solicitud de 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 se haya realizado correctamente.

Código	Campo	Descripción
BYSC	Bytes escaneados	Número de bytes analizados (recibidos) de los Storage Nodes. Es probable que BYSC y BYPR sean diferentes si el objeto está comprimido. Si el objeto está comprimido, BYSC tendría el recuento de bytes comprimidos y BYPR serían los bytes después de la descompresión.
BYPR	Bytes procesados	Número de bytes procesados. Indica cuántos bytes de "Bytes Scanned" se procesaron realmente o sobre los que actuó un trabajo de 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 de S3 Select ha recibido de los Storage Nodes.
RERT	Registros devueltos	Número de registros o filas que un trabajo de S3 Select devolvió al cliente.
JOFI	Trabajo finalizado	Indica si el trabajo de S3 Select terminó de procesarse o no. Si esto es falso, significa que el trabajo no pudo finalizar y es probable que los campos de error tengan datos. Es posible que el cliente haya recibido resultados parciales o que no haya recibido ningún resultado.
REID	ID de solicitud	Identificador de la solicitud S3 Select.
EXTM	Tiempo de ejecución	El tiempo, en segundos, que tardó en completarse el trabajo S3 Select.
ERMG	Mensaje de error	Mensaje de error que generó el trabajo S3 Select.
ERTY	Tipo de error	Tipo de error que generó el trabajo S3 Select.
ERST	Traza de error	Traza de pila de error que generó el trabajo S3 Select.
S3BK	Bucket de S3	El nombre del depósito de S3.

Código	Campo	Descripción
S3AK	ID de la clave de acceso de S3 (remitente de la solicitud)	El ID de la clave de acceso S3 del usuario que envió la solicitud.
S3AI	ID de la cuenta de inquilino de S3 (remitente de la solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud.
S3KY	Clave de S3	El nombre de la clave S3, sin incluir el nombre del bucket.

Mensaje de auditoría SADD para desactivar la auditoría de seguridad en StorageGRID

Este mensaje indica que el servicio de origen (ID de nodo) ha desactivado el registro de mensajes de auditoría. StorageGRID ya no recopila ni envía mensajes de auditoría.

Código	Campo	Descripción
AETM	Activar método	El método utilizado para desactivar la auditoría.
AEUN	Nombre de usuario	El nombre de usuario que ejecutó el comando para desactivar el registro de auditoría.
RSLT	Resultado	Este campo tiene el valor NONE. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. Se usa NONE en lugar de SUCS para que este mensaje no se filtre.

El mensaje da a entender que el registro estaba habilitado previamente, pero ahora se ha deshabilitado. Esto se suele utilizar solo durante la ingesta masiva para mejorar el rendimiento del sistema. Tras la actividad masiva, se restaura la auditoría (SADE) y la capacidad de deshabilitar la auditoría se bloquea de forma permanente.

Mensaje de auditoría SADE para habilitar la auditoría de seguridad en StorageGRID

Este mensaje indica que el servicio de origen (ID de nodo) ha restablecido el registro de mensajes de auditoría. StorageGRID vuelve a recopilar y enviar mensajes de auditoría.

Código	Campo	Descripción
AETM	Activar método	El método utilizado para habilitar la auditoría.
AEUN	Nombre de usuario	El nombre de usuario que ejecutó el comando para habilitar el registro de auditoría.

Código	Campo	Descripción
RSLT	Resultado	Este campo tiene el valor NONE. RSLT es un campo de mensaje obligatorio, pero no es relevante para este mensaje. Se usa NONE en lugar de SUCS para que este mensaje no se filtre.

El mensaje da a entender que el registro estaba desactivado anteriormente (SADD), pero que ahora se ha restablecido. Por lo general, esto solo se utiliza durante la importación masiva para mejorar el rendimiento del sistema. Una vez finalizada la actividad masiva, se restablece la auditoría y la posibilidad de desactivarla queda bloqueada de forma permanente.

Mensaje de auditoría SCMT para commits de almacén de objetos en StorageGRID

El contenido de la grid no está disponible 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 por completo en el disco y ha superado las comprobaciones de integridad correspondientes. Este mensaje se emite cuando un bloque de contenido se confirma en el almacenamiento.

Código	Campo	Descripción
CBID	Identificador del bloque de contenido	El identificador único del bloque de contenido confirmado en el almacenamiento permanente.
RSLT	Código de resultado	Estado en el momento en que el objeto se guardó en el disco: SUCS: Objeto guardado correctamente.

Este mensaje indica que un bloque de contenido determinado se ha almacenado y verificado por completo, y que ya puede solicitarse. Se puede utilizar para realizar un seguimiento del flujo de datos dentro del sistema.

Mensaje de auditoría SDEL para transacciones S3 DELETE en StorageGRID

Cuando un cliente S3 emite una transacción DELETE, se realiza una solicitud para eliminar el objeto o bucket especificado, o para eliminar un subrecurso de bucket/objeto. El servidor emite este mensaje si la transacción se realiza correctamente.

Código	Campo	Descripción
CBID	Identificador del 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 los buckets no incluyen este campo.
CNCH	Encabezado de control de coherencia	El valor del encabezado de solicitud HTTP Consistency-Control, si está presente en la solicitud.

Código	Campo	Descripción
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 buckets no incluyen este campo.
DMRK	Eliminar identificador de versión del marcador de eliminación	El identificador de versión del marcador de eliminación creado al eliminar un objeto de un bucket con control de versiones. Las operaciones en los buckets no incluyen este campo.
GFID	ID de conexión de Grid Federation	El ID de conexión de la conexión de la federación de grid asociada a una solicitud de eliminación de replicación entre grids. Solo se incluye en los registros de auditoría en el grid de destino.
GFSA	ID de cuenta de origen de la federación de grid	El ID de cuenta del inquilino en la red de origen para una solicitud de eliminación mediante replicación entre grids. Solo se incluye en los registros de auditoría en la grid de destino.
HTRH	Encabezado de solicitud HTTP	Lista de los nombres y valores de los encabezados de las solicitudes 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 valor de <code>`X-Forwarded-For`</code> 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.
MTME	Hora de la última modificación	La marca de tiempo Unix, en microsegundos, que indica cuándo se modificó por última vez el objeto.
RSLT	Código de resultado	Resultado de la transacción DELETE. El resultado es siempre: SUCS: Exitoso
S3AI	ID de la cuenta de inquilino de S3 (remitente de la solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.

Código	Campo	Descripción
S3AK	ID de la clave de acceso de S3 (remitente de la solicitud)	El ID de la clave de acceso a S3 con hash del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Bucket de S3	El nombre del depósito de S3.
S3KY	Clave de S3	El nombre de la clave S3, sin incluir el nombre del bucket. Las operaciones en buckets no incluyen este campo.
S3SR	Subrecurso S3	El subrecurso bucket u objeto sobre el que se está realizando la operación, si aplica.
SACC	Nombre de la cuenta de 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 hizo la solicitud.
SBAC	Nombre de la cuenta de tenant de S3 (propietario del bucket)	El nombre de la cuenta de inquilino del propietario del bucket. Se usa para identificar el acceso entre cuentas o el acceso anónimo.
SBAI	ID de la cuenta de tenant de S3 (propietario del bucket)	El ID de la cuenta de inquilino del propietario del bucket de destino. Se utiliza para identificar el acceso entre cuentas o el acceso anónimo.
SGRP	Sitio (Grupo)	Si existía, el objeto se eliminó en el sitio especificado, que no es el sitio donde se ingirió el objeto.
SUSR	URN de usuario de S3 (remitente de la solicitud)	El ID de la cuenta del tenant y el nombre de usuario de la persona que realiza la solicitud. El usuario puede ser tanto un usuario local como un usuario LDAP. Por ejemplo: urn:sgws:identity::03393893651506583485:root Dejar en blanco para solicitudes anónimas.
HORA	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.

Código	Campo	Descripción
TLIP	Dirección IP de equilibrador de carga de confianza	Si la solicitud fue redirigida por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
UUDM	Identificador único universal para un marcador de eliminación	El identificador de un marcador de eliminación. Los mensajes de 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 versión de la versión específica de un objeto que se eliminó. Las operaciones en buckets y objetos en buckets sin versiones no incluyen este campo.

Mensaje de auditoría SGET para transacciones S3 GET en StorageGRID

Cuando un cliente S3 emite una transacción GET, se realiza una solicitud para recuperar un objeto, listar los objetos en un bucket o eliminar un subrecurso de bucket/objeto. Este mensaje lo emite el servidor si la transacción es exitosa.

Código	Campo	Descripción
CBID	Identificador del 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 los buckets no incluyen este campo.
CNCH	Encabezado de control de coherencia	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 con buckets no incluyen este campo.

Código	Campo	Descripción
HTRH	Encabezado de solicitud HTTP	Lista de los nombres y valores de los encabezados de las solicitudes HTTP registrados, según se seleccionaron durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si el valor de `X-Forwarded-For` es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP).
LITY	ListObjectsV2	Se ha solicitado una respuesta en <i>formato v2</i> . Para más información, consulta "AWS ListObjectsV2" . Solo para operaciones GET en el bucket.
NCHD	Número de hijos	Incluye claves y prefijos comunes. Solo para operaciones GET en el bucket.
RANG	Lectura de rango	Solo para operaciones de lectura de rango. Indica el rango de bytes que leyó esta solicitud. El valor después de la barra diagonal (/) muestra el tamaño de todo el objeto.
RSLT	Código de resultado	Resultado de la transacción GET. El resultado siempre es: SUCS: Exitoso
S3AI	ID de la cuenta de inquilino de S3 (remitente de la solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de la clave de acceso de S3 (remitente de la solicitud)	El ID de la clave de acceso a S3 con hash del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Bucket de S3	El nombre del depósito de S3.
S3KY	Clave de S3	El nombre de la clave S3, sin incluir el nombre del bucket. Las operaciones en buckets no incluyen este campo.
S3SR	Subrecurso S3	El subrecurso bucket u objeto sobre el que se está realizando la operación, si aplica.

Código	Campo	Descripción
SACC	Nombre de la cuenta de 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 hizo la solicitud.
SBAC	Nombre de la cuenta de tenant de S3 (propietario del bucket)	El nombre de la cuenta de inquilino del propietario del bucket. Se usa para identificar el acceso entre cuentas o el acceso anónimo.
SBAI	ID de la cuenta de tenant de S3 (propietario del bucket)	El ID de la cuenta de inquilino del propietario del bucket de destino. Se utiliza para identificar el acceso entre cuentas o el acceso anónimo.
SUSR	URN de usuario de S3 (remitente de la solicitud)	El ID de la cuenta del tenant y el nombre de usuario de la persona que realiza la solicitud. El usuario puede ser tanto un usuario local como un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Dejar en blanco para solicitudes anónimas.
HORA	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP de equilibrador de carga de confianza	Si la solicitud fue redirigida por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
TRNC	Truncado o no truncado	Establece en false si se han devuelto todos los resultados. Establece en true si hay más resultados disponibles para devolver. Solo para operaciones GET con buckets.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
VSID	ID de versión	El identificador de la versión específica de un objeto que se ha solicitado. Las operaciones en buckets y objetos de buckets sin versiones no incluyen este campo.

Cuando un cliente S3 realiza una operación HEAD, se envía una solicitud para comprobar la existencia de un objeto o bucket y recuperar los metadatos de un objeto. Este mensaje lo envía el servidor si la operación se realiza con éxito.

Código	Campo	Descripción
CBID	Identificador del 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 los buckets 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 verificado en bytes. Las operaciones sobre los buckets no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de los nombres y valores de los encabezados de las solicitudes 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 valor de <code>`X-Forwarded-For`</code> 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 la cuenta de inquilino de S3 (remitente de la solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de la clave de acceso de S3 (remitente de la solicitud)	El ID de la clave de acceso a S3 con hash del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Bucket de S3	El nombre del depósito de S3.
S3KY	Clave de S3	El nombre de la clave S3, sin incluir el nombre del bucket. Las operaciones en buckets no incluyen este campo.

Código	Campo	Descripción
SACC	Nombre de la cuenta de 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 hizo la solicitud.
SBAC	Nombre de la cuenta de tenant de S3 (propietario del bucket)	El nombre de la cuenta de inquilino del propietario del bucket. Se usa para identificar el acceso entre cuentas o el acceso anónimo.
SBAI	ID de la cuenta de tenant de S3 (propietario del bucket)	El ID de la cuenta de inquilino del propietario del bucket de destino. Se utiliza para identificar el acceso entre cuentas o el acceso anónimo.
SUSR	URN de usuario de S3 (remitente de la solicitud)	El ID de la cuenta del tenant y el nombre de usuario de la persona que realiza la solicitud. El usuario puede ser tanto un usuario local como un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Dejar en blanco para solicitudes anónimas.
HORA	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP de equilibrador de carga de confianza	Si la solicitud fue redirigida por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
VSID	ID de versión	El identificador de la versión específica de un objeto que se ha solicitado. Las operaciones en buckets y objetos de buckets sin versiones no incluyen este campo.

Mensaje de auditoría SPOS para transacciones S3 POST en StorageGRID

Cuando un cliente de S3 envía una solicitud POST Object, este mensaje es emitido por el servidor si la transacción se realiza correctamente.

Código	Campo	Descripción
CBID	Identificador del bloque de contenido	El identificador único del bloque de contenido solicitado. Si el CBID es desconocido, este campo se establece en 0.
CNCH	Encabezado de control de coherencia	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 los nombres y valores de los encabezados de las solicitudes 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 valor de <code>`X-Forwarded-For`</code> es diferente de la dirección IP del remitente de la solicitud (campo de auditoría SAIP). (No está previsto para SPOS).
RSLT	Código de resultado	Resultado de la solicitud RestoreObject. El resultado siempre es: SUCS: Exitoso
S3AI	ID de la cuenta de inquilino de S3 (remitente de la solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de la clave de acceso de S3 (remitente de la solicitud)	El ID de la clave de acceso a S3 con hash del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Bucket de S3	El nombre del depósito de S3.
S3KY	Clave de S3	El nombre de la clave S3, sin incluir el nombre del bucket. Las operaciones en buckets no incluyen este campo.

Código	Campo	Descripción
S3SR	Subrecurso S3	El subrecurso bucket u objeto sobre el que se está realizando la operación, si aplica. Establece en «select» para una operación S3 Select.
SACC	Nombre de la cuenta de 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 hizo la solicitud.
SBAC	Nombre de la cuenta de tenant de S3 (propietario del bucket)	El nombre de la cuenta de inquilino del propietario del bucket. Se usa para identificar el acceso entre cuentas o el acceso anónimo.
SBAI	ID de la cuenta de tenant de S3 (propietario del bucket)	El ID de la cuenta de inquilino del propietario del bucket de destino. Se utiliza para identificar el acceso entre cuentas o el acceso anónimo.
SRCF	Configuración de subrecursos	Restaurar información.
SUSR	URN de usuario de S3 (remitente de la solicitud)	El ID de la cuenta del tenant y el nombre de usuario de la persona que realiza la solicitud. El usuario puede ser tanto un usuario local como un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Dejar en blanco para solicitudes anónimas.
HORA	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP de equilibrador de carga de confianza	Si la solicitud fue redirigida por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.

Código	Campo	Descripción
VSID	ID de versión	El identificador de la versión específica de un objeto que se ha solicitado. Las operaciones en buckets y objetos de buckets sin versiones no incluyen este campo.

Mensaje de auditoría SPUT para transacciones S3 PUT en StorageGRID

Cuando un cliente S3 envía una transacción PUT, se realiza una solicitud para crear un nuevo objeto o bucket, o para eliminar un subrecurso de bucket u objeto. Este mensaje lo emite el servidor si la transacción se realiza con éxito.

Código	Campo	Descripción
CBID	Identificador del 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 los buckets no incluyen este campo.
CMPS	Configuración de cumplimiento normativo	Los parámetros de cumplimiento utilizados al crear el bucket, si figuran en la solicitud (truncados a los primeros 1024 caracteres).
CNCH	Encabezado de control de coherencia	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 con buckets no incluyen este campo.
GFID	ID de conexión de Grid Federation	El ID de conexión de la conexión de federación de grid asociada a una solicitud PUT de replicación entre grids. Solo se incluye en los registros de auditoría del grid de destino.
GFSA	ID de cuenta de origen de la federación de grid	El ID de cuenta del inquilino en la red de origen para una solicitud PUT de replicación entre grids. Solo se incluye en los registros de auditoría de la red de destino.

Código	Campo	Descripción
HTRH	Encabezado de solicitud HTTP	Lista de los nombres y valores de los encabezados de las solicitudes HTTP registrados, según se seleccionaron durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si el valor de `X-Forwarded-For` 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 activado	Valor de la cabecera de la solicitud <code>x-amz-bucket-object-lock-enabled</code> , si está presente en la solicitud.
LKLH	Bloqueo de objetos Legal Hold	Valor del encabezado de solicitud <code>x-amz-object-lock-legal-hold</code> , si está presente en la solicitud <code>PutObject</code> .
LKMD	Modo de retención de bloqueo de objetos	Valor de la cabecera de la solicitud <code>x-amz-object-lock-mode</code> , si está presente en la solicitud <code>PutObject</code> .
LKRU	Retener bloqueo de objeto hasta la fecha	Valor del encabezado de solicitud <code>x-amz-object-lock-retain-until-date</code> , si está presente en la solicitud <code>PutObject</code> . Los valores se limitan a un intervalo de 100 años respecto a la fecha en que se incorporó el objeto.
MTME	Hora de la última modificación	La marca de tiempo Unix, en microsegundos, que indica cuándo se modificó por última vez el objeto.
RSLT	Código de resultado	Resultado de la operación PUT. El resultado es siempre: SUCS: Exitoso
S3AI	ID de la cuenta de inquilino de S3 (remitente de la solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de la clave de acceso de S3 (remitente de la solicitud)	El ID de la clave de acceso a S3 con hash del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.

Código	Campo	Descripción
S3BK	Bucket de S3	El nombre del depósito de S3.
S3KY	Clave de S3	El nombre de la clave S3, sin incluir el nombre del bucket. Las operaciones en buckets no incluyen este campo.
S3SR	Subrecurso S3	El subrecurso bucket u objeto sobre el que se está realizando la operación, si aplica.
SACC	Nombre de la cuenta de 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 hizo la solicitud.
SBAC	Nombre de la cuenta de tenant de S3 (propietario del bucket)	El nombre de la cuenta de inquilino del propietario del bucket. Se usa para identificar el acceso entre cuentas o el acceso anónimo.
SBAI	ID de la cuenta de tenant de S3 (propietario del bucket)	El ID de la cuenta de inquilino del propietario del bucket de destino. Se utiliza para identificar el acceso entre cuentas o el acceso anónimo.
SRCF	Configuración de subrecursos	La nueva configuración del subrecurso (truncada a los primeros 1024 caracteres).
SUSR	URN de usuario de S3 (remitente de la solicitud)	El ID de la cuenta del tenant y el nombre de usuario de la persona que realiza la solicitud. El usuario puede ser tanto un usuario local como un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Dejar en blanco para solicitudes anónimas.
HORA	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP de equilibrador de carga de confianza	Si la solicitud fue redirigida por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.

Código	Campo	Descripción
ULID	ID de subida	Incluido solo en los mensajes SPUT para operaciones de CompleteMultipartUpload. Indica que todas las partes se han cargado y ensamblado.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
VSID	ID de versión	El ID de versión de un nuevo objeto creado en un bucket con control de versiones. Las operaciones en buckets y objetos en buckets sin control de versiones no incluyen este campo.
VSST	Estado de versionado	El nuevo estado de control de versiones de un bucket. Se utilizan dos estados: «habilitado» o «suspendido». Las operaciones sobre objetos no incluyen este campo.

Mensaje de auditoría SREM para la eliminación del almacén de objetos en StorageGRID

Este mensaje se muestra cuando se elimina contenido del almacenamiento persistente y ya no se puede acceder a él a través de las API habituales.

Código	Campo	Descripción
CBID	Identificador del 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 se ha eliminado un bloque de contenido determinado de un nodo y ya no se puede solicitar directamente. Puedes usar el mensaje para realizar el seguimiento del flujo de contenido eliminado dentro del sistema.

Mensaje de auditoría SUPD para actualizaciones de metadatos S3 en StorageGRID

Este mensaje lo genera la API de S3 cuando un cliente de S3 actualiza los metadatos de un objeto incorporado. El servidor envía este mensaje si la actualización de los metadatos se realiza correctamente.

Código	Campo	Descripción
CBID	Identificador del 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 los buckets no incluyen este campo.

Código	Campo	Descripción
CNCH	Encabezado de control de coherencia	El valor del encabezado de solicitud HTTP Consistency-Control, si está presente en la solicitud, al actualizar la configuración de cumplimiento de un bucket.
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 con buckets no incluyen este campo.
HTRH	Encabezado de solicitud HTTP	Lista de los nombres y valores de los encabezados de las solicitudes HTTP registrados, según se seleccionaron durante la configuración. `X-Forwarded-For` se incluye automáticamente si está presente en la solicitud y si el valor de `X-Forwarded-For` 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 la cuenta de inquilino de S3 (remitente de la solicitud)	El ID de cuenta de inquilino del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3AK	ID de la clave de acceso de S3 (remitente de la solicitud)	El ID de la clave de acceso a S3 con hash del usuario que envió la solicitud. Un valor vacío indica acceso anónimo.
S3BK	Bucket de S3	El nombre del depósito de S3.
S3KY	Clave de S3	El nombre de la clave S3, sin incluir el nombre del bucket. Las operaciones en buckets no incluyen este campo.
SACC	Nombre de la cuenta de 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 hizo la solicitud.
SBAC	Nombre de la cuenta de tenant de S3 (propietario del bucket)	El nombre de la cuenta de inquilino del propietario del bucket. Se usa para identificar el acceso entre cuentas o el acceso anónimo.
SBAI	ID de la cuenta de tenant de S3 (propietario del bucket)	El ID de la cuenta de inquilino del propietario del bucket de destino. Se utiliza para identificar el acceso entre cuentas o el acceso anónimo.
SUSR	URN de usuario de S3 (remitente de la solicitud)	El ID de la cuenta del tenant y el nombre de usuario de la persona que realiza la solicitud. El usuario puede ser tanto un usuario local como un usuario LDAP. Por ejemplo: <code>urn:sgws:identity::03393893651506583485:root</code> Dejar en blanco para solicitudes anónimas.
HORA	Tiempo	Tiempo total de procesamiento de la solicitud en microsegundos.
TLIP	Dirección IP de equilibrador de carga de confianza	Si la solicitud fue redirigida por un equilibrador de carga de capa 7 de confianza, la dirección IP del equilibrador de carga.
UUID	Identificador único universal	El identificador del objeto dentro del sistema StorageGRID.
VSID	ID de versión	El ID de versión de la versión específica de un objeto cuyos metadatos se actualizaron. Las operaciones en buckets y objetos en buckets sin versiones no incluyen este campo.

Mensaje de auditoría SVRF para fallos de verificación de almacén de objetos en StorageGRID

Este mensaje se emite siempre que un bloque de contenido no supera el proceso de verificación. Cada vez que se leen o escriben en el disco datos de objetos replicados, se realizan varias comprobaciones de verificación e integridad para garantizar que los datos enviados al usuario que los solicita sean idénticos a los introducidos originalmente en el sistema. Si alguna de estas comprobaciones falla, el sistema pone automáticamente en cuarentena los datos de objetos replicados corruptos para evitar que se vuelvan a recuperar.

Código	Campo	Descripción
CBID	Identificador del bloque de contenido	El identificador único del bloque de contenido cuya verificación ha fallado.
RSLT	Código de resultado	Tipo de error de verificación: CRCF: Error en la comprobación de redundancia cíclica (CRC). HMAC: Falló la comprobación del código de autenticación de mensajes basado en hash (HMAC). EHSR: Hash de contenido cifrado inesperado. PHSR: Hash de contenido original inesperado. SEQC: Secuencia de datos incorrecta en el disco. PERR: Estructura no válida del archivo en disco. DERR: Error de disco. FNAM: Nombre de archivo incorrecto.



Debes supervisar este mensaje de cerca. Los fallos de verificación de contenido pueden indicar fallos de hardware inminentes.

Para determinar qué operación activó el mensaje, consulta 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.

Mensaje de auditoría SVRU para contenido desconocido de almacén de objetos en StorageGRID

El componente de almacenamiento del servicio LDR analiza continuamente todas las copias de los datos de objetos replicados en el almacén de objetos. Este mensaje se emite cuando se detecta una copia desconocida o inesperada de los 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 inesperada del objeto.
RSLT	Resultado	Este campo tiene el valor 'NONE'. 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 supervisarse de cerca. Significa que se detectaron copias inesperadas de datos de objetos en el almacén de objetos. Esta situación debe investigarse de inmediato para determinar cómo se crearon estas copias, porque puede indicar fallos de hardware inminentes.

Mensaje de auditoría SYSD para paradas de nodo graceful en StorageGRID

Cuando un servicio se detiene de forma ordenada, se genera este mensaje para indicar que se solicitó el apagado. Normalmente, este mensaje solo se envía después de un reinicio posterior, porque la cola de mensajes de auditoría no se borra antes del apagado. Busca el mensaje SYST, enviado al principio de la secuencia de apagado, si el servicio no se ha reiniciado.

Código	Campo	Descripción
RSLT	Apagado correcto	La naturaleza del cierre: SUCS: el sistema se ha apagado correctamente.

El mensaje no indica si se está deteniendo el servidor anfitrión, solo el servicio de generación de informes. El RSLT de un SYSD no puede indicar un apagado "sucio", porque el mensaje solo se genera en apagados "limpios".

Mensaje de auditoría SYST para nodo que se detiene en StorageGRID

Cuando un servicio se detiene de forma controlada, se genera este mensaje para indicar que se ha solicitado el apagado y que el servicio ha iniciado su secuencia de apagado. SYST se puede usar para determinar si se ha solicitado el apagado, antes de que el servicio se reinicie (a diferencia de SYSD, que normalmente se envía después de que el servicio se reinicia).

Código	Campo	Descripción
RSLT	Apagado correcto	La naturaleza del cierre: SUCS: el sistema se ha apagado correctamente.

El mensaje no indica si el servidor host se está deteniendo, solo el servicio de informes. El código RSLT de un mensaje SYST no puede indicar un apagado "no limpio", ya que el mensaje solo se genera mediante apagados "limpios".

Mensaje de auditoría SYSU para el inicio de nodo en StorageGRID

Cuando se reinicia un servicio, se genera este mensaje para indicar si el apagado anterior fue correcto (programado) o anómalo (inesperado).

Código	Campo	Descripción
RSLT	Apagado correcto	La naturaleza del cierre: SUCS: El sistema se ha apagado correctamente. DSDN: el sistema no se apagó correctamente. VRGN: El sistema se inició por primera vez después de la instalación (o reinstalación) del servidor.

El mensaje no indica si se ha iniciado el servidor host, solo el servicio de generación de informes. Este mensaje se puede utilizar para:

- Detectar discontinuidad en el registro de auditoría.
- Determina si un servicio está fallando durante su funcionamiento (ya que la naturaleza distribuida del sistema StorageGRID puede ocultar estos fallos). Administrador de servidores reinicia automáticamente un servicio que ha fallado.

Amplía la capacidad o las capacidades de tu sistema StorageGRID

Descubre cómo ampliar tu sistema StorageGRID

Descubre cómo ampliar tu sistema StorageGRID para aumentar la capacidad o las funcionalidades sin interrumpir las operaciones. Puedes añadir volúmenes de almacenamiento a los nodos de almacenamiento existentes, añadir nuevos nodos de grid a un sitio existente o añadir un nuevo sitio.

Antes de ampliar un nodo de la red, debes confirmar que no haya ningún trabajo de reparación de datos activo. Si alguna reparación ha fallado, debes reiniciarla y dejar que termine antes de realizar el procedimiento de decomisionar o ampliar. Consulta "[Comprobar los trabajos de reparación de datos](#)".

Una ampliación de StorageGRID te permite añadir:

- Volúmenes de almacenamiento a nodos de almacenamiento
- Nuevos nodos de grid en un sitio existente
- Un sitio completamente nuevo

El motivo por el que realizas la expansión determina cuántos nodos nuevos de cada tipo debes añadir y la ubicación de esos nuevos nodos. Por ejemplo, existen diferentes requisitos de nodos si realizas una expansión para aumentar la capacidad de almacenamiento, añadir capacidad de metadatos o añadir redundancia o nuevas funciones.

Sigue los pasos correspondientes al tipo de expansión que vas a realizar:

Agregar nodos de grid

1. Sigue los pasos para ["Agregar nodos de grid a un sitio existente"](#).
2. ["Actualizar las subredes"](#).
3. Implementar nodos de la red:
 - ["Dispositivos"](#)
 - ["VMware"](#)
 - ["Linux"](#)



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

1. ["Realiza la expansión"](#).
2. ["Configura el sistema ampliado"](#).

Agregar volúmenes de almacenamiento

Sigue los pasos para ["Agregar volúmenes de almacenamiento a los nodos de almacenamiento"](#).

Agregar nuevo sitio

1. Sigue los pasos para ["Añadir un nuevo sitio"](#).
2. ["Actualizar las subredes"](#).
3. Implementar nodos de la red:
 - ["Dispositivos"](#)
 - ["VMware"](#)
 - ["Linux"](#)



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

1. ["Realiza la expansión"](#).
2. ["Configura el sistema ampliado"](#).

Planificación de la expansión

Planificación de la ampliación de los datos replicados en StorageGRID

Si la política de gestión del ciclo de vida de la información (ILM) de tu implementación incluye una regla que crea copias replicadas de los objetos, debes tener en cuenta cuánto almacenamiento añadir y dónde añadir los nuevos volúmenes de almacenamiento o Storage Nodes.

Para obtener orientación sobre dónde añadir almacenamiento adicional, examina las reglas de ILM que crean copias replicadas. Si las reglas de ILM crean dos o más copias de objetos, planifica añadir almacenamiento en

cada ubicación donde se realicen copias de objetos. Como ejemplo sencillo, si tienes un grid de dos sitios y una regla de ILM que crea una copia de objeto en cada sitio, debes ["agregar almacenamiento"](#) a cada sitio para aumentar la capacidad de objetos global del grid. Para obtener información sobre la replicación de objetos, consulta ["¿Qué es la replicación?"](#).

Por motivos de rendimiento, conviene intentar mantener un equilibrio entre la capacidad de almacenamiento y la potencia de cálculo en todos los sitios. Así que, en este ejemplo, deberías añadir el mismo número de Storage Nodes a cada sitio o volúmenes de almacenamiento adicionales en cada sitio.

Si tienes una política de ILM más compleja que incluye reglas que colocan los objetos en diferentes ubicaciones según criterios como el nombre del bucket, o reglas que cambian la ubicación de los objetos con el tiempo, tu análisis de dónde se requiere almacenamiento para la ampliación será similar, pero más complejo.

Graficar la rapidez con la que se consume la capacidad de almacenamiento general puede ayudarte a entender cuánto almacenamiento añadir en la ampliación y cuándo se necesitará el espacio de almacenamiento adicional. Puedes usar el Grid Manager para ["supervisar y graficar la capacidad de almacenamiento"](#).

A la hora de planificar el momento adecuado para una ampliación, recuerda tener en cuenta el tiempo que podría llevar adquirir e instalar capacidad de almacenamiento adicional. Para simplificar la planificación de la ampliación, plantéate añadir Storage Nodes cuando los Storage Nodes existentes alcancen el 70% de capacidad.

Planificación de la expansión para datos con código de borrado (EC) en StorageGRID

Si tu política de ILM incluye una regla que crea copias con codificación de borrado, debes planificar dónde añadir nuevo almacenamiento y cuándo hacerlo. La cantidad de almacenamiento que añadas y el momento en que lo hagas pueden afectar a la capacidad de almacenamiento útil de la grid.

El primer paso para planificar una ampliación del almacenamiento es examinar las reglas de tu política de ILM que crean objetos con código de borrado. Como StorageGRID crea $k+m$ fragmentos para cada objeto con código de borrado y almacena cada fragmento en un nodo de almacenamiento diferente, debes asegurarte de que al menos $k+m$ nodos de almacenamiento tengan espacio para los nuevos datos con código de borrado después de la ampliación. Si el perfil de código de borrado proporciona protección contra la pérdida de un sitio, debes añadir almacenamiento a cada sitio. Consulta ["¿Qué son los esquemas de erasure coding?"](#) para obtener información sobre los perfiles de código de borrado.

El número de nodos que debes añadir también depende de lo llenos que estén los nodos existentes cuando realices la ampliación.

Recomendación general para añadir capacidad de almacenamiento para objetos con código de borrado

Si quieres evitar cálculos detallados, puedes añadir dos nodos de almacenamiento por sitio cuando los nodos de almacenamiento existentes alcancen el 70% de capacidad.

Esta recomendación general ofrece resultados razonables en una amplia gama de esquemas de código de borrado, tanto para grids de un solo sitio como para grids en las que el código de borrado proporciona protección frente a la pérdida de sitios.

Para entender mejor los factores que llevaron a esta recomendación o para desarrollar un plan más preciso

para tu sitio, consulta ["Aspectos a tener en cuenta para el reequilibrio de datos con código de borrado"](#). Para una recomendación personalizada optimizada para tu situación, contacta a tu consultor de Servicios Profesionales de NetApp.

Infórmate sobre el reequilibrio de EC tras la expansión en StorageGRID

Si estás llevando a cabo una ampliación para añadir nodos de almacenamiento y utilizas reglas de ILM para codificar datos con código de borrado, es posible que tengas que realizar el procedimiento de reequilibrio de EC (erasure coding) si no puedes añadir suficientes nodos de almacenamiento para el esquema de erasure coding que estás utilizando.

Después de revisar estas consideraciones, realiza la expansión y luego ve a ["Reequilibra los datos con código de borrado después de añadir Storage Nodes"](#) para ejecutar el procedimiento.

¿Qué es el reequilibrio de EC?

El reequilibrio de EC es un procedimiento de StorageGRID que puede ser necesario tras una ampliación de los nodos de almacenamiento. El procedimiento se ejecuta como un script de línea de comandos desde el nodo de administración principal. Al ejecutar el procedimiento de reequilibrio de EC, StorageGRID redistribuye los fragmentos con código de borrado entre los nodos de almacenamiento existentes y los recién añadidos en un sitio.

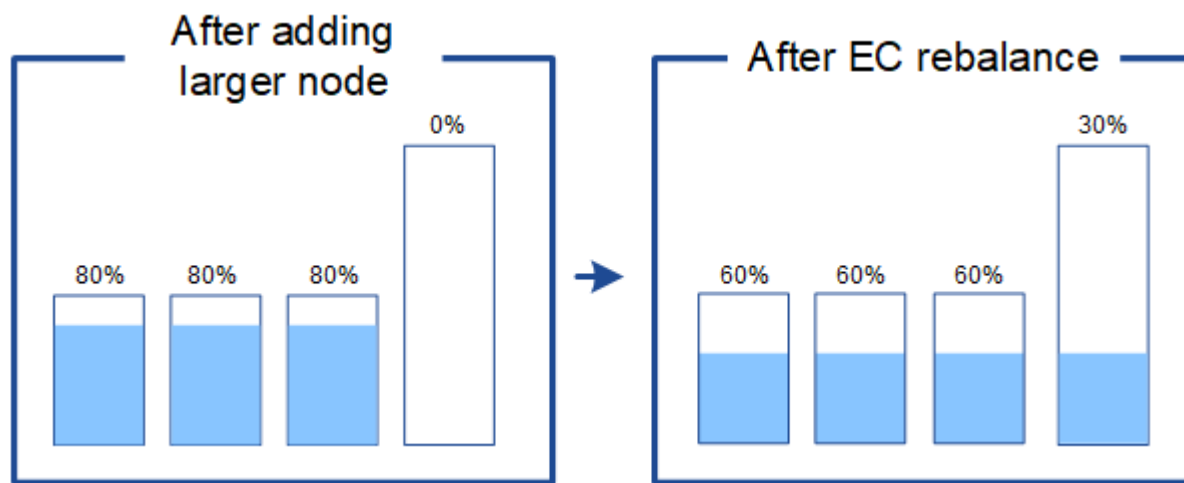
El procedimiento de reequilibrio de EC:

- Solo mueve datos de objetos con código de borrado. No mueve datos de objetos replicados.
- Redistribuye los datos dentro de un sitio. No mueve datos entre sitios.
- Redistribuye los datos entre todos los nodos de almacenamiento de un sitio. No redistribuye los datos dentro de los volúmenes de almacenamiento.
- Intenta distribuir el mismo número de bytes entre cada nodo. Los nodos que contengan más datos replicados almacenarán menos datos con código de borrado una vez finalizado el reequilibrio.
- Redistribuye los datos con código de borrado de manera uniforme entre los nodos de almacenamiento sin tener en cuenta las capacidades relativas de cada nodo. Los datos replicados se incluyen en el cálculo.
- No distribuirá datos con código de borrado a los nodos de almacenamiento que estén llenos en más de un 80%.
- Podría disminuir el rendimiento de las operaciones de ILM y de las operaciones del cliente S3 cuando se ejecuta, ya que se requieren recursos adicionales para redistribuir los fragmentos de código de borrado.

Cuando se complete el procedimiento de reequilibrio de EC:

- Los datos con código de borrado se habrán trasladado 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 sufrirá cambios.
- Los valores de Usado (%) pueden ser diferentes entre los nodos de almacenamiento por dos razones:
 - Las copias de los objetos replicados seguirán ocupando espacio en los nodos existentes—el procedimiento de reequilibrio del EC no traslada los datos replicados.
 - Los nodos de mayor capacidad estarán relativamente menos llenos que los de menor capacidad, aunque todos los nodos acabarán teniendo aproximadamente la misma cantidad de datos.

Por ejemplo, supón 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 añades un nodo de 400 TB y ejecutas 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.



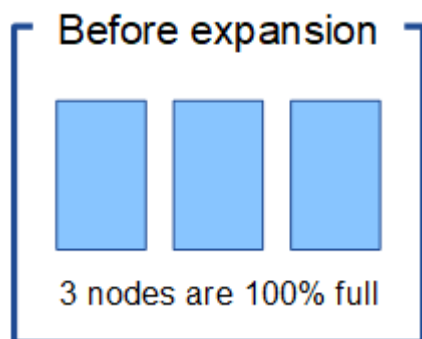
Cuándo reequilibrar los datos con código de borrado

El procedimiento de reequilibrado de EC redistribuye los datos con código de borrado existentes para garantizar que los nodos no se llenen ni permanezcan llenos. El procedimiento ayuda a garantizar que la codificación de EC pueda continuar en el sitio.

Ejecuta el procedimiento de reequilibrio cuando hay un sesgo preocupante en la distribución de los datos en un sitio y el sitio almacena principalmente datos de EC (ya que los datos replicados no se pueden mover mediante el reequilibrio).

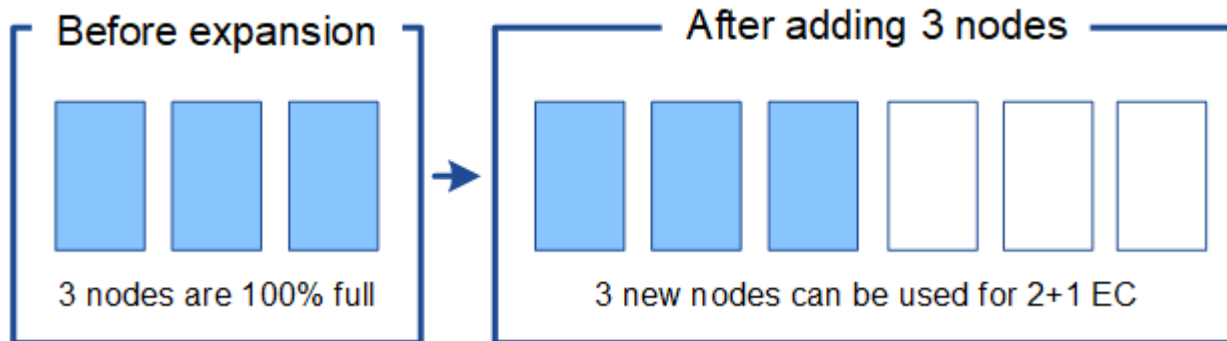
Imagina el siguiente escenario:

- StorageGRID se está ejecutando en un único sitio, que contiene tres nodos de almacenamiento.
- La política de ILM utiliza una regla de código de borrado 2+1 para todos los objetos de más de 1,0 MB y una regla de replicación de 2 copias para los objetos más pequeños.
- Todos los nodos de almacenamiento están completamente llenos. Se ha activado la alerta **Low Object Storage** con un nivel de gravedad mayor.



No es necesario realizar un reequilibrio si añades suficientes nodos

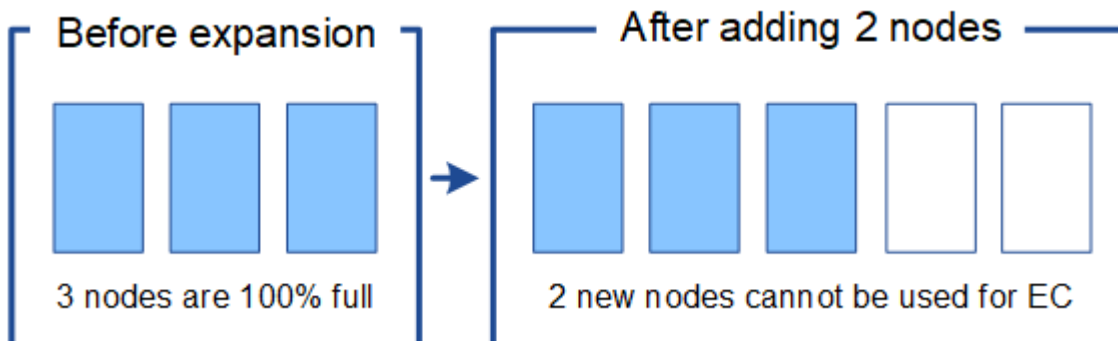
Para entender cuándo no es necesario realizar un reequilibrio de EC, supongamos que has añadido tres (o más) nuevos nodos de almacenamiento. En este caso, no necesitas realizar un reequilibrio de EC. Los nodos de almacenamiento originales seguirán llenos, pero los nuevos objetos ahora usarán los tres nuevos nodos para el código de borrado 2+1: los dos fragmentos de datos y el fragmento de paridad pueden almacenarse cada uno en un nodo diferente.



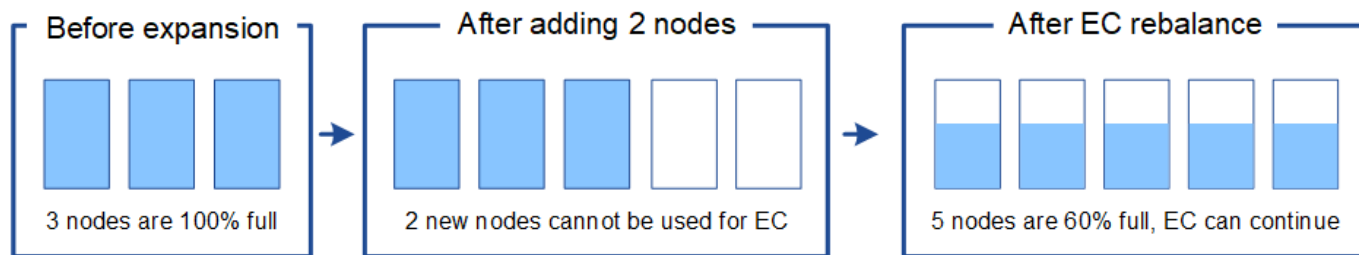
Aunque en este caso puedes ejecutar el procedimiento de reequilibrio de código de borrado, mover los datos existentes con código de borrado reducirá temporalmente el rendimiento del grid, lo que podría afectar las operaciones de los clientes.

Es necesario reequilibrar si no puedes añadir suficientes nodos

Para entender cuándo es necesario un reequilibrio de la codificación de borrado (EC), supón que solo puedes añadir dos nodos de almacenamiento, en lugar de tres. Porque el esquema 2+1 requiere que al menos tres nodos de almacenamiento tengan espacio disponible, los nodos vacíos no pueden usarse para nuevos datos con código de borrado.



Para utilizar los nuevos nodos de almacenamiento, debes ejecutar el procedimiento de reequilibrio de EC. Cuando se ejecuta este procedimiento, StorageGRID redistribuye los datos con código de borrado y los fragmentos de paridad existentes entre todos los nodos de almacenamiento del sitio. En este ejemplo, una vez finalizado el procedimiento de reequilibrio de EC, los cinco nodos están ahora a solo un 60 % de su capacidad, y se pueden seguir incorporando objetos al esquema de código de borrado 2+1 en todos los nodos de almacenamiento.



Recomendaciones para el reequilibrio de EC

NetApp requiere un reequilibrio de EC si *todas* las afirmaciones siguientes son ciertas:

- Utilizas código de borrado para tus datos de objetos.
- Se ha activado la alerta **Nivel bajo de almacenamiento de objetos** para uno o varios Storage Nodes en un sitio, lo que indica que los nodos están llenos en un 80 % o más.
- No puedes añadir suficientes Storage Nodes nuevos para el esquema de código de borrado en uso. Consulta ["Agrega capacidad de almacenamiento para objetos con código de borrado"](#).
- Tus clientes de S3 pueden soportar un rendimiento inferior en sus operaciones de escritura y lectura mientras se está ejecutando el procedimiento de reequilibrio de EC.

Opcionalmente, puedes ejecutar el procedimiento de reequilibrio de EC si prefieres que los nodos de almacenamiento se llenen hasta niveles similares y tus clientes S3 pueden tolerar un rendimiento inferior en sus operaciones de escritura y lectura mientras se ejecuta el procedimiento de reequilibrio de EC.

Cómo interactúa el procedimiento de reequilibrio de EC con otras tareas de mantenimiento

No puedes realizar ciertos procedimientos de mantenimiento al mismo tiempo que estás ejecutando el procedimiento de reequilibrio de EC.

Procedimiento	¿Se permite durante el procedimiento de reequilibrio de EC?
Procedimientos adicionales de reequilibrio de EC	No. Solo puedes ejecutar un procedimiento de reequilibrio de EC a la vez.
Procedimiento para decomisionar Trabajo de reparación de datos EC	No. • No puedes iniciar un procedimiento para decomisionar ni una reparación de datos de EC mientras se está ejecutando el procedimiento de reequilibrio de EC. • No puedes iniciar el procedimiento de reequilibrio de EC mientras se esté ejecutando un procedimiento para decomisionar un nodo de almacenamiento o una reparación de datos de EC.
Procedimiento de ampliación	No. Si necesitas añadir nuevos nodos de almacenamiento en una ampliación, ejecuta el procedimiento de reequilibrio de EC después de añadir todos los nuevos nodos.

Procedimiento	¿Se permite durante el procedimiento de reequilibrio de EC?
Procedimiento de actualización	No. Si necesitas actualizar el software StorageGRID, realiza el procedimiento de actualización antes o después de ejecutar el procedimiento de rebalanceo de EC. Si es necesario, puedes finalizar el procedimiento de rebalanceo de EC para realizar una actualización de software.
Procedimiento de clonación de un nodo de appliance	No. Si necesitas clonar un nodo de almacenamiento de un appliance, ejecuta el procedimiento de reequilibrio de EC tras añadir el nuevo nodo.
Procedimiento de corrección urgente	Sí. Puedes aplicar una corrección urgente de StorageGRID mientras se está ejecutando el procedimiento de reequilibrio de EC.
Otros procedimientos de mantenimiento	No. Debes finalizar el procedimiento de reequilibrio de EC antes de ejecutar otros procedimientos de mantenimiento.

Cómo interactúa el procedimiento de reequilibrio de EC con ILM

Mientras se esté ejecutando el procedimiento de reequilibrio de EC, evita realizar cambios en ILM que puedan modificar la ubicación de los objetos con código de borrado existentes. Por ejemplo, no empieces a utilizar una regla de ILM que tenga un perfil de código de borrado diferente. Si necesitas realizar dichos cambios en ILM, debes interrumpir el procedimiento de reequilibrio de EC.

Directrices de expansión

Directrices para añadir capacidad de objetos en StorageGRID

Puedes ampliar la capacidad de almacenamiento de objetos de tu sistema StorageGRID añadiendo volúmenes de almacenamiento a los Storage Nodes existentes o añadiendo nuevos Storage Nodes a los sitios existentes. Debes añadir capacidad de almacenamiento de manera que cumpla con los requisitos de tu política de gestión del ciclo de vida de la información (ILM).

Guía para añadir volúmenes de almacenamiento

Antes de añadir volúmenes de almacenamiento a los nodos de almacenamiento existentes, revisa las siguientes directrices y limitaciones:

- Debes revisar tus reglas actuales de ILM para determinar dónde y cuándo ["añadir volúmenes de almacenamiento"](#) para aumentar la capacidad de almacenamiento disponible para ["objetos replicados"](#) o

["objetos con código de borrado"](#).

- No puedes aumentar la capacidad de metadatos de tu sistema añadiendo volúmenes de almacenamiento porque los metadatos de los objetos solo se almacenan en el volumen 0.
- Cada nodo de almacenamiento basado en software puede admitir un máximo de 48 volúmenes de almacenamiento. Si necesitas añadir capacidad más allá de ese límite, debes añadir nuevos nodos de almacenamiento.
- Puedes añadir una o dos bandejas de expansión a cada dispositivo SG6060. Cada bandeja de expansión añade 16 volúmenes de almacenamiento. Con ambas bandejas de expansión instaladas, el SG6060 puede admitir un total de 48 volúmenes de almacenamiento.
- Puedes añadir una o dos bandejas de expansión a cada SG6160. Cada bandeja de expansión añade 60 volúmenes de almacenamiento. Con ambas bandejas de expansión instaladas, el SG6160 puede admitir un total de 180 volúmenes de almacenamiento.
- No puedes añadir volúmenes de almacenamiento a ningún otro dispositivo de almacenamiento.
- No puedes aumentar el tamaño de un volumen de almacenamiento existente.
- No puedes añadir volúmenes de almacenamiento a un nodo de almacenamiento al mismo tiempo que realizas una actualización del sistema, una operación de recuperación u otra expansión.

Una vez que hayas decidido añadir volúmenes de almacenamiento y hayas determinado qué nodos de almacenamiento debes ampliar para cumplir con tu política de ILM, sigue las instrucciones correspondientes a tu tipo de nodo de almacenamiento:

- Para añadir una o dos bandejas de expansión a un dispositivo de almacenamiento SG6060, visita ["Agregar bandeja de expansión a SG6060 desplegado"](#).
- Para añadir una o dos bandejas de expansión a un dispositivo de almacenamiento SG6160, ve a ["Agregar bandeja de expansión a SG6160 desplegado"](#)
- Para un nodo basado en software, sigue las instrucciones para ["Agregar volúmenes de almacenamiento a los nodos de almacenamiento"](#).

Guía para añadir nodos de almacenamiento

Antes de añadir nodos de almacenamiento a los sitios existentes, revisa las siguientes directrices y limitaciones:

- Debes revisar tus reglas actuales de ILM para determinar dónde y cuándo añadir nodos de almacenamiento para aumentar el almacenamiento disponible para ["objetos replicados"](#) o ["objetos con código de borrado"](#).
- No debes añadir más de 10 nodos de almacenamiento en un solo procedimiento de expansión.
- Puedes añadir nodos de almacenamiento a más de un sitio en un único procedimiento de expansión.
- Puedes añadir Storage Nodes y otros tipos de nodos en un único proceso de ampliación.
- Antes de iniciar el procedimiento de expansión, debes confirmar que todas las operaciones de reparación de datos realizadas como parte de una recuperación estén completas. Consulta ["Comprobar los trabajos de reparación de datos"](#).
- Si necesitas eliminar nodos de almacenamiento antes o después de realizar una expansión, no debes decomisionar más de 10 nodos de almacenamiento en un solo procedimiento de Decomisionar nodo.
- Añade suficientes nodos de almacenamiento para mantener el rendimiento de E/S del almacenamiento subyacente. Las operaciones de escritura se distribuirán entre los nodos de almacenamiento en función de la capacidad de almacenamiento disponible. Si los nodos de almacenamiento ampliados tienen una capacidad de almacenamiento disponible significativamente mayor, esos nodos recibirán un número

significativamente mayor de escrituras. En particular, cuando los nodos de almacenamiento existentes estén casi llenos, las nuevas escrituras dependerán solo de los nodos de almacenamiento ampliados. Las operaciones de lectura y eliminación se gestionarán según tu carga de trabajo específica.

Directrices para el servicio ADC en los nodos de almacenamiento

Al configurar la ampliación, debes elegir si deseas incluir el servicio de 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 grid.

- Puedes ["trasladar el servicio ADC de un nodo de almacenamiento a otro en el mismo sitio"](#).
- El sistema StorageGRID requiere que un ["quórum de los servicios de ADC"](#) esté disponible en cada sede y en todo momento.
- Al menos tres nodos de almacenamiento en cada sitio deben incluir el servicio ADC.
- No se recomienda añadir el servicio ADC a todos los nodos de almacenamiento. Incluir demasiados servicios ADC puede provocar ralentizaciones debido al aumento de la comunicación entre los nodos.
- Una misma grid no debe tener más de 48 nodos de almacenamiento con el servicio ADC. Esto equivale a 16 sitios con tres servicios ADC en cada sitio.
- En general, cuando selecciones la configuración **ADC Service** para un nuevo nodo, deberías seleccionar **Automatic**. Selecciona **Yes** solo si el nuevo nodo reemplazará a otro nodo de almacenamiento que incluya el servicio ADC. Como no puedes decomisionar un nodo de almacenamiento si quedan muy pocos servicios ADC, seleccionar **Yes** garantiza que haya un nuevo servicio ADC disponible antes de eliminar el servicio antiguo.

Directrices para ampliar la capacidad de metadatos en StorageGRID

Para garantizar que haya espacio suficiente para los metadatos de los objetos, puede que tengas que realizar un procedimiento de ampliación para añadir nuevos Storage Nodes en cada sitio.

StorageGRID reserva espacio para los metadatos de objetos en el volumen 0 de cada nodo de almacenamiento. Se mantienen tres copias de todos los metadatos de objetos en cada sitio, distribuidas de manera uniforme entre todos los nodos de almacenamiento.

Puedes utilizar el Grid Manager para supervisar la capacidad de metadatos de los nodos de almacenamiento y calcular a qué ritmo se está consumiendo dicha capacidad. Además, se activa la alerta **Low metadata storage** para un nodo de almacenamiento cuando el espacio de metadatos utilizado alcanza determinados umbrales.

Ten en cuenta que la capacidad de metadatos de objetos de una grid puede agotarse más rápido que su capacidad de almacenamiento de objetos, dependiendo de cómo utilices la grid. Por ejemplo, si normalmente incorporas grandes cantidades de objetos pequeños o añades grandes cantidades de metadatos de usuario o etiquetas a los objetos, puede que necesites añadir Storage Nodes para aumentar la capacidad de metadatos, aunque aún quede suficiente capacidad de almacenamiento de objetos.

Para obtener más información, consulta lo siguiente:

- ["Gestiona el almacenamiento de metadatos de objetos"](#)
- ["Supervisa la capacidad de metadatos de objetos para cada Storage Node"](#)

Directrices para aumentar la capacidad de metadatos

Antes de añadir nodos de almacenamiento para aumentar la capacidad de metadatos, revisa las siguientes directrices y limitaciones:

- Siempre que se disponga de suficiente capacidad de almacenamiento de objetos, contar con más espacio disponible para los metadatos de los objetos aumenta el número de objetos que puedes almacenar en tu sistema StorageGRID.
- Puedes aumentar la capacidad de metadatos de una grid añadiendo uno o varios Storage Nodes a cada sitio.
- El espacio real reservado para los metadatos de los objetos en un Storage Node concreto depende de la opción de almacenamiento Metadata Reserved Space (configuración a nivel de sistema), de la cantidad de RAM asignada al nodo y del tamaño del volumen 0 del nodo.
- No puedes aumentar la capacidad de metadatos añadiendo volúmenes de almacenamiento a los Storage Nodes existentes, porque los metadatos solo se almacenan en el volumen 0.
- No puedes aumentar la capacidad de metadatos añadiendo un nuevo sitio.
- StorageGRID mantiene tres copias de todos los metadatos de objetos en cada sitio. Por este motivo, la capacidad de metadatos de tu sistema se ve limitada por la capacidad de metadatos de tu sitio más pequeño.
- Al ampliar la capacidad de metadatos, debes añadir el mismo número de nodos de almacenamiento a cada sitio.

Los nodos de almacenamiento exclusivos para metadatos tienen requisitos de hardware específicos:

- Al utilizar dispositivos StorageGRID, los nodos dedicados exclusivamente a metadatos solo se pueden configurar en dispositivos SGF6112 con doce unidades de 1,9 TB o doce de 3,8 TB.
- Cuando se utilizan nodos basados en software, los recursos de nodos solo metadatos deben coincidir con los recursos de Storage Nodes existentes. Por ejemplo:
 - Si el sitio de StorageGRID existente utiliza dispositivos SG6000 o SG6100, los nodos basados en software y dedicados exclusivamente a los metadatos 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 utiliza nodos de almacenamiento virtuales con 24 GB de RAM, 8 núcleos de CPU y 3 TB o 4 TB de almacenamiento de metadatos, los nodos basados en software dedicados exclusivamente a metadatos deberían utilizar recursos similares (24 GB de RAM, 8 núcleos de CPU y 4 TB de almacenamiento de metadatos (rangedb/0)).
- Al añadir un nuevo sitio de StorageGRID, la capacidad total de metadatos del nuevo sitio debe, como mínimo, igualar la de los sitios de StorageGRID existentes y los recursos del nuevo sitio deben igualar los nodos de almacenamiento en los sitios de StorageGRID existentes.

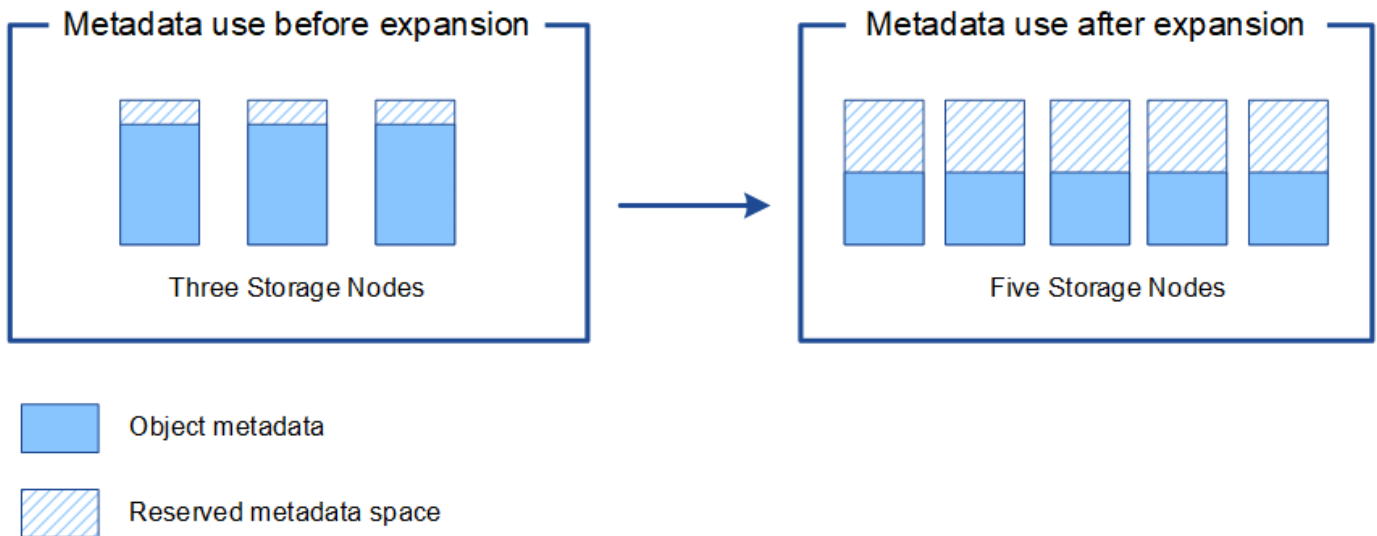
Consulta el ["Descripción de qué es el espacio reservado para metadatos"](#).

Cómo se redistribuyen los metadatos al añadir nodos de almacenamiento

Al añadir nodos de almacenamiento en una ampliación, StorageGRID redistribuye los metadatos de los objetos existentes a los nuevos nodos de cada sitio, lo que aumenta la capacidad total de metadatos del grid. No se requiere ninguna acción por parte del usuario.

La siguiente figura muestra cómo StorageGRID redistribuye los metadatos de objetos cuando añades Storage Nodes en una ampliación. El lado izquierdo de la figura representa el volumen 0 de tres Storage Nodes antes de una ampliación. Los metadatos están consumiendo una parte relativamente grande del espacio de metadatos disponible de cada nodo, y se ha activado la alerta **Low metadata storage**.

La parte derecha de la figura muestra cómo se redistribuyen los metadatos existentes tras añadir dos nodos de almacenamiento al sitio. La cantidad de metadatos en cada nodo ha disminuido, la alerta **Low metadata storage** ya no se activa y el espacio disponible para metadatos ha aumentado.



Directrices para añadir nodos de grid en StorageGRID

Puedes añadir redundancia o capacidades adicionales a un sistema StorageGRID agregando nuevos nodos de grid a los sitios existentes.

Por ejemplo, puedes optar por añadir nodos de puerta de enlace para utilizarlos en un grupo de alta disponibilidad (HA), o bien añadir un nodo de administración en una sede remota para permitir la supervisión mediante un nodo local.

Puedes añadir uno o varios de los siguientes tipos de nodos a uno o varios sitios existentes en una única operación de ampliación:

- Nodos de administración no primarios
- Nodos de almacenamiento
- Nodos de puerta de enlace

Al prepararte para añadir nodos de grid, ten en cuenta las siguientes limitaciones:

- El nodo de administración principal se implementa durante la instalación inicial. No puedes añadir un nodo de administración principal durante una ampliación.
- Puedes añadir nodos de almacenamiento y otros tipos de nodos en la misma expansión.
- Al añadir nodos de almacenamiento, debes planificar cuidadosamente el número y la ubicación de los nuevos nodos. Consulta ["Directrices para agregar capacidad de objetos"](#).
- Si la opción **Establecer valor predeterminado del nuevo nodo** está configurada como **No fiable** en la pestaña «Redes de clientes no fiables» de la página de control del cortafuegos, las aplicaciones cliente que se conectan a los nodos de expansión mediante la red de clientes deben conectarse usando un

puerto de punto final del equilibrador de carga (**Configuración > Seguridad > Control del cortafuegos**). Consulta las instrucciones para ["modificar la configuración de seguridad del nuevo nodo"](#) y para ["Configura los endpoints del balanceador de carga"](#).

Guía para añadir un nuevo sitio en StorageGRID

Puedes ampliar tu sistema StorageGRID añadiendo un nuevo sitio.

Instrucciones para añadir un sitio

Antes de añadir un sitio, revisa los siguientes requisitos y limitaciones:

- Solo puedes añadir un sitio por operación de ampliación.
- No puedes añadir nodos de grid a un sitio ya existente como parte de la misma ampliación.
- Todas las ubicaciones deben incluir al menos tres Storage Nodes.
- Añadir un nuevo sitio no aumenta automáticamente el número de objetos que puedes almacenar. La capacidad total de objetos de una grid depende de la cantidad de almacenamiento disponible, la política de ILM y la capacidad de metadatos en cada sitio.
- A la hora de dimensionar un nuevo sitio, debes asegurarte de que cuente con suficiente capacidad para metadatos.

StorageGRID guarda una copia de todos los metadatos de objetos en cada sitio. Cuando agregues un nuevo sitio, debes asegurarte de que incluya suficiente capacidad de metadatos para los metadatos de objetos existentes y suficiente capacidad de metadatos para el crecimiento.

Para obtener más información, consulta lo siguiente:

- ["Gestiona el almacenamiento de metadatos de objetos"](#)
- ["Supervisa la capacidad de metadatos de objetos para cada Storage Node"](#)
- Debes tener en cuenta el ancho de banda de red disponible entre los sitios y la latencia de red. Las actualizaciones de metadatos se replican de forma continua entre los sitios, incluso si todos los objetos se almacenan únicamente en el sitio en el que se ingieren.
- Como tu sistema StorageGRID sigue operativo durante la ampliación, debes revisar las reglas de ILM antes de iniciar el procedimiento de ampliación. Debes asegurarte de que no se almacenen copias de objetos en el nuevo sitio hasta que el procedimiento de ampliación esté completo.

Por ejemplo, antes de comenzar la expansión, determina si alguna regla utiliza el pool de almacenamiento predeterminado (All Storage Nodes). Si es así, debes crear un nuevo pool de almacenamiento que contenga los nodos de almacenamiento existentes y actualizar tus reglas de ILM para usar el nuevo pool de almacenamiento. De lo contrario, los objetos se copiarán en el nuevo sitio tan pronto como el primer nodo de ese sitio se active.

Para obtener más información sobre cómo cambiar el ILM al añadir un nuevo sitio, consulta la ["Ejemplo de cómo modificar una política de ILM"](#).

Prepárate para ampliar tu sistema StorageGRID

Antes de llevar a cabo una operación de ampliación, reúne los materiales e instala y configura cualquier nuevo hardware y redes.

Artículo	Notas
Archivo de instalación de StorageGRID	Si vas a añadir nuevos nodos de grid o un nuevo sitio, debes descargar y extraer el archivo de instalación de StorageGRID. Debes usar la misma versión que se esté ejecutando actualmente en el grid. Para obtener más detalles, consulta las instrucciones de descargar y descomprimir los archivos de instalación de StorageGRID. Nota: No es necesario descargar archivos si vas a añadir nuevos volúmenes de almacenamiento a nodos de almacenamiento ya existentes o si vas a instalar un nuevo dispositivo StorageGRID.
Portátil de servicio	El ordenador portátil de servicio cuenta con 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 grid desde la línea de comandos. Incluido en el paquete de recuperación.
Contraseña de aprovisionamiento	La frase de contraseña se crea y se documenta al instalar el sistema StorageGRID por primera vez. La frase de contraseña de aprovisionamiento no está en el archivo Passwords.txt.
Documentación de StorageGRID	• "Administrar StorageGRID" • "Notas de publicación". Debes iniciar sesión con tu cuenta de NetApp o crear una cuenta para acceder a las notas de la versión. • "Instrucciones de instalación para tu plataforma"
Documentación actual para tu plataforma	Para conocer las versiones compatibles, consulta "Herramienta de matriz de interoperabilidad (IMT)" .

Descarga y descomprime los archivos de instalación de StorageGRID

[[descargar y extraer los archivos de instalación]]

Antes de poder añadir nuevos nodos de grid o un nuevo sitio, debes descargar el archivo de instalación de StorageGRID correspondiente y descomprimir los archivos.

Acerca de esta tarea

Debes realizar las operaciones de expansión utilizando la versión de StorageGRID que se esté ejecutando actualmente en la grid.

Pasos

1. Ve a ["Descargas de NetApp: StorageGRID"](#).
2. Selecciona la versión de StorageGRID que se está ejecutando actualmente en el grid.
3. Inicia sesión con el nombre de usuario y la contraseña de tu cuenta de NetApp.

- Lee el Acuerdo de licencia de usuario final, marca la casilla de verificación y luego selecciona **Aceptar y continuar**.
- En la columna **Instalar StorageGRID** de la página de descargas, selecciona el archivo .tgz o .zip correspondiente a tu plataforma.

La versión que figura en el archivo de instalación debe coincidir con la versión del software que está instalada actualmente.

Utiliza el archivo .zip si el portátil de servicio está ejecutando Windows.

Plataforma	Archivo de instalación
RHEL	StorageGRID-Webscale-version-RPM-uniqueID.zip StorageGRID-Webscale-version-RPM-uniqueID.tgz
Ubuntu o Debian o dispositivos preconfigurados	StorageGRID-Webscale-version-DEB-uniqueID.zip StorageGRID-Webscale-version-DEB-uniqueID.tgz
VMware	StorageGRID-Webscale-version-VMware-uniqueID.zip StorageGRID-Webscale-version-VMware-uniqueID.tgz
OpenStack/otro hipervisor	Para ampliar una implementación existente en OpenStack, debes implementar una máquina virtual que ejecute una de las distribuciones de Linux compatibles indicadas anteriormente y seguir las instrucciones correspondientes para Linux.

- Descarga y descomprime el archivo comprimido.
- Sigue el paso correspondiente a tu plataforma para elegir los archivos que necesitas, según tu plataforma, la topología de grid planificada y cómo vas a expandir tu sistema StorageGRID.

Las rutas que figuran en el paso correspondiente a cada plataforma son relativas al directorio de nivel superior instalado por el archivo comprimido.

- Si vas a ampliar un sistema RHEL, selecciona los archivos correspondientes.

Ruta y nombre del archivo	Descripción
	Un archivo de texto que describe todos los archivos que contiene el archivo de descarga de StorageGRID.
	Una licencia gratuita que no da derecho a ningún tipo de asistencia técnica para el producto.
	Paquete RPM para instalar las imágenes de los nodos de StorageGRID en tus hosts RHEL.
	Paquete RPM para instalar el servicio de host de StorageGRID en tus hosts RHEL.

Ruta y nombre del archivo	Descripción
Herramienta de creación de scripts de implementación	Descripción
	Un script de Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Un script en Python que se utiliza para automatizar la configuración de los appliances StorageGRID.
	Un archivo de configuración de ejemplo para usar con el script <code>configure-storagegrid.py</code> .
	Un script de Python de ejemplo que puedes usar para iniciar sesión en la Grid Management API cuando el inicio de sesión único está habilitado. También puedes usar este script para la integración con Ping Federate.
	Un archivo de configuración en blanco para usar con el script <code>configure-storagegrid.py</code> .
	Ejemplo de rol y playbook de Ansible para configurar hosts de RHEL para el despliegue de contenedores de StorageGRID. Puedes personalizar el rol o el playbook según sea necesario.
	Un script de ejemplo en Python que puedes utilizar para iniciar sesión en la API de gestión de la red cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script auxiliar llamado por el script de Python compañero <code>storagegrid-ssoauth-azure.py</code> para realizar interacciones de inicio de sesión único con Azure.
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puedes utilizar estos esquemas para confirmar que cualquier código que hayas escrito para utilizar las API de gestión de StorageGRID será compatible con la nueva versión de StorageGRID si no tienes un entorno de StorageGRID que no sea de producción para pruebas de compatibilidad con la actualización.

1. Si vas a ampliar un sistema Ubuntu o Debian, selecciona los archivos correspondientes.

Ruta y nombre del archivo	Descripción
	Un archivo de texto que describe todos los archivos que contiene el archivo de descarga de StorageGRID.
	Un archivo de licencia de NetApp que no es de producción y que puedes utilizar para pruebas e implementaciones de prueba de concepto.
	Paquete DEB para instalar las imágenes de los nodos de 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 de StorageGRID en hosts con Ubuntu o Debian.
Herramienta de creación de scripts de implementación	Descripción
	Un script de Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Un script en Python que se utiliza para automatizar la configuración de los appliances StorageGRID.
	Un script de Python de ejemplo que puedes usar para iniciar sesión en la Grid Management API cuando el inicio de sesión único está habilitado. También puedes usar este script para la integración con Ping Federate.
	Un archivo de configuración de ejemplo para usar con el script <code>configure-storagegrid.py</code> .
	Un archivo de configuración en blanco para usar con el script <code>configure-storagegrid.py</code> .
	Ejemplo de rol y playbook de Ansible para configurar hosts de Ubuntu o Debian para el despliegue de contenedores de StorageGRID. Puedes personalizar el rol o el playbook según sea necesario.

Ruta y nombre del archivo	Descripción
	Un script de ejemplo en Python que puedes utilizar para iniciar sesión en la API de gestión de la red cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script auxiliar llamado por el script de Python compañero <code>storagegrid-ssoauth-azure.py</code> para realizar interacciones de inicio de sesión único con Azure.
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puedes utilizar estos esquemas para confirmar que cualquier código que hayas escrito para utilizar las API de gestión de StorageGRID será compatible con la nueva versión de StorageGRID si no tienes un entorno de StorageGRID que no sea de producción para pruebas de compatibilidad con la actualización.

1. Si vas a ampliar un sistema VMware, selecciona los archivos correspondientes.

Ruta y nombre del archivo	Descripción
	Un archivo de texto que describe todos los archivos que contiene el archivo de descarga de StorageGRID.
	Una licencia gratuita que no da derecho a ningún tipo de asistencia técnica para el producto.
	El archivo de disco de la máquina virtual que se utiliza como plantilla para crear máquinas virtuales de nodos de grid.
	El archivo de plantilla de Open Virtualization Format (.ovf) y el archivo de manifiesto (.mf) para implementar el nodo de administración primario.
	El archivo de plantilla (.ovf) y el archivo de manifiesto (.mf) para implementar nodos de administración no principales.
	El archivo de plantilla (.ovf) y el archivo de manifiesto (.mf) para implementar Gateway Nodes.

Ruta y nombre del archivo	Descripción
	El archivo de plantilla (.ovf) y el archivo de manifiesto (.mf) para desplegar nodos de almacenamiento basados en máquinas virtuales.
Herramienta de creación de scripts de implementación	Descripción
	Un script de Bash que se usa para automatizar el despliegue de nodos de grid virtuales.
	Un archivo de configuración de ejemplo para usarlo con el script <code>deploy-vsphere-ovftool.sh</code> .
	Un script de Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Un script en Python que se utiliza para automatizar la configuración de los appliances StorageGRID.
	Un script de ejemplo en Python que puedes utilizar para iniciar sesión en la API de gestión de la red cuando está habilitado el inicio de sesión único (SSO). También puedes utilizar este script para la integración con Ping Federate.
	Un archivo de configuración de ejemplo para usar con el script <code>configure-storagegrid.py</code> .
	Un archivo de configuración en blanco para usar con el script <code>configure-storagegrid.py</code> .
	Un script de ejemplo en Python que puedes utilizar para iniciar sesión en la API de gestión de la red cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script auxiliar llamado por el script de Python compañero <code>storagegrid-ssoauth-azure.py</code> para realizar interacciones de inicio de sesión único con Azure.

Ruta y nombre del archivo	Descripción
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puedes utilizar estos esquemas para confirmar que cualquier código que hayas escrito para utilizar las API de gestión de StorageGRID será compatible con la nueva versión de StorageGRID si no tienes un entorno de StorageGRID que no sea de producción para pruebas de compatibilidad con la actualización.

1. Si vas a ampliar un sistema basado en dispositivos StorageGRID, selecciona los archivos correspondientes.



Para la instalación del dispositivo, estos archivos solo son necesarios si necesitas evitar el tráfico de red. El dispositivo puede descargar los archivos necesarios desde el nodo de administración donde realizas el procedimiento de recuperación.

Ruta y nombre del archivo	Descripción
	Paquete DEB para instalar las imágenes de los nodos de StorageGRID en tus dispositivos.
	Suma de comprobación MD5 para el archivo <code>/debs/storagegridwebscale-images-version-SHA.deb</code> .

Verifica el hardware y la red

Antes de comenzar la ampliación de tu sistema StorageGRID, asegúrate de lo siguiente:

- Se ha instalado y configurado el hardware necesario para dar soporte a los nuevos nodos de grid o al nuevo sitio.
- Todos los nodos nuevos tienen rutas de comunicación bidireccional con todos los nodos existentes y nuevos (un requisito para la red de grid). En particular, confirma que los siguientes puertos TCP estén abiertos entre los nuevos nodos que estás añadiendo en la expansión y el nodo de administración principal:
 - 1055
 - 7443
 - 8011
 - 10342

Consulta ["Comunicaciones internas entre nodos de grid"](#).

- El nodo de administración principal puede comunicarse con todos los servidores de expansión destinados a alojar el sistema StorageGRID.
- Si alguno de los nuevos nodos tiene una dirección IP de la Grid Network en una subred que no se haya utilizado antes, ya la has ["añadiste la nueva subred"](#) a la lista de subredes de la Grid Network. De lo

contrario, tendrás que cancelar la expansión, añadir la nueva subred y volver a iniciar el procedimiento.

- No estás utilizando la traducción de direcciones de red (NAT) en la Grid Network entre los nodos de la cuadrícula o entre los sitios de StorageGRID. Cuando utilizas direcciones IPv4 privadas para la Grid Network, esas direcciones deben ser directamente enrutables desde cada nodo de la cuadrícula en cada sitio. El uso de NAT para conectar la Grid Network a través de un segmento de red pública solo se admite si utilizas una aplicación de túnel que sea transparente para todos los nodos de la cuadrícula, lo que significa que los nodos de la cuadrícula no necesitan conocer las direcciones IP públicas.

Esta restricción de NAT es específica de los nodos de grid y de la Grid Network. Si es necesario, puedes utilizar NAT entre clientes externos y nodos de grid, por ejemplo, para proporcionar una dirección IP pública a un Gateway Node.

Agregar nodos de grid o sitio

Resumen del flujo de trabajo para añadir nodos de grid o nuevos sitios a StorageGRID

Sigue este procedimiento para añadir nodos de grid a sitios existentes o para añadir un sitio nuevo. Solo puedes realizar un tipo de expansión a la vez.

Antes de empezar

- Tienes el ["Acceso root o permiso de mantenimiento"](#).
- Todos los nodos existentes en la grid están en funcionamiento en todos los sitios.
- Cualquier procedimiento previo de ampliación, actualización, decomisionar o recuperación ya está completo.



No puedes iniciar una expansión mientras haya otra expansión, actualización, recuperación o procedimiento de decomisionado activo en curso. Sin embargo, si es necesario, puedes pausar un procedimiento de decomisionado para iniciar una expansión.

Pasos

1. ["Actualizar las subredes de la red Grid"](#).
2. ["Implementa los nuevos nodos de la red"](#).
3. ["Realiza la expansión"](#).

Agrega o actualiza subredes a la Grid Network para expansión en StorageGRID

Al añadir nodos de grid o un nuevo sitio en una ampliación, es posible que tengas que actualizar o añadir subredes a la Grid Network.

StorageGRID mantiene una lista de las subredes utilizadas para la comunicación entre los nodos de la red Grid (eth0). Estas entradas incluyen las subredes que utiliza cada sitio de tu sistema StorageGRID para la red Grid, así como cualquier subred utilizada para NTP, DNS, LDAP u otros servidores externos a los que se accede a través de la pasarela de la red Grid.

Antes de empezar

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

- Tienes el "[Permiso de mantenimiento o acceso de usuario raíz](#)".
- Tienes la frase de contraseña de aprovisionamiento.
- Dispones de las direcciones de red, en notación CIDR, de las subredes que desees configurar.

Acerca de esta tarea

Si alguno de los nuevos nodos tiene una dirección IP de la red Grid en una subred que no se haya utilizado anteriormente, debes añadir la nueva subred a la lista de subredes de la red Grid antes de iniciar la ampliación. De lo contrario, tendrás que cancelar la ampliación, añadir la nueva subred y volver a iniciar el procedimiento.



No utilices subredes que contengan las siguientes direcciones IPv4 para la Grid Network, Admin Network o Client Network de ningún nodo:

- 192.168.130.101
- 192.168.130.121
- 192.168.131.101
- 192.168.131.121
- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 198.51.100.2
- 198.51.100.4

Por ejemplo, no utilices los siguientes rangos de subred para la Grid Network, Admin Network o Client Network 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. Selecciona **Mantenimiento > Red > Red de grid**.
2. Selecciona **Add another subnet** para añadir una nueva subred en notación CIDR.

Por ejemplo, escribe 10.96.104.0/22.

3. Introduce la contraseña de aprovisionamiento y selecciona **Guardar**.
4. Espera a que se apliquen los cambios y luego descarga un nuevo paquete de recuperación.
 - a. Selecciona **Mantenimiento > Sistema > Paquete de recuperación**.
 - b. Introduce la **frase de contraseña de aprovisionamiento**.



Debes proteger el archivo del paquete de recuperación porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID. También se utiliza para recuperar el nodo de administración primario.

Las subredes que has especificado se configuran automáticamente para tu sistema StorageGRID.

Implementar nuevos nodos de grid en StorageGRID

Los pasos para implementar nuevos nodos de red en una ampliación son los mismos que los utilizados cuando se instaló la red por primera vez. Debes implementar todos los nuevos nodos de red antes de poder llevar a cabo la ampliación.

Cuando expandes un grid, los nodos que añades no tienen que coincidir con los tipos de nodos existentes. Puedes añadir nodos de VMware, nodos basados en contenedores de Linux o nodos de appliance.

VMware: implementar nodos de grid

Debes implementar una máquina virtual en VMware vSphere para cada nodo de VMware que desees añadir en la ampliación.

Pasos

1. ["Implementa el nuevo nodo como máquina virtual"](#) y conéctalo a una o más redes de StorageGRID.

Cuando implementas el nodo, puedes opcionalmente reasignar los puertos del nodo o aumentar la configuración de CPU o memoria.

2. Una vez que hayas implementado todos los nuevos nodos de VMware, ["llevar a cabo el procedimiento de expansión"](#).

Linux: implementa nodos de red

Puedes implementar nodos de grid en nuevos hosts Linux o en hosts Linux ya existentes. Si necesitas hosts Linux adicionales para satisfacer los requisitos de CPU, RAM y almacenamiento de los nodos de StorageGRID que quieres añadir a tu grid, debes prepararlos de la misma forma en que preparaste los hosts cuando los instalaste por primera vez. Luego, implementas los nodos de expansión de la misma forma en que implementaste los nodos de grid durante la instalación.

Antes de empezar

- Tienes las instrucciones para instalar StorageGRID en tu versión de Linux y has revisado la ["Requisitos de hardware y almacenamiento"](#).
- Si planeas implementar nuevos nodos de grid en los hosts existentes, ya confirmaste que los hosts tienen suficiente CPU, RAM y capacidad de almacenamiento para los nodos adicionales.
- Tienes un plan para minimizar los dominios de fallo. Por ejemplo, no debes implementar todos los Gateway Nodes en un único host físico.



En una implementación de producción, no ejecutes más de un Storage Node en un solo host físico o virtual. Usar un host dedicado para cada Storage Node proporciona un dominio de fallo aislado.

- Si el nodo de StorageGRID utiliza almacenamiento asignado desde un sistema NetApp ONTAP, comprueba que el volumen no tenga una política de nivelación de FabricPool habilitada. Desactivar la

nivelación de FabricPool para los volúmenes usados con nodos de StorageGRID simplifica la solución de problemas y las operaciones de almacenamiento.

Pasos

1. Si vas a añadir nuevos hosts, consulta las instrucciones de instalación para implementar nodos de StorageGRID.
2. Para implementar los nuevos hosts, sigue las instrucciones para prepararlos.
3. Para crear los archivos de configuración de los nodos y validar la configuración de StorageGRID, sigue las instrucciones para implementar los nodos de la red.
4. Si vas a añadir nodos a un nuevo host Linux, inicia el servicio de StorageGRID.
5. Si vas a añadir nodos a un host de Linux ya existente, inicia los nuevos nodos usando la CLI del servicio `storagegrid host:sudo storagegrid node start [<node name>]`

Después de que termines

Una vez implementados todos los nuevos nodos de la red, puedes ["realizar la expansión"](#).

Dispositivos: implementación de almacenamiento, gateway o nodos de administración no principales

Para instalar el software StorageGRID en un nodo de dispositivo, usas el StorageGRID Appliance Installer, que viene 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 nodo de administración no primario. Cualquier dispositivo se puede conectar a la red de grid, a la red de administración y a la red de clientes.

Antes de empezar

- El dispositivo se ha instalado en un rack o armario, se ha conectado a tus redes y se ha encendido.
- Has completado los ["Configurar el hardware"](#) pasos.

La configuración del hardware del dispositivo incluye los pasos necesarios para configurar las conexiones de StorageGRID (enlaces de red y direcciones IP), así como los pasos opcionales para habilitar el cifrado de nodo, 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 StorageGRID Appliance Installer se han definido en la Grid Network Subnet List del nodo de administración principal.
- El firmware del StorageGRID Appliance Installer en el dispositivo de reemplazo es compatible con la versión del software StorageGRID que está ejecutándose actualmente en tu grid. Si las versiones no son compatibles, tienes que actualizar el firmware del StorageGRID Appliance Installer.
- Tienes un portátil de servicio con un ["navegador web compatible"](#).
- Conoces una de las direcciones IP asignadas al controlador de computación del dispositivo. Puedes usar la dirección IP para cualquier red de StorageGRID conectada.

Acerca de esta tarea

El proceso de instalación de StorageGRID en un nodo de dispositivo consta de las siguientes fases:

- Debes especificar o confirmar la dirección IP del nodo de administración principal y el nombre del nodo de la appliance.
- Inicia la instalación y espera a que se configuren los volúmenes y se instale el software.

A mitad de las tareas de instalación de los dispositivos, la instalación se detiene. Para reanudar la instalación, debes iniciar sesión en Grid Manager, aprobar todos los nodos de la grid y completar el

proceso de instalación de StorageGRID.



Si necesitas implementar varios nodos de appliance a la vez, puedes automatizar el proceso de instalación utilizando el `configure-sga.py` script de instalación de appliances.

Pasos

1. Abre un navegador e introduce una de las direcciones IP del controlador de cómputo del appliance.

```
https://Controller_IP:8443
```

Aparece la página de inicio del instalador de StorageGRID Appliance.

2. En la sección de conexión del **Nodo de administración principal**, comprueba si necesitas especificar la dirección IP del nodo de administración principal.

Si ya has instalado otros nodos en este centro de datos, el instalador de StorageGRID Appliance puede detectar esta dirección IP automáticamente, siempre que el nodo de administración principal, o al menos otro nodo de grid con ADMIN_IP configurado, esté presente en la misma subred.

3. Si esta dirección IP no aparece o necesitas cambiarla, indica la dirección:

Opción	Descripción
Introducción manual de la dirección IP	a. Desmarca la casilla Habilitar detección de nodos de administración. b. Introduce la dirección IP manualmente. c. Haz clic en Guardar. d. Espera a que el estado de conexión de la nueva dirección IP esté listo.
Detección automática de todos los nodos de administración principales conectados	a. Marca la casilla Habilitar detección de nodos de administración. b. Espera a que aparezca la lista de direcciones IP detectadas. c. Selecciona el nodo de administración principal del grid donde se va a implementar este nodo de almacenamiento del appliance. d. Haz clic en Guardar. e. Espera a que el estado de conexión de la nueva dirección IP esté listo.

4. En el campo **Nombre de nodo**, introduce el nombre que quieras utilizar para este nodo del appliance y selecciona **Guardar**.

El nombre de nodo se asigna a este nodo del dispositivo en el sistema StorageGRID. Aparece en la página Nodos (pestaña Resumen) en Grid Manager. Si lo necesitas, puedes cambiar el nombre cuando apruebes el nodo.

5. En la sección **Instalación**, comprueba que el estado actual sea «Listo para iniciar la instalación de *nombre de nodo* en la grid 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 debas cambiar la configuración de red o los ajustes de puerto. Para obtener instrucciones, consulta las instrucciones de mantenimiento de tu dispositivo.

6. En la página de inicio del instalador de StorageGRID Appliance, selecciona **Iniciar instalación**.

El estado actual cambia a «Instalación en curso» y se muestra la página «Supervisar la instalación».

7. Si tu ampliación incluye varios nodos de appliance, repite los pasos anteriores para cada appliance.



Si necesitas implementar varios nodos de almacenamiento appliance a la vez, puedes automatizar el proceso de instalación utilizando el script de instalación appliance configure-sga.py.

8. Si necesitas acceder manualmente a la página **Monitor Installation**, selecciona **Monitor Installation** en la barra de menús.

La página de instalación del monitor muestra el progreso de la instalación.

La barra de estado azul indica qué tarea está actualmente en progreso. Las barras de estado verdes indican las tareas que se han completado correctamente.



El instalador se asegura de que las tareas completadas en una instalación anterior no se vuelvan a ejecutar. Si vuelves a ejecutar una instalación, las tareas que no necesiten volver a ejecutarse se muestran con una barra de estado verde y el estado "Skipped".

9. Revisa el avance de las dos primeras fases de la instalación.

1. Configura el dispositivo

Durante esta etapa, ocurre 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 los volúmenes y configura la configuración del host.
- En el caso de un dispositivo de servicios, el instalador borra cualquier configuración existente de las unidades del controlador de cálculo y configura los ajustes del host.

2. Instala el sistema operativo

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

10. Sigue supervisando el progreso de la instalación hasta que aparezca un mensaje en la ventana de la consola en el que se te pida que utilices el Grid Manager para aprobar el nodo.



Espera hasta que todos los nodos que añadiste en esta ampliación estén listos para su aprobación antes de ir al Grid Manager para aprobar los nodos.

Realiza una ampliación de StorageGRID

Al llevar a cabo la ampliación, los nuevos nodos de la red se añaden a tu implementación actual de StorageGRID.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes la frase de contraseña de aprovisionamiento.
- Ya has implementado todos los nodos de la red que se añaden en esta ampliación.
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- Si vas a añadir nodos de almacenamiento, asegúrate de que todas las operaciones de reparación de datos realizadas como parte de una recuperación estén completas. Consulta ["Comprobar los trabajos de reparación de datos"](#).
- Si estás añadiendo nodos de almacenamiento y quieres asignarles un grado de almacenamiento personalizado, ya has ["creaste el nivel de almacenamiento personalizado"](#). También tienes el permiso de acceso Root o bien los permisos de Maintenance e ILM.
- Si vas a añadir un nuevo sitio, ya habrás revisado y actualizado las reglas de ILM. Debes asegurarte de que las copias de los objetos no se almacenen en el nuevo sitio hasta que se haya completado la expansión. Por ejemplo, si una regla utiliza el grupo de almacenamiento predeterminado (**Todos los nodos de almacenamiento**), debes ["crear un nuevo grupo de almacenamiento"](#) que contenga únicamente los nodos de almacenamiento existentes y ["Actualizar las reglas de ILM"](#) y la política de ILM para usar ese nuevo grupo de almacenamiento. De lo contrario, los objetos se copiarán al nuevo sitio tan pronto como el primer nodo de dicho sitio se active.

Acerca de esta tarea

Realizar la ampliación incluye estas tareas principales para el usuario:

1. Configura la ampliación.
2. Inicia la expansión.
3. Descarga un nuevo archivo del paquete de recuperación.
4. Supervisa los pasos y las fases de la expansión hasta que todos los nuevos nodos estén instalados y configurados y todos los servicios se hayan iniciado.



Algunos pasos y fases de la expansión pueden tardar bastante tiempo en completarse en una grid de gran tamaño. Por ejemplo, hacer streaming de Cassandra a un nuevo Storage Node puede tardar solo unos minutos si la base de datos de Cassandra está vacía. Sin embargo, si la base de datos de Cassandra contiene una gran cantidad de metadatos de objetos, esta fase puede tardar varias horas o incluso más. No reinicies ningún Storage Node durante las etapas "Expanding the Cassandra cluster" o "Starting Cassandra and streaming data".

Pasos

1. Selecciona **Mantenimiento > Tareas > Ampliación**.

Aparece la página «Ampliación de la red». En la sección «Nodos pendientes» se muestran los nodos que están listos para ser añadidos.

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

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
00:50:56:a7:7a:c0	rlco-010-096-106-151	Storage Node	VMware VM	10.96.106.151/22
00:50:56:a7:0f:2e	rlco-010-096-106-156	API Gateway Node	VMware VM	10.96.106.156/22

2. Selecciona **Configurar expansión**.

Aparece el cuadro de diálogo «Selección de ubicación».

3. Selecciona el tipo de ampliación que vas a iniciar:

- Si vas a añadir un nuevo sitio, selecciona **Nuevo** e introduce el nombre del nuevo sitio.
- Si vas a añadir uno o más nodos a un sitio ya existente, selecciona **Existente**.

4. Selecciona **Guardar**.

5. Revisa la lista **Nodos pendientes** y comprueba que aparecen todos los nodos de grid que has implementado.

Si lo deseas, puedes situar el cursor sobre la **Grid Network MAC Address** de un nodo para ver los detalles de dicho 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, confirma que se haya implementado correctamente.

6. En la lista de nodos pendientes, aprueba los nodos que quieras añadir en esta ampliación.
- a. Selecciona el botón de opción situado junto al primer nodo de grid pendiente que quieras aprobar.
 - b. Selecciona **Approve**.
- Aparece el formulario de configuración del nodo de la red.
- c. Modifica la configuración general según sea necesario:

Campo	Descripción
Sitio	El nombre del sitio con el que se asociará el nodo de grid. Si vas a añadir varios nodos, asegúrate de seleccionar el sitio correcto para cada nodo. Si vas a añadir un nuevo sitio, todos los nodos se añadirán al nuevo sitio.
Nombre	El nombre del sistema del nodo. Los nombres de los sistemas 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 de objetos y metadatos • Solo datos: Nodo de almacenamiento que contiene únicamente datos de objetos (sin metadatos) • Solo metadatos: Nodo de almacenamiento que contiene únicamente metadatos (sin datos de objetos)

Campo	Descripción
Función de NTP	La función de Protocolo de tiempo de red (NTP) del nodo de grid: • Selecciona Automático (predeterminado) para asignar automáticamente el rol NTP al nodo. El rol primario se asignará a los nodos de administración, los nodos de almacenamiento con servicios ADC, los nodos de puerta de enlace y cualquier nodo de grid que tenga direcciones IP no estáticas. El rol de cliente se asignará a todos los demás nodos de grid. • Selecciona Primary para asignar manualmente el rol de NTP primario al nodo. Al menos dos nodos en cada sitio deben tener el rol primario para proporcionar acceso redundante del sistema a fuentes de sincronización externas. • Selecciona Client para asignar manualmente la función NTP de Client al nodo.
Servicio ADC (nodos de almacenamiento combinados o solo de metadatos)	Si este nodo de almacenamiento ejecutará 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 grid. Al menos tres nodos de almacenamiento de cada sitio deben incluir el servicio ADC. • Selecciona Sí si el nodo de almacenamiento que vas a sustituir incluye el servicio ADC. Como no puedes decomisionar un nodo de almacenamiento si quedaran muy pocos servicios ADC, este ajuste garantiza que haya un nuevo servicio ADC disponible antes de que se elimine el servicio antiguo. • Puedes "trasladar el servicio ADC a otro Storage Node en el mismo sitio" para garantizar que se cumpla el quórum del servicio ADC. • Selecciona Automático para que el sistema determine si este nodo necesita el servicio ADC. Aprende sobre "Quórum del ADC".
Nivel de almacenamiento (nodos de almacenamiento combinados o solo de datos)	Utiliza el nivel de almacenamiento Predeterminado o selecciona el nivel de almacenamiento personalizado que desees asignar a este nuevo nodo. Los niveles de almacenamiento son utilizados por los grupos de almacenamiento de ILM, así que tu elección puede influir en qué objetos se colocarán en el Storage Node.

d. Según sea necesario, modifica la configuración de la Grid Network, Admin Network y Client Network.

- **Dirección IPv4 (CIDR):** La dirección de red CIDR de la interfaz de red. Por ejemplo:
172.16.10.100/24



Si, mientras apruebas los nodos, detectas que algunos de ellos tienen direcciones IP duplicadas en la Grid Network, debes cancelar la expansión, volver a implementar las máquinas virtuales o los appliances con una dirección IP que no esté 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 varias subredes para la red de administración.

e. Selecciona **Guardar**.

El nodo de la red aprobado pasa a la lista de nodos aprobados.

- Para modificar las propiedades de un nodo de grid aprobado, selecciona su botón de opción y selecciona **Editar**.
- Para mover un nodo de la red aprobado de nuevo a la lista de Nodos pendientes, selecciona su botón de opción y selecciona **Restablecer**.
- Para eliminar definitivamente un nodo de red aprobado, apaga el nodo. Luego, selecciona su botón de opción y selecciona **Remove**.

f. Repite estos pasos para cada nodo de grid pendiente que quieras aprobar.



Si es posible, deberías aprobar todos los nodos de la cuadrícula pendientes y realizar una única expansión. Llevará más tiempo si realizas varias expansiones pequeñas.

7. Cuando hayas aprobado todos los nodos de la grid, introduce la **Provisioning Passphrase** y selecciona **Expand**.

Al cabo de unos minutos, esta página se actualiza para mostrar el estado del procedimiento de expansión. Cuando hay tareas en curso que afectan a nodos individuales del grid, la sección Estado de los nodos del grid muestra el estado actual de cada nodo del grid.



Durante el paso «Instalación de nodos de la red» de un nuevo appliance, el StorageGRID Appliance Installer muestra que la instalación pasa de la etapa 3 a la etapa 4, Finalizar instalación. Cuando finaliza la etapa 4, el controller se reinicia.



La ampliación de un sitio incluye una tarea adicional para configurar Cassandra para el nuevo sitio.

8. En cuanto aparezca el enlace **Descargar paquete de recuperación**, descarga el archivo del paquete de recuperación.

Debes descargar una copia actualizada del archivo del paquete de recuperación lo antes posible después de realizar cambios en la topología de la cuadrícula en el sistema StorageGRID. El archivo del paquete de recuperación te permite restaurar el sistema si se produce un fallo.

- Selecciona el enlace de descarga.
- Introduce la contraseña de aprovisionamiento y selecciona **Iniciar descarga**.
- Cuando finalice la descarga, abre el .zip archivo y comprueba que puedes acceder a su contenido, incluido el `Passwords.txt` archivo.

- d. Copia el archivo del paquete de recuperación descargado (.zip en dos ubicaciones seguras y distintas.



El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

9. Si vas a añadir nodos de almacenamiento a un sitio ya existente o vas a añadir un sitio, supervisa las fases de Cassandra, que ocurren cuando se inician los servicios en los nuevos nodos de la grid.



No reinicies ningún nodo de almacenamiento durante las fases «Expanding the Cassandra cluster» o «Starting Cassandra and streaming data». Estas fases 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 vas a añadir nodos de almacenamiento a un sitio ya existente, revisa el porcentaje que aparece en el mensaje de estado "Starting Cassandra and streaming data".

Este porcentaje estima qué tan completa está la operación de transmisión de Cassandra, basándose en la cantidad total de datos de Cassandra disponibles y en la cantidad que ya se ha escrito en el nuevo nodo.

Agregar sitio

Si vas a añadir un nuevo sitio, utiliza `nodetool status` para supervisar el progreso de la transmisión de Cassandra y ver cuántos metadatos se han copiado al nuevo sitio durante la etapa "Expanding the Cassandra cluster". La carga total de datos en el nuevo sitio debe estar dentro de aproximadamente un 20% del total de un sitio actual.

10. Sigue supervisando la ampliación hasta que se hayan completado todas las tareas y vuelva a aparecer el botón **Configure Expansion**.

Después de que termines

Dependiendo de los tipos de nodos de red que hayas añadido, realiza los pasos adicionales de integración y configuración. Consulta ["Pasos de configuración tras la ampliación"](#).

Agregar volúmenes de almacenamiento

Agrega volúmenes de almacenamiento a tu sistema StorageGRID

Puedes ampliar la capacidad de almacenamiento de los nodos de almacenamiento que estén por debajo del número máximo de volúmenes admitido. Es posible que tengas que añadir volúmenes de almacenamiento a más de un nodo de almacenamiento para cumplir con los requisitos de ILM para las copias replicadas o con codificación de borrado.

Antes de empezar

Antes de añadir volúmenes de almacenamiento, revisa ["Directrices para añadir capacidad de objetos"](#) para asegurarte de que sabes dónde añadir volúmenes para cumplir con los requisitos de tu política de ILM.



Estas instrucciones se aplican únicamente a los nodos de almacenamiento basados en software. Consulta ["Agregar bandeja de expansión a SG6060 desplegado"](#) o ["Agregar bandeja de expansión a SG6160 desplegado"](#) para saber cómo añadir volúmenes de almacenamiento a SG6060 o SG6160 mediante la instalación de bandejas de expansión. Otros nodos de almacenamiento de appliance no se pueden ampliar.

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 basado en bloques que el sistema StorageGRID formatea y monta para almacenar objetos. Cada nodo de almacenamiento puede admitir hasta 48 volúmenes de almacenamiento, que en el Grid Manager se llaman *object stores*.



Los metadatos de los objetos se almacenan siempre en el almacén de objetos 0.

Cada almacén de objetos se monta en un volumen que corresponde a su ID. Por ejemplo, el almacén de objetos con un ID de 0000 corresponde al punto de montaje `/var/local/rangedb/0`.

Antes de añadir nuevos volúmenes de almacenamiento, usa el Grid Manager para ver los almacenes de objetos actuales de cada Storage Node, así como los puntos de montaje correspondientes. Puedes usar esta información al añadir volúmenes de almacenamiento.

Pasos

1. Selecciona **Nodes > site > Storage Node > Storage**.
2. Desplázate hacia abajo para ver las cantidades de almacenamiento disponibles para cada volumen y almacén de objetos.

En el caso de los nodos de almacenamiento del dispositivo, el nombre global de cada disco coincide con el identificador global del volumen (WWID) que aparece al consultar las propiedades estándar del volumen en SANtricity OS (el software de gestión conectado al controlador de almacenamiento del dispositivo).

Para ayudarte a interpretar las estadísticas de lectura y escritura del disco relacionadas con los puntos de montaje de los volúmenes, la primera parte del nombre que aparece en la columna **Nombre** de la tabla «Dispositivos de disco» (es decir, *sdc*, *sdd*, *sde*, y así sucesivamente) coincide con el valor que aparece 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. Sigue las instrucciones para tu plataforma para añadir nuevos volúmenes de almacenamiento al nodo de almacenamiento.
 - ["VMware: agrega volúmenes de almacenamiento al nodo de almacenamiento"](#)
 - ["Linux: Añade volúmenes conectados directamente o de SAN al nodo de almacenamiento"](#)

Agrega volúmenes de almacenamiento a los nodos de almacenamiento de VMware en StorageGRID

Si un nodo de almacenamiento incluye menos de 16 volúmenes de almacenamiento, puedes aumentar su capacidad utilizando VMware vSphere para añadir volúmenes.

Antes de empezar

- Tienes acceso a ["Instrucciones para instalar StorageGRID en entornos de VMware"](#).
- Tienes el archivo `Passwords.txt`.
- Tienes ["permisos de acceso específicos"](#).



No intentes añadir volúmenes de almacenamiento a un nodo de almacenamiento mientras una actualización de software, un procedimiento de recuperación u otro procedimiento de expansión esté activo.

Acerca de esta tarea

El nodo de almacenamiento queda indisponible durante un breve periodo de tiempo al añadir volúmenes de almacenamiento. Deberías realizar este procedimiento en un solo nodo de almacenamiento a la vez para evitar afectar los servicios de grid orientados al cliente.

Pasos

1. Si es necesario, instala nuevo hardware de almacenamiento y crea nuevos datastores de VMware.
2. Añade uno o varios discos duros a la máquina virtual para utilizarlos como almacenamiento (object stores).

a. Abre VMware vSphere Client.

b. Modifica la configuración de la máquina virtual para añadir uno o varios discos duros adicionales.

Los discos duros suelen configurarse como discos de máquina virtual (VMDK). Los VMDK son los más habituales y más fáciles de gestionar, mientras que los RDM pueden ofrecer un mejor rendimiento para cargas de trabajo que utilizan objetos de mayor tamaño (por ejemplo, superiores a 100 MB). Para obtener más información sobre cómo añadir discos duros a máquinas virtuales, consulta la documentación de VMware vSphere.

3. Reinicia la máquina virtual utilizando la opción **Reiniciar el sistema operativo invitado** en el cliente VMware vSphere, o introduciendo el siguiente comando en una sesión ssh a la máquina virtual:`sudo reboot`



No utilices **Apagar** o **Restablecer** para reiniciar la máquina virtual.

4. Configura el nuevo almacenamiento para que lo utilice el nodo de almacenamiento:

a. Inicia sesión en el nodo de la grid:

i. Introduce el siguiente comando: `ssh admin@grid_node_IP`

- ii. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- iii. Introduce el siguiente comando para pasar a ser usuario root: `su -`
- iv. Introduce la contraseña que figura en el archivo `Passwords.txt`. Cuando hayas iniciado sesión como root, el indicador de comandos cambia de `$` a `#`.

b. Configura los nuevos volúmenes de almacenamiento:

```
sudo add_rangedbs.rb
```

Este script detecta cualquier volumen de almacenamiento nuevo y te pide que los formatees.

- c. Escribe **y** para aceptar el formato.
- d. Si alguno de los volúmenes se ha formateado anteriormente, decide si quieres volver a formatearlos.
 - Introduce **y** para volver a dar formato.
 - Introduce **n** para omitir el reformato.

El `setup_rangedbs.sh` script se ejecuta automáticamente.

5. Comprueba que los servicios se inicien correctamente:

a. Ver una lista del estado de todos los servicios en el servidor:

```
sudo storagegrid-status
```

El estado se actualiza automáticamente.

- a. Espera hasta que todos los servicios estén en ejecución o verificados.
- b. Salir de la pantalla de estado:

```
Ctrl+C
```

6. Verifica que el nodo de almacenamiento esté en línea:

- a. Inicia sesión en Grid Manager usando una ["navegador web compatible"](#) cuenta.
- b. Selecciona **Nodos > Storage Node > Tareas**.
- c. Si la lista desplegable **Estado de almacenamiento** está configurada en **Solo lectura** o **Sin conexión**, selecciona **En línea**.
- d. Selecciona **Guardar**.

7. Para ver los nuevos almacenes de objetos, selecciona **Storage**.

8. Consulta los detalles en la tabla **Volúmenes**.

Resultado

Puedes utilizar la capacidad ampliada de los nodos de almacenamiento para guardar datos de objetos.

Agrega volúmenes directos o SAN a los nodos de almacenamiento Linux en StorageGRID

Si un nodo de almacenamiento incluye menos de 48 volúmenes de almacenamiento, puedes aumentar su capacidad añadiendo nuevos dispositivos de almacenamiento en

bloque, haciéndolos visibles para los hosts Linux y añadiendo las nuevas asignaciones de dispositivos en bloque al archivo de configuración de StorageGRID utilizado para el nodo de almacenamiento.

Antes de empezar

- Tienes acceso a la ["Instrucciones para instalar StorageGRID"](#) para tu plataforma Linux.
- Tienes el archivo `Passwords.txt`.
- Tienes ["permisos de acceso específicos"](#).



No intentes añadir volúmenes de almacenamiento a un nodo de almacenamiento mientras una actualización de software, un procedimiento de recuperación u otro procedimiento de expansión esté activo.

Acerca de esta tarea

El nodo de almacenamiento queda indisponible durante un breve periodo de tiempo al añadir volúmenes de almacenamiento. Deberías realizar este procedimiento en un solo nodo de almacenamiento a la vez para evitar afectar los servicios de grid orientados al cliente.

Pasos

1. Instala el nuevo hardware de almacenamiento.

Para obtener más información, consulta la documentación proporcionada por tu proveedor de hardware.

2. Crea nuevos volúmenes de almacenamiento en bloque con los tamaños deseados.
 - Conecta las nuevas unidades y actualiza la configuración de la controladora RAID según sea necesario, o asigna los nuevos LUN de la SAN en las matrices de almacenamiento compartido y permite que el host Linux acceda a ellos.
 - Utiliza el mismo esquema de nomenclatura persistente que utilizaste para los volúmenes de almacenamiento del nodo de almacenamiento existente.
 - Si usas la función de migración de nodos de StorageGRID, haz que los nuevos volúmenes sean visibles para otros hosts de Linux que sean destinos de migración para este nodo de almacenamiento. Para obtener más información, consulta las instrucciones de instalación de StorageGRID para tu plataforma Linux.
3. Inicia sesión en el host Linux que soporta el nodo de almacenamiento como root o con una cuenta que tenga permisos sudo.
4. Comprueba que los nuevos volúmenes de almacenamiento sean visibles en el host Linux.

Es posible que tengas que volver a buscar dispositivos.

5. Ejecuta el siguiente comando para desactivar temporalmente el nodo de almacenamiento:

```
sudo storagegrid node stop <node-name>
```

6. Con un editor de texto como vim o pico, edita el archivo de configuración del nodo para el Storage Node, que puedes encontrar en `/etc/storagegrid/nodes/<node-name>.conf`.
7. Localiza la sección del archivo de configuración del nodo que contiene las asignaciones existentes de dispositivos de bloque de almacenamiento de objetos.

En el ejemplo, `BLOCK_DEVICE_RANGEDB_00` a `BLOCK_DEVICE_RANGEDB_03` son las asignaciones

existentes de dispositivos de bloque de almacenamiento de objetos.

```
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. Añade nuevas asignaciones de dispositivos de almacenamiento de objetos en bloque correspondientes a los volúmenes de almacenamiento en bloque que has añadido para este Storage Node.

Asegúrate de empezar en el siguiente `BLOCK_DEVICE_RANGEDB_nn`. No dejes ningún espacio.

- Siguiendo el ejemplo anterior, empieza por `BLOCK_DEVICE_RANGEDB_04`.
- En el ejemplo siguiente, se han añadido 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. Ejecuta el siguiente comando para validar los cambios realizados en el archivo de configuración del nodo de almacenamiento de Storage Node:

```
sudo storagegrid node validate <node-name>
```

Soluciona cualquier error o advertencia antes de pasar al siguiente paso.



Si observas un error similar al siguiente, significa que el archivo de configuración del nodo está intentando asignar el dispositivo de bloques utilizado por <node-name> para <PURPOSE> a la ruta <path-name> en el sistema de archivos de Linux, pero no existe ningún archivo especial de dispositivo de bloques válido (ni ningún enlace simbólico a un archivo especial de dispositivo de bloques) en esa ubicación.

```
Checking configuration file for node <node-name>...  
ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>  
<path-name> is not a valid block device
```

Comprueba que has introducido correctamente <path-name>.

10. Ejecuta el siguiente comando para reiniciar el nodo con las nuevas asignaciones de dispositivos de bloque ya aplicadas:

```
sudo storagegrid node start <node-name>
```

11. Inicia sesión en el nodo de almacenamiento como admin con la contraseña que aparece en el archivo `Passwords.txt`.

12. Comprueba que los servicios se inicien correctamente:

- a. Ver una lista del estado de todos los servicios del servidor:

```
sudo storagegrid-status
```

El estado se actualiza automáticamente.

- b. Espera hasta que todos los servicios estén en ejecución o verificados.

- c. Salir de la pantalla de estado:

```
Ctrl+C
```

13. Configura el nuevo almacenamiento para que lo utilice el nodo de almacenamiento:

- a. Configura los nuevos volúmenes de almacenamiento:

```
sudo add_rangedbs.rb
```

Este script detecta cualquier volumen de almacenamiento nuevo y te pide que los formatees.

- b. Introduce **y** para formatear los volúmenes de almacenamiento.

- c. Si alguno de los volúmenes se ha formateado anteriormente, decide si quieres volver a formatearlos.

- Introduce **y** para volver a dar formato.
- Introduce **n** para omitir el reformateo.

El `setup_rangedbs.sh` script se ejecuta automáticamente.

14. Comprueba que el estado de almacenamiento del nodo de almacenamiento esté en línea:
 - a. Inicia sesión en Grid Manager usando una ["navegador web compatible"](#) cuenta.
 - b. Selecciona **Nodos > Storage Node > Tareas**.
 - c. Si la lista desplegable **Estado de almacenamiento** está configurada en **Solo lectura** o **Sin conexión**, selecciona **En línea**.
 - d. Selecciona **Guardar**.
15. Para ver los nuevos almacenes de objetos, selecciona **Storage**.
16. Consulta los detalles en la tabla **Volúmenes**.

Resultado

Ahora puedes utilizar la mayor capacidad de los Storage Nodes para guardar datos de objetos.

Configura el sistema ampliado

Configura los nodos y sitios recién añadidos en StorageGRID

Una vez completada una ampliación, debes llevar a cabo pasos adicionales de integración y configuración.

Acerca de esta tarea

Debes completar las tareas de configuración que se enumeran a continuación para los nodos de red o los sitios que vayas añadiendo en tu ampliación. Algunas tareas pueden ser opcionales, dependiendo de las opciones seleccionadas al instalar y administrar tu sistema, y de cómo quieras configurar los nodos y sitios añadidos durante la ampliación.

Pasos

1. Si has añadido un sitio:
 - ["Crear un grupo de almacenamiento"](#) para el sitio y cada grado de almacenamiento que seleccionaste para los nuevos Storage Nodes.
 - Confirma que la política de ILM cumple con los nuevos requisitos. Si es necesario cambiar las reglas, ["crear nuevas reglas"](#) y ["actualizar la política de ILM"](#). Si las reglas ya son correctas, ["activar una nueva política"](#) sin cambiar ninguna regla para asegurarte de que StorageGRID use los nuevos nodos.
 - Comprueba que se pueda acceder a los servidores NTP desde ese sitio. Consulta ["Gestionar servidores NTP"](#).



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

2. Si has añadido uno o varios nodos de almacenamiento a un sitio ya existente:
 - ["Ver detalles del grupo de almacenamiento"](#) para comprobar que cada nodo que añadiste esté incluido en los grupos de almacenamiento esperados y se use en las reglas de ILM esperadas.
 - Confirma que la política de ILM cumple con los nuevos requisitos. Si es necesario cambiar las reglas, ["crear nuevas reglas"](#) y ["actualizar la política de ILM"](#). Si las reglas ya son correctas, ["activar una](#)

nueva política" sin cambiar ninguna regla para asegurarte de que StorageGRID use los nuevos nodos.

- ["Comprueba que el nodo de almacenamiento esté activo"](#) y capaz de ingerir objetos.
- Si no has podido añadir el número recomendado de nodos de almacenamiento, reequilibra los datos con código de borrado. Consulta ["Reequilibra los datos con código de borrado después de añadir Storage Nodes"](#).

3. Si añadiste un nodo de puerta de enlace:

- Si se utilizan grupos de alta disponibilidad (HA) para las conexiones de clientes, de forma opcional puedes añadir el nodo de puerta de enlace a un grupo de HA. Selecciona **Configuración > Red > Grupos de alta disponibilidad** para revisar la lista de grupos de HA existentes y añadir el nuevo nodo. Consulta ["Configurar grupos de alta disponibilidad"](#).

4. Si has añadido un nodo de administración:

- a. Si el inicio de sesión único (SSO) está habilitado para tu sistema StorageGRID, crea una relación de confianza de parte dependiente para el nuevo nodo de administración. No podrás iniciar sesión en el nodo hasta que crees esta relación de confianza de parte dependiente. Consulta ["Configura el inicio de sesión único"](#).
- b. Si planeas usar el servicio Load Balancer en los nodos de administración, opcionalmente puedes añadir el nuevo nodo de administración a un grupo de alta disponibilidad. Selecciona **Configuración > Red > Grupos de alta disponibilidad** para revisar la lista de grupos de alta disponibilidad existentes y añadir el nuevo nodo. Consulta ["Configurar grupos de alta disponibilidad"](#).
- c. Opcionalmente, copia la base de datos del nodo de administración desde el nodo de administración primario al nodo de administración de expansión si quieres mantener la coherencia de la información de atributos y auditoría en cada nodo de administración. Consulta ["Copia la base de datos del nodo de administración"](#).
- d. Si lo deseas, copia la base de datos de Prometheus del nodo de administración principal al nodo de administración de expansión si quieres mantener la coherencia de las métricas históricas en cada nodo de administración. Consulta ["Copiar métricas de Prometheus"](#).
- e. Si lo deseas, copia los registros de auditoría existentes del nodo de administración principal al nodo de administración de expansión si quieres mantener la coherencia de la información histórica de los registros en cada nodo de administración. Consulta ["Copiar los registros de auditoría"](#).

5. Para comprobar si se han añadido nodos de expansión con una Client Network no fiable o para cambiar si la Client Network de un nodo es no fiable o fiable, ve a **Configuración > Seguridad > Control de cortafuegos**.

Si la red de clientes en el nodo de expansión no es de confianza, debes realizar las conexiones al nodo en la red de clientes mediante un endpoint de equilibrador de carga. Consulta ["Configura los puntos de conexión del equilibrador de carga"](#) y ["Gestiona los controles del cortafuegos"](#).

6. Configura el DNS.

Si has estado configurando los ajustes de DNS por separado para cada nodo de la red, debes añadir ajustes de DNS personalizados por nodo para los nuevos nodos. Consulta ["Modificar la configuración de DNS para un único nodo de la red"](#).

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

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

Comprueba que los nodos de almacenamiento estén activos tras una ampliación de StorageGRID

Una vez completada la operación de expansión que añade nuevos nodos de almacenamiento, el sistema StorageGRID debería empezar a utilizar los nuevos nodos de almacenamiento de forma automática. Debes usar el sistema StorageGRID para verificar que el nuevo nodo de almacenamiento está activo.

Pasos

1. Inicia sesión en Grid Manager usando una ["navegador web compatible"](#) cuenta.
2. Selecciona **Nodos > Nodo de almacenamiento de expansión > Almacenamiento**.
3. Coloca el cursor sobre el gráfico **Espacio utilizado - Datos de objetos** para ver el valor de **Utilizado**, que es la cantidad de espacio total utilizable que se ha usado para los datos de objetos.
4. Comprueba que el valor de **Usado** vaya aumentando a medida que desplazas el cursor hacia la derecha en el gráfico.

Copia la base de datos del nodo de administración a los nuevos nodos de administración en StorageGRID

Al añadir nodos de administración mediante un procedimiento de ampliación, puedes optar por copiar la base de datos del nodo de administración principal al nuevo nodo de administración. Copiar la base de datos te permite conservar información histórica sobre atributos y alertas.

Antes de empezar

- Ya has completado los pasos de ampliación necesarios para añadir un Admin Node.
- Tienes el archivo `Passwords.txt`.
- Tienes la frase de 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 sobre los servidores y servicios que forman parte del sistema actualmente o que se agreguen más adelante. Esta base de datos del nodo de administración incluye la siguiente información:

- Historial de alertas
- Datos históricos de atributos, que se usan en los gráficos de estilo clásico en la página Nodes

Para garantizar que la base de datos del nodo de administración sea coherente entre los nodos, puedes copiar la base de datos del nodo de administración principal al nodo de administración de expansión.



La copia de la base de datos desde el 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 tiempo, el Grid Manager no estará accesible.

Sigue 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. Sigue estos pasos en el nodo de administración principal:

- a. Inicia sesión en el nodo de administración:
 - i. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - iii. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - iv. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- b. Ejecuta el siguiente comando: `recover-access-points`
- c. Introduce la contraseña de aprovisionamiento.
- d. Detén el servicio MI: `service mi stop`
- e. Detén el servicio de la interfaz de programación de aplicaciones de gestión (mgmt-api): `service mgmt-api stop`

2. Completa los siguientes pasos en el nodo Admin de la expansión:

- a. Inicia sesión en el nodo de administración de la expansión:
 - i. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - iii. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - iv. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- b. Detén el servicio MI: `service mi stop`
- c. Detén el servicio API mgmt-api: `service mgmt-api stop`
- d. Añade la clave privada SSH al agente SSH. Introduce: `ssh-add`
- e. Introduce la contraseña de acceso SSH que figura en el archivo `Passwords.txt`.
- f. Copia la base de datos desde el 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 te solicite, confirma que quieres sobrescribir la base de datos MI en el nodo de administración de la expansión.

La base de datos y sus datos históricos se copian en el nodo de administración de la ampliación. Una vez finalizada la operación de copia, el script inicia el nodo de administración de la ampliación.

- h. Cuando ya no necesites acceso sin contraseña a otros servidores, elimina la clave privada del agente SSH. Introduce: `ssh-add -D`

3. Reinicia los servicios en el nodo de administración principal: `service servermanager start`

Copia las métricas de Prometheus a los nuevos nodos de administración en StorageGRID

Después de añadir un nuevo nodo de administración, puedes copiar opcionalmente las

métricas históricas que mantiene Prometheus desde el nodo de administración primario al nuevo nodo de administración. Copiar las métricas garantiza que las métricas históricas sean coherentes entre los nodos de administración.

Antes de empezar

- El nuevo nodo de administración ya está instalado y en funcionamiento.
- Tienes el archivo `Passwords.txt`.
- Tienes la frase de contraseña de aprovisionamiento.

Acerca de esta tarea

Al añadir un nodo de administración, el proceso de instalación del software crea una nueva base de datos de Prometheus. Puedes mantener la coherencia de las métricas históricas entre los nodos copiando la base de datos de Prometheus del nodo de administración principal (el *nodo de administración de origen*) al nuevo nodo de administración.



Copiar la base de datos de Prometheus puede tardar una hora o más. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios estén detenidos en el Admin Node de origen.

Pasos

1. Inicia sesión en el nodo Admin de origen:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.
2. Desde el nodo de administración de origen, detén el servicio Prometheus: `service prometheus stop`
3. Sigue estos pasos en el nuevo Admin Node:
 - a. Inicia sesión en el nuevo nodo de administración:
 - i. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - iii. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - iv. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - b. Detén el servicio Prometheus: `service prometheus stop`
 - c. Añade la clave privada SSH al agente SSH. Introduce: `ssh-add`
 - d. Introduce la contraseña de acceso SSH que figura en el archivo `Passwords.txt`.
 - e. Copia la base de datos de Prometheus desde el 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 te solicite, pulsa **Intro** para confirmar que quieres eliminar 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 Admin Node.

Cuando termina la operación de copia, el script inicia el nuevo Admin Node. Aparece el siguiente estado:

```
Database cloned, starting services
```

- a. Cuando ya no necesites acceso sin contraseña a otros servidores, elimina la clave privada del agente SSH. Introduce:

```
ssh-add -D
```

4. Reinicia el servicio Prometheus en el nodo de administración de origen.

```
service prometheus start
```

Copia los registros de auditoría en los nuevos nodos de administración en StorageGRID

Cuando agregas un nuevo nodo de administración mediante un procedimiento de expansión, su servicio AMS solo registra los eventos y las acciones que ocurren después de que se une al sistema. Si lo necesitas, puedes copiar los registros de auditoría de un nodo de administración instalado previamente en el nuevo nodo de administración de expansión para que esté sincronizado con el resto del sistema StorageGRID.

Antes de empezar

- Ya has completado los pasos de ampliación necesarios para añadir un Admin Node.
- Tienes el archivo `Passwords.txt`.

Acerca de esta tarea

Para que los mensajes de auditoría históricos estén disponibles en un nuevo nodo de administración, debes 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 `localaudit` log en cada nodo. Para usar este procedimiento, debes haber configurado los Admin Nodes como destino de la auditoría de la siguiente manera:



- Has configurado **Nodos de administración/nodos locales** como destino de registro.
- Configuraste **nodos de administración y servidor syslog externo** como destino de los registros.

Consulta "[Configura los mensajes de auditoría y el servidor syslog externo](#)" para obtener más detalles.

Pasos

1. Inicia sesión en el nodo de administración principal:
 - a. Introduce el siguiente comando: `ssh admin@_primary_Admin_Node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`

d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

2. Detén el servicio AMS para evitar que cree un nuevo archivo: `service ams stop`

3. Accede al directorio de exportación de auditorías:

```
cd /var/local/audit/export/
```

4. Cambia el nombre del archivo `audit.log` fuente para asegurarte de que no sobrescriba el archivo en el nodo Admin de expansión al que lo estás copiando:

```
ls -l
mv audit.log _new_name_.txt
```

5. Copia todos los archivos de auditoría en la ubicación de destino del nodo de administración de la expansión:

```
scp -p * IP_address:/var/local/audit/export/
```

6. Si se te solicita la frase de contraseña de `/root/.ssh/id_rsa`, introduce la contraseña de acceso SSH del nodo de administración principal que figura en el archivo `Passwords.txt`.

7. Restaura el archivo original `audit.log`:

```
mv new_name.txt audit.log
```

8. Inicia el servicio AMS:

```
service ams start
```

9. Cerrar sesión en el servidor:

```
exit
```

10. Inicia sesión en el nodo de administración de la expansión:

a. Introduce el siguiente comando: `ssh admin@expansion_Admin_Node_IP`

b. Introduce la contraseña que figura en el archivo `Passwords.txt`.

c. Introduce el siguiente comando para pasar a ser usuario root: `su -`

d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

11. Actualiza la configuración de usuario y grupo para los archivos de registro de auditoría:

```
cd /var/local/audit/export/
```

```
chown ams-user:bycast *
```

12. Cerrar sesión en el servidor:

```
exit
```

Reequilibra los datos con código de borrado tras añadir nodos a tu sistema StorageGRID

Después de añadir los nodos de almacenamiento, puedes usar el procedimiento de reequilibrio de erasure coding (EC) para redistribuir los fragmentos codificados mediante erasure coding entre los nodos de almacenamiento existentes y los nuevos.

Antes de empezar

- Ya has completado los pasos de ampliación para añadir los nuevos nodos de almacenamiento.
- Has revisado la ["consideraciones para el reequilibrio de datos con código de borrado"](#).
- Entiendes que este procedimiento no moverá los datos de objetos replicados y que el procedimiento de reequilibrio de EC no mueve los datos replicados. Sin embargo, los datos replicados se tienen en cuenta al determinar a dónde mover los datos de EC.
- Tienes el archivo `Passwords.txt`.

Qué ocurre cuando se ejecuta este procedimiento

Antes de iniciar el procedimiento, ten 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 estado de error.
- El procedimiento de reequilibrio de EC 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, tanto si el procedimiento falla como si tiene éxito.
- Si un volumen se desconecta mientras se está llevando a cabo el procedimiento de reequilibrio de EC, dicho procedimiento se interrumpirá. Los fragmentos de datos que ya se hayan trasladado permanecerán en sus nuevas ubicaciones y no se perderá ningún dato.

Puedes volver a ejecutar el procedimiento una vez que todos los volúmenes estén de nuevo operativos.

- Cuando se está ejecutando el procedimiento de reequilibrio del 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) podrían fallar durante el procedimiento de reequilibrio de EC si requieren más de 24 horas para completarse. Las operaciones PUT de larga duración fallarán si la regla de ILM aplicable utiliza la ubicación Balanced o Strict en la ingesta. Se notificará el siguiente error: 500 Internal Server Error.

- **Condiciones de finalización de la tarea.** El procedimiento de reequilibrio de EC se considera finalizado cuando se cumple cualquiera de las siguientes condiciones:
 - Ya no puede mover más datos con código de borrado.
 - Los datos de todos los nodos se encuentran dentro de una desviación del 5% respecto a la partición de datos objetivo.

- El procedimiento lleva 30 días en marcha.

Pasos

1. Revisa los detalles actuales del almacenamiento de objetos del sitio que pretendes reequilibrar.
 - a. Selecciona **Nodos**.
 - b. Selecciona el primer nodo de almacenamiento del sitio.
 - c. Selecciona la pestaña **Storage**.
 - d. Coloca el cursor sobre el gráfico «Almacenamiento utilizado - Datos de objetos» para ver la cantidad actual de datos replicados y de datos con código de borrado en el Storage Node.
 - e. Repite estos pasos para ver los demás Storage Nodes en el sitio.
2. Inicia sesión en el nodo de administración principal:
 - a. Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Quando inicias sesión como root, el indicador cambia de \$ a #.

3. Inicia el procedimiento:

```
`rebalance-data start --site "site-name"
```

Para "site-name", especifica el primer sitio en el que añadiste el nuevo Storage Node o nodos. Enciérralo site-name entre comillas.

Se inicia el procedimiento de reequilibrio de EC y se devuelve un job ID.

4. Copia el ID del trabajo.
5. Supervisa el estado del procedimiento de reequilibrio del EC.

- Para consultar el estado de un procedimiento de reequilibrio de EC concreto:

```
rebalance-data status --job-id job-id
```

Para *job-id*, especifica el ID que se devolvió al iniciar el procedimiento.

- Para consultar el estado del procedimiento de reequilibrio de EC en curso y de cualquier procedimiento completado anteriormente:

```
rebalance-data status
```



Para obtener ayuda sobre el comando «rebalance-data»:

```
rebalance-data --help
```

6. Realiza los pasos adicionales en función del estado devuelto:

- Si State es `In progress`, la operación de reequilibrio de EC aún se está ejecutando. Debes

supervisar periódicamente el procedimiento hasta que se complete.

Ve a la página [Nodos](#) para evaluar la distribución de los datos entre los Storage Nodes del sitio.

La tarea de reequilibrio de EC se considerará completada y se detendrá cuando los datos de todos los nodos se encuentren dentro de una desviación del 5 % respecto a la partición de datos objetivo.

- Si `State` es `Success`, opcionalmente [Revisa el almacenamiento de objetos](#) para ver los detalles actualizados del sitio.

Los datos codificados con código de borrado deberían estar ahora más equilibrados entre los nodos de almacenamiento del sitio.

- Si `State` es `Failure`:
 - i. Comprueba que todos los nodos de almacenamiento del sitio estén conectados a la grid.
 - ii. Comprueba y resuelve cualquier alerta que pueda estar afectando a estos Storage Nodes.
 - iii. Reinicia el procedimiento de reequilibrio de EC:

```
rebalance-data start --job-id job-id
```

- iv. [Ver el estado](#) del nuevo procedimiento. Si `State` sigue `Failure`, ponte en contacto con soporte técnico.

7. Si el procedimiento de reequilibrio del EC está generando demasiada carga (por ejemplo, las operaciones de ingesta se ven afectadas), pausa el procedimiento.

```
rebalance-data pause --job-id job-id
```

8. Si necesitas interrumpir el procedimiento de reequilibrio del EC (por ejemplo, para poder realizar una actualización del software de StorageGRID), introduce lo siguiente:

```
rebalance-data terminate --job-id job-id
```



Al finalizar un procedimiento de reequilibrio de EC, los fragmentos de datos que ya se hayan trasladado permanecen en sus nuevas ubicaciones. Los datos no se vuelven a trasladar a su ubicación original.

9. Si estás utilizando el código de borrado en más de un sitio, ejecuta este procedimiento en todos los demás sitios afectados.

Solucionar errores de expansión en StorageGRID

Si durante el proceso de ampliación de la red se producen errores que no puedes resolver, o si falla alguna tarea de la red, recopila los archivos de registro y ponte en contacto con el soporte técnico.

Antes de ponerte en contacto con el soporte técnico, recopila los archivos de registro necesarios para facilitar la resolución del problema.

Pasos

1. El acceso externo por SSH está bloqueado de forma predeterminada. Si es necesario, ["permitir el acceso de forma temporal"](#).

2. Conéctate al nodo de expansión que ha sufrido fallos:

a. Introduce 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 contenedores en el que se ejecuta StorageGRID.

b. Introduce la contraseña que figura en el archivo `Passwords.txt`.

c. Introduce el siguiente comando para pasar a ser usuario root: `su -`

d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Después de que inicies sesión como root, el indicador cambia de `$` a `#`.

3. En función de la fase en la que se encuentre la instalación, recupera cualquiera de los siguientes registros que estén disponibles en el nodo de la grid:

Plataforma	Registros
VMware	• <code>/var/log/daemon.log</code> • <code>/var/log/storagegrid/daemon.log</code> • <code>/var/log/storagegrid/nodes/<node-name>.log</code>
Linux	• <code>/var/log/storagegrid/daemon.log</code> • <code>/etc/storagegrid/nodes/<node-name>.conf</code> (por cada nodo fallido) • <code>/var/log/storagegrid/nodes/<node-name>.log</code> (por cada nodo con errores; podría no existir)

4. Si has permitido el acceso SSH externo, "bloquear el acceso" cuando hayas terminado la tarea.

Mantén un sistema StorageGRID

Mantenimiento de grid de StorageGRID

Las tareas de mantenimiento de la grid incluyen decomisionar un nodo o un sitio, cambiar el nombre de una grid, nodo o sitio, y mantener las redes. También puedes realizar procedimientos de host y middleware y procedimientos de nodos de la grid.



En estas instrucciones, «Linux» hace referencia a una instalación de Red Hat® Enterprise Linux® (RHEL), Ubuntu® o Debian®. Para consultar la lista de versiones compatibles, consulta ["Herramienta NetApp Interoperability Matrix Tool"](#).

Antes de empezar

- Tienes un amplio conocimiento del sistema StorageGRID.
- Has revisado la topología de tu sistema StorageGRID y entiendes la configuración de la grid.
- Entiendes que debes seguir todas las instrucciones exactamente y prestar atención a todas las advertencias.
- Debes entender que los procedimientos de mantenimiento que no se describen no están soportados o requieren la contratación de un servicio.

Procedimientos de mantenimiento para los appliances

Para los procedimientos de hardware, consulta la ["Instrucciones de mantenimiento para tu StorageGRID appliance"](#).

Descarga el paquete de recuperación StorageGRID

El archivo del paquete de recuperación te permite restaurar el sistema StorageGRID en caso de que se produzca un fallo.

Antes de empezar

- Desde cualquier nodo de administración, inicias sesión en Grid Manager usando una ["navegador web compatible"](#).
- Tienes la frase de contraseña de aprovisionamiento.
- Tienes ["permisos de acceso específicos"](#).

Descarga el archivo del paquete de recuperación actual antes de realizar cambios en la topología de la grid del sistema StorageGRID o antes de actualizar el software. Luego, descarga una nueva copia del paquete de recuperación después de hacer cambios en la topología de la grid o después de actualizar el software.

Pasos

1. Selecciona **Mantenimiento > Sistema > Paquete de recuperación**.
2. Introduce la contraseña de aprovisionamiento y selecciona **Iniciar descarga**.

La descarga comienza de inmediato.

3. Cuando finalice la descarga, abre el `.zip` archivo y comprueba que puedes acceder a su contenido, incluido el `Passwords.txt` archivo.
4. Copia el archivo del paquete de recuperación descargado (`.zip` en dos ubicaciones seguras y distintas.



El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

Decomisionar nodos o sitio

Decomisionar un nodo o sitio de StorageGRID

Puedes llevar a cabo un procedimiento de decomisionar para eliminar de forma permanente nodos de la red o una sede completa del sistema StorageGRID.

Para eliminar un nodo de la red o una instalación, realiza uno de los siguientes procedimientos de decomisionar:

- Realiza una **"decomisionar nodo de la red"** para eliminar uno o varios nodos, que pueden estar en uno o varios sitios. Los nodos que elimines pueden estar en línea y conectados al sistema StorageGRID, o pueden estar fuera de línea y desconectados.
- Realiza un **"decomisionar el sitio"** para eliminar un sitio. Realiza una **decomisión de sitio conectado** si todos los nodos están conectados a StorageGRID. Realiza una **decomisión de sitio desconectado** si todos los nodos están desconectados de StorageGRID. Si el sitio contiene una combinación de nodos conectados y desconectados, debes volver a poner en línea todos los nodos que estén fuera de línea.



Antes de descomisionar un sitio desconectado, ponte en contacto con tu representante de cuenta de NetApp. NetApp revisará tus requisitos antes de habilitar todos los pasos del asistente de descomisionamiento de sitios. No debes intentar descomisionar un sitio desconectado si crees que podría ser posible recuperar el sitio o recuperar los datos de objetos del sitio.

Antes de decomisionar un nodo de grid, debes confirmar que no hay trabajos de reparación de datos activos. Si alguna reparación ha fallado, debes reiniciarla y dejar que termine antes de realizar el procedimiento de decomisionamiento. Consulta **"Comprobar los trabajos de reparación de datos"**.

Decomisionar nodos

Decomisionar un nodo de grid de StorageGRID

Puedes usar el procedimiento de decomisionar nodos para eliminar uno o más nodos de la grid en uno o más sitios. No puedes decomisionar el nodo de administración principal.

Cuándo decomisionar un nodo

Utiliza el procedimiento de decomisionar el nodo cuando se cumpla alguna de las siguientes condiciones:

- Has añadido un nodo de almacenamiento más grande en una ampliación y quieres eliminar uno o varios nodos de almacenamiento más pequeños, conservando al mismo tiempo los objetos.



Si quieres sustituir un dispositivo antiguo por uno más nuevo, plantéate ["clonación del nodo del appliance"](#) en lugar de añadir un nuevo dispositivo en una ampliación y luego decomisionar el dispositivo antiguo.

- Necesitas menos espacio de almacenamiento en total.
- Ya no necesitas un nodo de puerta de enlace.
- Ya no necesitas un nodo de administración secundario.
- Tu grid incluye un nodo desconectado que no puedes recuperar ni volver a poner en línea.
- Tu grid incluye un Archive Node.

Cómo decomisionar un nodo

Puedes decomisionar nodos de grid conectados o nodos de grid desconectados.

Decomisionar los nodos conectados

En general, solo debes decomisionar nodos de la red cuando estén conectados al sistema StorageGRID y solo cuando todos los nodos se encuentren en buen estado (con iconos verdes en las páginas **Nodos** y en la página **Decomisionar nodos**).

Para ver las instrucciones, consulta ["Decomisionar los nodos conectados a la red"](#).

Decomisionar los nodos desconectados

En algunos casos, es posible que tengas que decomisionar un nodo de la red que no esté conectado actualmente a la red (uno cuyo estado sea Desconocido o Administrativamente inactivo).

Para ver las instrucciones, consulta ["Decomisionar nodos de grid desconectados"](#).

Qué hay que tener en cuenta antes de decomisionar un nodo

Antes de realizar cualquiera de los dos procedimientos, revisa las consideraciones para cada tipo de nodo:

- ["Aspectos a tener en cuenta para decomisionar un nodo de administración o de pasarela"](#)
- ["Aspectos a tener en cuenta para decomisionar un nodo de almacenamiento"](#)

Consideraciones para decomisionar un nodo Admin o Gateway de StorageGRID

Revisa las consideraciones para decomisionar un nodo de administración o un nodo de gateway.

Aspectos a tener en cuenta para el nodo de administración

- No puedes decomisionar el nodo de administración principal.
- No puedes decomisionar un nodo de administración si una de sus interfaces de red forma parte de un grupo de alta disponibilidad (HA). Primero debes eliminar las interfaces de red del grupo de alta disponibilidad. Consulta las instrucciones para ["gestión de grupos de alta disponibilidad"](#).
- Si es necesario, puedes modificar con total seguridad las políticas de ILM mientras decomisionas un nodo de administración.
- Si descomisionas un nodo de administración y tienes habilitado el inicio de sesión único (SSO) en tu sistema StorageGRID, debes acordarte de eliminar la confianza de parte dependiente de dicho nodo en Active Directory Federation Services (AD FS).

- Si utilizas ["federación de grid"](#), asegúrate de que la dirección IP del nodo que vas a descomisionar no se haya especificado para una conexión de federación de grid.
- Al decomisionar un nodo de administración desconectado, perderás los registros de auditoría de ese nodo; sin embargo, estos registros también deberían existir en el nodo de administración principal.

Consideraciones para el nodo de puerta de enlace

- No puedes decomisionar un nodo Gateway si una de sus interfaces de red forma parte de un grupo de alta disponibilidad (HA). Primero debes eliminar las interfaces de red del grupo HA. Consulta las instrucciones para ["gestión de grupos de alta disponibilidad"](#).
- Si es necesario, puedes modificar con total seguridad las políticas de ILM mientras decomisionas un nodo de puerta de enlace.
- Si utilizas ["federación de grid"](#), asegúrate de que la dirección IP del nodo que vas a descomisionar no se haya especificado para una conexión de federación de grid.
- Puedes decomisionar un Gateway Node de forma segura mientras está desconectado.

Aspectos a tener en cuenta para los nodos de almacenamiento

Consideraciones para decomisionar un Storage Node en StorageGRID

Antes de decomisionar un nodo de almacenamiento, plantéate si puedes clonarlo en su lugar. Luego, si decides decomisionar el nodo, revisa cómo StorageGRID gestiona los objetos y los metadatos durante el procedimiento de decomisionamiento.

Cuándo clonar un nodo en lugar de descomisionarlo

Si deseas sustituir un nodo de almacenamiento de appliance antiguo por uno de appliance más nuevo o de mayor capacidad, considera clonar el nodo de appliance en lugar de añadir un nuevo appliance en una ampliación y luego decomisionar el appliance antiguo.

La clonación de nodos de appliance te permite sustituir fácilmente un nodo de appliance existente por un appliance compatible en el mismo sitio de StorageGRID. El proceso de clonación transfiere todos los datos al nuevo appliance, pone en servicio el nuevo appliance y deja el antiguo en un estado previo a la instalación.

Puedes clonar un nodo de dispositivo si necesitas:

- Sustituye un appliance que está llegando al final de su vida útil.
- Actualiza un nodo existente para aprovechar la tecnología mejorada del dispositivo.
- Aumenta la capacidad de almacenamiento en grid sin cambiar el número de Storage Nodes en tu sistema StorageGRID.
- Mejora la eficiencia del almacenamiento, como cambiando el modo RAID.

Consulta ["Clonación de nodos de appliance"](#) para más detalles.

Aspectos a tener en cuenta en los nodos de almacenamiento conectados

Revisa las consideraciones para decomisionar un nodo de almacenamiento conectado.

- No debes decomisionar más de 10 Storage Nodes en un solo procedimiento de Decommission Node.
- El sistema debe contar, en todo momento, con suficientes nodos de almacenamiento para satisfacer los

requisitos operativos, incluidos el ["Quórum del ADC"](#) y el ["Política de ILM"](#) activo. Para cumplir esta restricción, es posible que tengas que añadir un nuevo nodo de almacenamiento en una operación de ampliación antes de poder decomisionar un nodo de almacenamiento existente.

Actúa con precaución al decomisionar nodos de almacenamiento en una grid que contenga nodos basados en software destinados exclusivamente a metadatos. Si decomisionas todos los nodos configurados para almacenar *tanto* objetos como metadatos, la capacidad de almacenar objetos se elimina de la grid. Consulta ["Tipos de nodos de almacenamiento"](#) para obtener más información sobre los nodos de almacenamiento destinados exclusivamente a metadatos.

- Al eliminar un nodo de almacenamiento, se transfieren grandes volúmenes de datos de objetos a través de la red. Aunque estas transferencias no deberían afectar el funcionamiento normal del sistema, pueden influir en la cantidad total de ancho de banda de red que consume el sistema StorageGRID.
- Las tareas relacionadas con el proceso de decomisionar un nodo de almacenamiento tienen una prioridad menor que las tareas relacionadas con el funcionamiento normal del sistema. Esto significa que decomisionar no interfiere con el funcionamiento normal del sistema StorageGRID y no es necesario programarlo para un periodo de inactividad del sistema. Dado que decomisionar se realiza en segundo plano, es difícil estimar cuánto tiempo tomará completar el proceso. En general, decomisionar termina más rápido cuando el sistema está tranquilo o si solo se retira un nodo de almacenamiento a la vez.
- Podría tardar días o semanas en decomisionar un nodo de almacenamiento. Planifica este procedimiento en consecuencia. Aunque el proceso de decomisionar está diseñado para no afectar las operaciones del sistema, puede limitar otros procedimientos. En general, deberías realizar cualquier actualización o expansión planificada del sistema antes de eliminar nodos del grid.
- Si necesitas realizar otro procedimiento de mantenimiento mientras se están eliminando los nodos de almacenamiento, puedes ["pausar el procedimiento de decomisionar"](#) y reanudarlo una vez que el otro procedimiento haya finalizado.



El botón **Pausa** solo está disponible cuando se llega a las fases de evaluación de ILM o de decomisionamiento de datos con código de borrado; sin embargo, la evaluación de ILM (migración de datos) seguirá ejecutándose en segundo plano.

- No puedes ejecutar operaciones de reparación de datos en ningún nodo de la grid mientras se está ejecutando una tarea de decomisionar.
- No debes realizar ningún cambio en una política de ILM mientras se está descomisionando un nodo de almacenamiento.
- Para eliminar los datos de forma permanente y segura, debes borrar las unidades del Storage Node después de que se complete el procedimiento de decomisionar.

Consideraciones para los nodos de almacenamiento desconectados

Revisa las consideraciones para decomisionar un nodo de almacenamiento desconectado.

- Nunca descomisiones un nodo desconectado a menos que estés seguro de que no se puede volver a poner en línea ni recuperar.



No realices este procedimiento si crees que podría ser posible recuperar los datos de objetos del nodo. En su lugar, ponte en contacto con soporte técnico para determinar si la recuperación del nodo es posible.

- Cuando decomisionas 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 decomisionas más de un nodo de almacenamiento desconectado. Es posible que el sistema no pueda reconstruir los datos si no quedan disponibles suficientes copias de objetos, fragmentos con código de borrado o metadatos de los objetos. Cuando decomisionas nodos de almacenamiento en un grid con nodos basados en software solo para metadatos, decomisionar todos los nodos configurados para almacenar tanto objetos como metadatos elimina todo el almacenamiento de objetos del grid. Consulta ["Tipos de nodos de almacenamiento"](#) para más información sobre los nodos de almacenamiento solo para metadatos.



Si tienes más de un nodo de almacenamiento desconectado que no puedes recuperar, ponte en contacto con soporte técnico para determinar cuál es la mejor forma de proceder.

- Cuando decomisionas un nodo de almacenamiento desconectado, StorageGRID inicia tareas de reparación de datos al final del proceso de decomisionamiento. Estas tareas intentan reconstruir los datos de los objetos y los metadatos que estaban almacenados en el nodo desconectado.
- Cuando decomisionas un nodo de almacenamiento desconectado, el procedimiento de decomisionado se completa con relativa rapidez. Sin embargo, los trabajos de reparación de datos pueden tardar días o semanas en ejecutarse y no son supervisados por el procedimiento de decomisionado. Debes supervisar manualmente estos trabajos y reiniciarlos cuando sea necesario. Consulta ["Comprobar los trabajos de reparación de datos"](#).
- Si decomisionas un nodo de almacenamiento desconectado que contiene la única copia de un objeto, el objeto se perderá. Las tareas de reparación de datos solo pueden reconstruir y recuperar objetos si existe al menos una copia replicada o suficientes fragmentos con código de borrado en nodos de almacenamiento que estén conectados en ese momento.

¿Qué es el quórum de StorageGRID ADC?

Es posible que no puedas decomisionar ciertos nodos de almacenamiento en un sitio si, después de la descomisión, quedarían muy pocos servicios de Administrative Domain Controller (ADC).

El servicio ADC, presente en algunos nodos de almacenamiento, gestiona la información sobre la topología de la grid y proporciona servicios de configuración a la grid. El sistema StorageGRID requiere que haya un quórum de servicios ADC disponibles en cada sitio y en todo momento.

No se puede descomisionar un nodo de almacenamiento si, al eliminarlo, se dejara de cumplir el quórum del ADC. Para cumplir el quórum del ADC durante el proceso de descomisionamiento, debe haber un mínimo de tres nodos de almacenamiento en cada sitio que cuenten con el servicio ADC. Si un sitio cuenta con más de tres nodos de almacenamiento con el servicio ADC, una mayoría simple de dichos nodos debe permanecer disponible tras el proceso de descomisionamiento: $((0.5 * \text{Storage Nodes with ADC}) + 1)$



Actúa con precaución al decomisionar nodos de almacenamiento en una grid que contenga nodos basados en software destinados exclusivamente a metadatos. Si decomisionas todos los nodos configurados para almacenar *tanto* objetos como metadatos, la capacidad de almacenar objetos se elimina de la grid. Consulta ["Tipos de nodos de almacenamiento"](#) para obtener más información sobre los nodos de almacenamiento destinados exclusivamente a metadatos.

Por ejemplo, supongamos que un sitio cuenta actualmente con seis nodos de almacenamiento con servicios ADC y que quieres decomisionar tres nodos de almacenamiento. Debido al requisito de quórum de ADC, debes completar dos procedimientos de decomisionamiento, como sigue:

- En el primer procedimiento de decomisionar, debes asegurarte de que sigan estando disponibles cuatro nodos de almacenamiento con servicios ADC: $((0.5 * 6) + 1)$. Esto significa que solo puedes decomisionar dos nodos de almacenamiento inicialmente.
- En el segundo procedimiento de decomisionar, puedes eliminar el tercer Storage Node porque el quórum del ADC ahora solo requiere que permanezcan disponibles tres servicios de ADC: $((0.5 * 4) + 1)$.

Si necesitas decomisionar un Nodo de Almacenamiento, puedes continuar cumpliendo con el requisito de quórum del ADC "[Mover el servicio ADC a otro nodo de almacenamiento en el mismo sitio](#)" o agregando un nuevo Nodo de Almacenamiento en un "[expansión](#)" y especificando que debe tener un servicio de ADC. Luego, puedes decomisionar el Nodo de Almacenamiento existente sin afectar el quórum.

Revisa la política ILM de StorageGRID y la configuración de almacenamiento

Si tienes previsto decomisionar un nodo de almacenamiento, deberías revisar la política de ILM de tu sistema StorageGRID antes de empezar el proceso de decomisionamiento.

Durante el proceso de descomisionamiento, todos los datos de los objetos se migran desde el nodo de almacenamiento descomisionado a otros nodos de almacenamiento.



La política de ILM que tengas *durante* el decomisionado será la que se utilice *después* del decomisionado. Debes asegurarte de que esta política cumpla con tus requisitos de datos tanto antes de iniciar el decomisionado como una vez finalizado este.

Debes revisar las reglas en cada "[política de ILM activa](#)" para asegurarte de que el sistema StorageGRID seguirá teniendo suficiente capacidad del tipo correcto y en las ubicaciones correctas para acomodar el decomisionado de un Storage Node.

Ten en cuenta lo siguiente:

- ¿Será posible que los servicios de evaluación de ILM copien los datos de los objetos de tal forma que se cumplan las reglas de ILM?
- ¿Qué ocurre si un emplazamiento queda temporalmente fuera de servicio mientras se lleva a cabo el proceso de decomisionar? ¿Se pueden realizar copias adicionales en una ubicación alternativa?
- ¿Cómo afectará el proceso de decomisionar a la distribución final del contenido? Como se describe en "[Consolidar nodos de almacenamiento](#)", debes "[agrega nuevos nodos de almacenamiento](#)" antes de decomisionar los antiguos. Si agregas un nodo de almacenamiento de reemplazo más grande después de decomisionar un nodo de almacenamiento más pequeño, los nodos de almacenamiento antiguos podrían estar casi al límite de su capacidad de almacenamiento y el nuevo nodo de almacenamiento podría no tener casi ningún contenido. La mayoría de las operaciones de escritura para nuevos datos de objetos se dirigirían entonces al nuevo nodo de almacenamiento, reduciendo la eficiencia general de las operaciones del sistema.
- ¿Contará el sistema, en todo momento, con suficientes nodos de almacenamiento para cumplir con las políticas de ILM activas?



Una política de ILM que no se pueda cumplir provocará atascos y alertas, y podría interrumpir el funcionamiento del sistema StorageGRID.

Comprueba que la topología propuesta que resultará del proceso de decomisionar cumpla con la política de ILM evaluando las áreas que figuran en la tabla.

Área a evaluar	Aspectos a tener en cuenta
Capacidad disponible	¿Habr� suficiente capacidad de almacenamiento para albergar todos los datos de objetos almacenados en el sistema StorageGRID, incluidas las copias permanentes de los datos de objetos que actualmente se encuentran almacenados en el nodo de almacenamiento que se va a decomisionar? ¿Habr� capacidad suficiente para gestionar el crecimiento previsto de los datos de objetos almacenados durante un periodo de tiempo razonable despu�s de que se haya completado el proceso de decomisionar?
Ubicaci�n del almacenamiento	Si queda suficiente capacidad en el sistema StorageGRID en su conjunto, � se encuentra esa capacidad en las ubicaciones adecuadas para cumplir las reglas de negocio del sistema StorageGRID?
Tipo de almacenamiento	� Habr� suficiente capacidad de almacenamiento del tipo adecuado una vez que se haya completado el proceso de decomisionar? Por ejemplo, las reglas de ILM pueden trasladar contenido de un tipo de almacenamiento a otro a medida que este va envejeciendo. En este caso, debes asegurarte de que haya suficiente almacenamiento del tipo adecuado disponible en la configuraci�n final del sistema StorageGRID.

Consolida los nodos de almacenamiento StorageGRID

Puedes consolidar nodos de almacenamiento para reducir el n mero de nodos de almacenamiento de un sitio o una implementaci n mientras aumentas la capacidad de almacenamiento.

Cuando consolidas nodos de almacenamiento, "[ampliar el sistema StorageGRID](#)" a ades nuevos nodos de almacenamiento de mayor capacidad y luego decomisionas los antiguos nodos de almacenamiento de menor capacidad. Durante el procedimiento de decomisionar, los objetos se migran de los antiguos nodos de almacenamiento a los nuevos.



Si est s consolidando appliances antiguos y m s peque os con modelos nuevos o appliances de mayor capacidad, considera "[clonaci n del nodo del appliance](#)" (o usa la clonaci n de nodos de appliances y el procedimiento de decomisionar si no est s haciendo un reemplazo uno a uno).

Por ejemplo, podr as a adir dos nuevos nodos de almacenamiento de mayor capacidad para sustituir tres nodos de almacenamiento antiguos. Primero usar as el procedimiento de ampliaci n para a adir los dos nuevos nodos de almacenamiento de mayor capacidad y luego usar as el procedimiento de decomisionar para eliminar los tres nodos de almacenamiento antiguos de menor capacidad.

Al a adir nueva capacidad antes de eliminar los nodos de almacenamiento existentes, aseguras una distribuci n m s equilibrada de los datos en todo el sistema StorageGRID. Tambi n reduces la posibilidad de que un nodo de almacenamiento existente supere el nivel de marca de agua de almacenamiento.

Decomisionar varios nodos de almacenamiento StorageGRID

Si necesitas eliminar más de un nodo de almacenamiento, puedes decomisionarlos de forma secuencial o en paralelo.



Actúa con precaución al decomisionar nodos de almacenamiento en una grid que contenga nodos basados en software destinados exclusivamente a metadatos. Si decomisionas todos los nodos configurados para almacenar *tanto* objetos como metadatos, la capacidad de almacenar objetos se elimina de la grid. Consulta "[Tipos de nodos de almacenamiento](#)" para obtener más información sobre los nodos de almacenamiento destinados exclusivamente a metadatos.

- Si descomisionas los nodos de almacenamiento de forma secuencial, debes esperar a que el primer nodo de almacenamiento haya finalizado el proceso de decomisionar antes de empezar a decomisionar el siguiente nodo de almacenamiento.
- Si decomisionas los nodos de almacenamiento en paralelo, los nodos de almacenamiento procesan simultáneamente las tareas de decomisionar para todos los nodos de almacenamiento que se están decomisionando. Esto puede resultar en una situación donde todas las copias permanentes de un archivo se marquen como "solo lectura", deshabilitando temporalmente la eliminación en los grids donde esta funcionalidad está habilitada.

Revisa los trabajos de reparación de datos en StorageGRID

Antes de decomisionar o ampliar un nodo de la red, debes asegurarte de que no haya ninguna tarea de reparación de datos en curso. Si alguna reparación ha fallado, debes reiniciarla y esperar a que se complete antes de realizar el procedimiento de decomisionar.

Consulta "[Tipos de expansión](#)" para obtener más información sobre cómo ampliar un nodo de la cuadrícula.

Acerca de esta tarea

Si necesitas decomisionar un nodo de almacenamiento desconectado, sigue estos pasos una vez finalizado el procedimiento de decomisionar para asegurarte de que la tarea de reparación de datos se ha completado. Debes asegurarte de que se hayan restaurado todos los fragmentos con código de borrado que estaban en el nodo retirado.

Estos pasos solo se aplican a los sistemas que tienen objetos con código de borrado.

Pasos

1. Inicia sesión en el nodo de administración principal:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Quando inicias sesión como root, el indicador cambia de \$ a #.

2. Comprueba si hay reparaciones de emergencia: `repair-data show-ec-repair-status`

- Si nunca has ejecutado una tarea de reparación de datos, el resultado es `No job found. No`

necesitas reiniciar ninguna tarea de reparación.

- Si la tarea de reparación de datos se ha ejecutado anteriormente o se está ejecutando en este momento, la salida muestra información sobre la reparación. Cada reparación tiene un ID de reparación único.

```
root@ADM1-0:~# repair-data show-ec-repair-status
```

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	2022-08-17T21:37:37.328998	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



Si lo deseas, puedes utilizar el Grid Manager para supervisar los procesos de restauración en curso y visualizar el historial de restauraciones. Consulta ["Restaura datos de objetos usando Grid Manager"](#).

3. Si el estado de todas las reparaciones es `Completed`, no necesitas reiniciar ningún trabajo de reparación.
4. Si el estado de cualquier reparación es `Stopped`, debes reiniciar dicha reparación.
 - a. Obtén el ID de la reparación fallida de la salida.
 - b. Ejecuta el comando `repair-data start-ec-node-repair`.

Utiliza la opción `--repair-id` para especificar el ID de reparación. Por ejemplo, si quieres volver a intentar una reparación con el ID de reparación 949292, ejecuta este comando: `repair-data start-ec-node-repair --repair-id 949292`

- c. Sigue supervisando el estado de las correcciones de datos de la EC hasta que el estado de todas las correcciones sea `Completed`.

Reúne el material necesario para decomisionar el nodo StorageGRID

Antes de decomisionar un nodo de la red, debes obtener la siguiente información.

Artículo	Notas
Archivo del paquete de recuperación .zip	Debes "descargar el paquete de recuperación más reciente" .zip archivo (<code>sgws-recovery-package-id-revision.zip</code>). Puedes utilizar el archivo del paquete de recuperación para restaurar el sistema en caso de que se produzca un fallo.
Passwords.txt archivo	Este archivo contiene las contraseñas necesarias para acceder a los nodos de la grid desde la línea de comandos y se incluye en el paquete de recuperación.
Contraseña de aprovisionamiento	La frase de contraseña se crea y se documenta al instalar el sistema StorageGRID por primera vez. La frase de contraseña de aprovisionamiento no está en el archivo <code>Passwords.txt</code> .
Descripción de la topología del sistema StorageGRID antes de decomisionar	Si está disponible, consigue toda la documentación que describa la topología actual del sistema.

Información relacionada

Accede a la página Decommission Nodes en StorageGRID

Al acceder a la página Decommission Nodes en el Grid Manager, puedes ver de un vistazo qué nodos se pueden decomisionar.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de mantenimiento o acceso de usuario raíz".



Actúa con precaución al decomisionar nodos de almacenamiento en una grid que contenga nodos basados en software destinados exclusivamente a metadatos. Si decomisionas todos los nodos configurados para almacenar *tanto* objetos como metadatos, la capacidad de almacenar objetos se elimina de la grid. Consulta "Tipos de nodos de almacenamiento" para obtener más información sobre los nodos de almacenamiento destinados exclusivamente a metadatos.

Pasos

1. Selecciona **Mantenimiento > Tareas > Decomisionar**.
2. Selecciona **Decomisionar nodos**.

Aparece la página «Nodos decomisionados». Desde esta página, puedes:

- Determina qué nodos de la red pueden decomisionarse en este momento.
- Ver el estado de todos los nodos de la red
- Ordena la lista en orden ascendente o descendente por **Nombre**, **Sitio**, **Tipo** o **Tiene ADC**.
- Introduce los términos de búsqueda para encontrar rápidamente nodos concretos.

En este ejemplo, la columna Decommission Possible indica que puedes decomisionar el Gateway Node y uno de los cuatro Storage Nodes.

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. Revisa la columna **Decommission Possible** de cada nodo que quieras decomisionar.

Si un nodo de la red puede ser descomisionado, esta columna incluye una marca de verificación verde y la columna de la izquierda incluye una casilla de selección. Si un nodo no puede ser descomisionado, esta columna describe el problema. Si hay más de un motivo por el que un nodo no puede ser descomisionado,

se muestra el motivo más grave.

Decomisionar posible motivo	Descripción	Pasos para resolverlo
No, no se admite decomisionar el <i>node type</i> .	No puedes decomisionar el nodo de administración principal.	Ninguno.
No, al menos un nodo de la grid está desconectado. Nota: Este mensaje solo se muestra en los nodos conectados a la red.	No puedes decomisionar un nodo de la red conectado si hay algún nodo de la red desconectado. La columna Estado incluye uno de estos iconos para los nodos de la cuadrícula que están desconectados:  (gris): administrativamente inactivo  (azul): desconocido	Debes volver a poner en línea todos los nodos desconectados o "decomisionar todos los nodos desconectados" antes de poder eliminar un nodo conectado. Nota: Si tu red contiene varios nodos desconectados, el software te obliga a decomisionarlos todos a la vez, lo que aumenta la posibilidad de que se produzcan resultados inesperados.
No, uno o más nodos obligatorios están desconectados en este momento y deben recuperarse. Nota: Este mensaje solo se muestra en los nodos de la red que están desconectados.	No puedes decomisionar un nodo de la red que esté desconectado si uno o más nodos necesarios también están desconectados (por ejemplo, un nodo de almacenamiento que se requiere para el quórum del ADC).	- Revisa los mensajes «Posible decomisionamiento» de todos los nodos desconectados. - Determina qué nodos no se pueden decomisionar porque son imprescindibles. - Si el estado de un nodo obligatorio es Administrativamente inactivo, vuelve a poner el nodo en línea. - Si el estado de un nodo obligatorio es Unknown, realiza un procedimiento de recuperación del nodo para recuperarlo.
No, miembro del grupo de alta disponibilidad: <i>nombre del grupo</i> . Antes de poder decomisionar este nodo, debes eliminarlo de todos los grupos de alta disponibilidad.	No puedes decomisionar un nodo de administración ni un nodo de puerta de enlace si una interfaz del nodo pertenece a un grupo de alta disponibilidad (HA).	Edita el grupo de HA para eliminar la interfaz del nodo o elimina todo el grupo de HA. Consulta "Configurar grupos de alta disponibilidad" .

Decomisionar posible motivo	Descripción	Pasos para resolverlo
No, el sitio x requiere un mínimo de n nodos de almacenamiento con servicios ADC.	Solo nodos de almacenamiento (nodos de almacenamiento combinados o de solo metadatos). No puedes decomisionar un nodo de almacenamiento si quedarían nodos insuficientes en el sitio para cumplir los requisitos de quórum del ADC. Sin embargo, puedes mover el servicio ADC a otro nodo de almacenamiento.	"Mueve el servicio ADC a otro nodo de almacenamiento en el mismo sitio" , o bien realiza una ampliación añadiendo un nuevo nodo de almacenamiento al sitio y especificando que debe tener un servicio ADC. Consulta "Quórum del ADC" .
No, uno o varios perfiles de código de borrado necesitan al menos n nodos de almacenamiento. Si el perfil no se utiliza en una regla de ILM, puedes desactivarlo.	Solo nodos de almacenamiento. No puedes decomisionar un nodo de almacenamiento a menos que queden suficientes nodos para los perfiles de código de borrado existentes. Por ejemplo, si existe un perfil de código de borrado para 4+2 erasure coding, deben quedar al menos 6 Storage Nodes.	Para cada perfil de código de borrado afectado, realiza uno de los siguientes pasos, según cómo se esté usando el perfil: • Utilizado en políticas ILM activas: Realiza una ampliación. Agrega suficientes nodos de almacenamiento nuevos para que el código de borrado pueda continuar. Consulta las instrucciones para "Ampliando tu grid". • Utilizada en una regla de ILM, pero no en políticas de ILM activas: edita o elimina la regla y luego desactiva el perfil de código de borrado. • No se utiliza en ninguna regla de ILM: desactiva el perfil de código de borrado. Nota: Aparece un mensaje de error si intentas desactivar un perfil de código de borrado y aún hay datos de objetos asociados a dicho perfil. Es posible que tengas que esperar varias semanas antes de volver a intentar el proceso de desactivación. Conoce más sobre "Desactivar un perfil de código de borrado".

Decomisionar posible motivo	Descripción	Pasos para resolverlo
No, no puedes decomisionar un nodo de archivo a menos que esté desconectado.	Si un nodo de archivo sigue conectado, no podrás eliminarlo.	Nota: Se ha eliminado la compatibilidad con los nodos de archivo. Si necesitas decomisionar un nodo de archivo, consulta "Decomisionar un nodo de grid (sitio de documentación de StorageGRID 11.8)"

Decomisionar nodos StorageGRID desconectados

Es posible que tengas que decomisionar un nodo que no esté conectado actualmente a la grid (uno cuyo estado sea Desconocido o Administratively Down).

Antes de empezar

- Conoces los aspectos que hay que tener en cuenta para decomisionar ["Nodos de administración y de pasarela"](#) y los aspectos que hay que tener en cuenta para decomisionar ["Nodos de almacenamiento"](#).
- Ya has conseguido todos los objetos necesarios.
- Te has asegurado de que no haya ninguna tarea de reparación de datos activa. Consulta ["Comprobar los trabajos de reparación de datos"](#).
- Has confirmado que no hay ninguna recuperación de Storage Node en curso en ninguna parte del grid. Si la hay, debes esperar a que finalice cualquier reconstrucción de Cassandra que se esté llevando a cabo como parte de la recuperación. Luego puedes proceder a decomisionar.
- Te has asegurado de que no se ejecuten otros procedimientos de mantenimiento mientras se está ejecutando el procedimiento de decomisionar el nodo, a menos que el procedimiento de decomisionar el nodo esté en pausa.
- La columna **Posibilidad de decomisionar** correspondiente al nodo o nodos desconectados que quieres decomisionar incluye una marca de verificación verde.
- Tienes la frase de contraseña de aprovisionamiento.

Acerca de esta tarea

Puedes identificar los nodos desconectados buscando el icono azul Unknown  o el icono gris Administratively down  en la columna **Health**.

Antes de decomisionar cualquier nodo desconectado, ten en cuenta lo siguiente:

- Este procedimiento está pensado principalmente para eliminar un único nodo desconectado. Si tu grid contiene varios nodos desconectados, el software requiere que los decomisiones todos al mismo tiempo, lo que aumenta la posibilidad de resultados inesperados.



Podría producirse una pérdida de datos si se decomisiona más de un nodo de almacenamiento desconectado a la vez. Véase ["Consideraciones para los nodos de almacenamiento desconectados"](#).



Actúa con precaución al decomisionar nodos de almacenamiento en una grid que contenga nodos basados en software destinados exclusivamente a metadatos. Si decomisionas todos los nodos configurados para almacenar *tanto* objetos como metadatos, la capacidad de almacenar objetos se elimina de la grid. Consulta "[Tipos de nodos de almacenamiento](#)" para obtener más información sobre los nodos de almacenamiento destinados exclusivamente a metadatos.

- Si no es posible eliminar un nodo desconectado (por ejemplo, un Storage Node que es necesario para el quórum del ADC), tampoco se puede eliminar ningún otro nodo desconectado.

Pasos

1. A menos que estés decomisionando un Archive Node (que debe desconectarse), intenta volver a poner en línea o recuperar cualquier nodo de grid que esté desconectado.

Consulta "[Procedimientos de recuperación de nodos de la grid](#)" para obtener instrucciones.

2. Si no puedes recuperar un nodo de la grid que está desconectado y quieres decomisionarlo mientras está desconectado, selecciona la casilla de verificación para ese nodo.



Si tu red contiene varios nodos desconectados, el software te obliga a descomisionarlos todos al mismo tiempo, lo que aumenta la probabilidad de que se produzcan resultados inesperados.



Ten cuidado al decidir decomisionar más de un nodo de la red desconectado a la vez, especialmente si seleccionas varios nodos de almacenamiento desconectados. Si tienes más de un nodo de almacenamiento desconectado que no puedes recuperar, ponte en contacto con soporte técnico para determinar cuál es la mejor forma de proceder.

3. Introduce la contraseña de aprovisionamiento.

El botón **Iniciar decomisionar** está habilitado.

4. Haz clic en **Iniciar decomisionar**.

Aparece un aviso que indica que has seleccionado un nodo desconectado y que se perderán los datos del objeto si el nodo tiene la única copia de un objeto.

5. Revisa la lista de nodos y haz clic en **OK**.

Se inicia el procedimiento de decomisionar y se muestra el progreso de cada nodo. Durante el procedimiento, se genera un nuevo paquete de recuperación que contiene el cambio de configuración de la grid.

6. En cuanto esté disponible el nuevo paquete de recuperación, haz clic en el enlace o selecciona **Mantenimiento > Sistema > Paquete de recuperación** para acceder a la página del paquete de recuperación. Luego, descarga el archivo .zip.

Consulta las instrucciones para "[descargar el paquete de recuperación](#)".



Descarga el paquete de recuperación lo antes posible para asegurarte de que puedas recuperar tu grid si algo sale mal durante el procedimiento de descomisionar.



El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

7. Supervisa periódicamente la página de Decomisionamiento para asegurarte de que todos los nodos seleccionados se hayan descomisionado correctamente.

El proceso de decomisionar los nodos de almacenamiento puede tardar días o semanas. Cuando se hayan completado todas las tareas, se vuelve a mostrar la lista de selección de nodos con un mensaje de éxito. Si decomisionaste un nodo de almacenamiento desconectado, aparecerá un mensaje informativo indicando que se han iniciado los trabajos de reparación.

8. Una vez que los nodos se hayan apagado automáticamente como parte del procedimiento de decomisionar, elimina cualquier máquina virtual restante u otros recursos asociados al nodo descomisionado.



No realices este paso hasta que los nodos se hayan apagado automáticamente.

9. Si vas a decomisionar un nodo de almacenamiento, supervisa el estado de las tareas de reparación de los **datos replicados** y de los **datos con código de borrado (EC)** que se inician automáticamente durante el proceso de decomisionamiento.

Datos replicados

- Para obtener un porcentaje estimado de finalización de la reparación replicada, añade la opción `show-replicated-repair-status` al comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Para comprobar si las reparaciones se han completado:
 - a. Selecciona **Nodos > Nodo de almacenamiento en reparación > ILM**.
 - b. Revisa los atributos en la sección de evaluación. Cuando se completen las reparaciones, el atributo **Awaiting - All** indica 0 objetos.
- Para monitorear la reparación con más detalle:
 - a. Selecciona **Nodos**.
 - b. Selecciona **nombre de la cuadrícula > ILM**.
 - c. Coloca el cursor sobre el gráfico de la cola de ILM para ver el valor del atributo **Frecuencia de escaneo (objetos/seg)**, que es la velocidad a la que se escanean los objetos en el grid y se colocan en la cola de ILM.
 - d. En la sección Cola de ILM, fíjate en los siguientes atributos:
 - **Duración del escaneo - estimada:** El tiempo estimado para completar un escaneo ILM completo de todos los objetos.

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

- **Reparaciones intentadas:** el número total de operaciones de reparación de objetos intentadas para datos replicados que se consideran de alto riesgo. Los objetos de alto riesgo son aquellos a los que les queda una sola copia, ya sea porque así lo especifica la política de ILM o como resultado de la pérdida de copias. Este recuento se incrementa cada vez que un Storage Node intenta reparar un objeto de alto riesgo. Las reparaciones de ILM de alto riesgo se priorizan si el grid se ocupa.

La misma reparación de objetos podría volver a incrementarse si la replicación falló después de la reparación. + Estos atributos pueden ser útiles cuando estés monitorizando el progreso de la recuperación de volúmenes del Storage Node. Si el número de intentos de reparación ha dejado de aumentar y se ha completado un escaneo completo, es probable que la reparación haya finalizado.

- e. Como alternativa, envía una consulta de Prometheus para `storagegrid_ilm_scan_period_estimated_minutes` y `storagegrid_ilm_repairs_attempted`.

Datos con código de borrado (EC)

Para supervisar la reparación de los datos con código de borrado y volver a intentar cualquier solicitud que haya podido fallar:

1. Determina el estado de las reparaciones de los datos con código de borrado:
 - Selecciona **Support > Tools > Metrics** para ver el tiempo estimado hasta la finalización y el porcentaje de finalización del trabajo actual. Luego, selecciona **EC Overview** en la sección de Grafana. Consulta los paneles **Grid EC Job Estimated Time to Completion** y **Grid EC Job Percentage Completed**.

- Usa este comando para ver el estado de una operación `repair-data` específica:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Utiliza este comando para listar todas las reparaciones:

```
repair-data show-ec-repair-status
```

El resultado muestra información, incluida `repair ID`, sobre todas las reparaciones que se han realizado anteriormente y las que se están llevando a cabo actualmente.

2. Si el resultado indica que la operación de reparación ha fallado, utiliza la opción `--repair-id` para volver a intentar la reparación.

Este comando vuelve a intentar la reparación de un nodo que ha fallado, usando el ID de reparación 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando vuelve a intentar una reparación de volumen que ha fallado, usando el ID de reparación 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Después de que termines

Tan pronto como se hayan decomisionado los nodos desconectados y se hayan completado todas las tareas de reparación de datos, podrás decomisionar cualquier nodo de la red conectado, según sea necesario.

A continuación, sigue estos pasos una vez que hayas finalizado el procedimiento de decomisionar:

- Asegúrate de que las unidades del nodo de red decomisionado se borren por completo. Utiliza una herramienta o un servicio de borrado de datos disponible en el mercado para eliminar de forma permanente y segura los datos de las unidades.
- Si decomisionaste un nodo de dispositivo y los datos del dispositivo estaban protegidos mediante el cifrado de nodos, usa el StorageGRID Appliance Installer para borrar la configuración del servidor de gestión de claves (Clear KMS). Debes borrar la configuración del KMS si quieres añadir el dispositivo a otra grid. Para obtener instrucciones, consulta ["Supervisar el cifrado de los nodos en modo de mantenimiento"](#).

Decomisionar nodos StorageGRID conectados

Puedes decomisionar y eliminar definitivamente los nodos que están conectados a la grid.

Antes de empezar

- Conoces los aspectos que hay que tener en cuenta para decomisionar ["Nodos de administración y de pasarela"](#) y los aspectos que hay que tener en cuenta para decomisionar ["Nodos de almacenamiento"](#).
- Ya has reunido todos los materiales necesarios.
- Te has asegurado de que no haya ninguna tarea de reparación de datos activa.
- Has confirmado que no hay ninguna recuperación de Storage Node en curso en ninguna parte del grid. Si

es así, espera a que finalice cualquier reconstrucción de Cassandra que se esté llevando a cabo como parte de la recuperación. Luego puedes proceder a decomisionar.

- Te has asegurado de que no se ejecuten otros procedimientos de mantenimiento mientras se está ejecutando el procedimiento de decomisionar el nodo, a menos que el procedimiento de decomisionar el nodo esté en pausa.
- Tienes la frase de contraseña de aprovisionamiento.
- Los nodos de la red están conectados.
- La columna «**Posibilidad de decomisionar**» correspondiente al nodo o nodos que desees decomisionar incluye una marca de verificación verde.



El proceso de decomisionar no se iniciará si uno o más volúmenes están sin conexión (desmontados) o si están en línea (montados) pero en estado de error.



Si uno o más volúmenes se desconectan mientras se está llevando a cabo el proceso de decomisionar, el proceso de decomisionar finaliza después de que estos volúmenes hayan vuelto a estar en línea.

- Todos los nodos de la red tienen un estado Normal (verde) . Si ves uno de estos iconos en la columna **Health**, debes intentar resolver el problema:

Icono	Color	Gravedad
	Amarillo	Aviso
	Naranja claro	Menor
	Naranja oscuro	Mayor
	Rojo	Crítico

- Si anteriormente descomisionaste un nodo de almacenamiento desconectado, todas las tareas de reparación de datos se han completado correctamente. Consulta ["Comprobar los trabajos de reparación de datos"](#).



No elimines la máquina virtual ni otros recursos de un nodo de la grid hasta que se te indique hacerlo en este procedimiento.



Actúa con precaución al decomisionar nodos de almacenamiento en una grid que contenga nodos basados en software destinados exclusivamente a metadatos. Si decomisionas todos los nodos configurados para almacenar *tanto* objetos como metadatos, la capacidad de almacenar objetos se elimina de la grid. Consulta ["Tipos de nodos de almacenamiento"](#) para obtener más información sobre los nodos de almacenamiento destinados exclusivamente a metadatos.

Acerca de esta tarea

Cuando se decomisiona un nodo, se desactivan sus servicios y el nodo se apaga automáticamente.

Pasos

1. En la página Decomisionar nodos, marca la casilla correspondiente a cada nodo de grid que quieras descomisionar.
2. Introduce la contraseña de aprovisionamiento.

El botón **Iniciar descomisionar** está habilitado.

3. Selecciona **Start Decommission**.
4. Revisa la lista de nodos en el cuadro de diálogo de confirmación y selecciona **OK**.

El procedimiento de descomisionar el nodo comienza y se muestra el progreso de cada nodo.



No desconectes un nodo de almacenamiento después de que se haya iniciado el procedimiento de descomisionar. Cambiar el estado podría hacer que parte del contenido no se copie a otras ubicaciones.

5. En cuanto esté disponible el nuevo paquete de recuperación, haz clic en el enlace del paquete de recuperación que aparece en el banner o selecciona **Mantenimiento > Sistema > Paquete de recuperación** para acceder a la página del paquete de recuperación. Luego, descarga el archivo .zip.

Consulta "[descargar el paquete de recuperación](#)".



Descarga el paquete de recuperación lo antes posible para asegurarte de que puedas recuperar tu grid si algo sale mal durante el procedimiento de descomisionar.

6. Supervisa periódicamente la página Decommission Nodes para asegurarte de que todos los nodos seleccionados se hayan descomisionado correctamente.



Descomisionar los nodos de almacenamiento puede tardar días o semanas.

Cuando se hayan completado todas las tareas, se vuelve a mostrar la lista de selección de nodos con un mensaje de éxito.

Después de que termines

Sigue estos pasos una vez que hayas completado el procedimiento de descomisionar el nodo:

1. Sigue los pasos correspondientes a tu plataforma. Por ejemplo:
 - **Linux:** Es posible que quieras desconectar los volúmenes y eliminar los archivos de configuración del nodo que creaste durante la instalación. Consulta "[Instalar StorageGRID en nodos basados en software](#)".
 - **VMware:** Es posible que te interese utilizar la opción «Eliminar del disco» de vCenter para eliminar la máquina virtual. Es posible que también tengas que eliminar cualquier disco de datos que sea independiente de la máquina virtual.
 - **Dispositivo StorageGRID:** El nodo del dispositivo vuelve automáticamente a un estado sin implementar, desde el que puedes acceder al instalador del dispositivo StorageGRID. Puedes apagar el dispositivo o añadirlo a otro sistema StorageGRID.
2. Asegúrate de que las unidades del nodo de red descomisionado se borren por completo. Utiliza una herramienta o un servicio de borrado de datos disponible en el mercado para eliminar de forma permanente y segura los datos de las unidades.

3. Si decomisionaste un nodo de dispositivo y los datos del dispositivo estaban protegidos mediante el cifrado de nodos, usa el StorageGRID Appliance Installer para borrar la configuración del servidor de gestión de claves (Clear KMS). Debes borrar la configuración del KMS si quieres añadir el dispositivo a otra grid. Para obtener instrucciones, consulta ["Supervisar el cifrado de los nodos en modo de mantenimiento"](#).

Pausar y reanudar el proceso de decomisionar los nodos de almacenamiento StorageGRID

Si necesitas realizar un segundo procedimiento de mantenimiento, puedes pausar el procedimiento de decomisionar un Storage Node durante determinadas fases. Después de que el otro procedimiento termine, puedes reanudar el decomisionamiento.



El botón **Pausa** solo está disponible cuando se llega a las fases de evaluación de ILM o de decomisionamiento de datos con código de borrado; sin embargo, la evaluación de ILM (migración de datos) seguirá ejecutándose en segundo plano.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).

Pasos

1. Selecciona **Mantenimiento > Tareas > Decomisionar**.

Aparece la página Decommission.

2. Selecciona **Decomisionar nodos**.

Aparece la página Decommission Nodes. Cuando el procedimiento de decomisionar llega a cualquiera de las siguientes fases, se activa el botón **Pause**.

- Evaluación de ILM
- Decomisionar datos con código de borrado

3. Selecciona **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 Q				
Name	Type	Progress	Stage	
DC1-S5	Storage Node		Evaluating ILM	

Pause

Resume

- Una vez finalizado el otro procedimiento de mantenimiento, selecciona **Reanudar** para continuar con el decomisionar.

Descomisionar sitio

Consideraciones para decomisionar un sitio en StorageGRID

Antes de utilizar el procedimiento para decomisionar un sitio, debes revisar las consideraciones.

¿Qué ocurre cuando decomisionas un sitio?

Al decomisionar un sitio, StorageGRID elimina de forma permanente todos los nodos de dicho sitio y el propio sitio del sistema StorageGRID.

Cuando se complete el procedimiento para decomisionar el sitio:

- Ya no puedes utilizar StorageGRID para ver o acceder al sitio ni a ninguno de los nodos de dicho sitio.
- Ya no podrás utilizar ningún grupo de almacenamiento ni perfil de código de borrado que hiciera referencia a ese sitio. Cuando StorageGRID decomisiona un sitio, elimina automáticamente estos grupos de almacenamiento y desactiva estos perfiles de código de borrado.

Diferencias entre los procedimientos de decomisionar sitios conectados y sitios desconectados

Puedes usar el procedimiento de decomisionar un sitio para eliminar un sitio en el que todos los nodos están conectados a StorageGRID (lo que se llama decomisionar un sitio conectado) o para eliminar un sitio en el que todos los nodos están desconectados de StorageGRID (lo que se llama decomisionar un sitio desconectado). Antes de empezar, debes entender las diferencias entre estos procedimientos.



Si un sitio contiene una combinación de nodos conectados () y nodos desconectados ( o ) , debes volver a poner en línea todos los nodos que estén fuera de línea.

- Decomisionar un sitio conectado permite eliminar un sitio operativo del sistema StorageGRID. Por ejemplo, puedes llevar a cabo el decomisionamiento de un sitio conectado para eliminar un sitio que está

operativo pero que ya no es necesario.

- Cuando StorageGRID elimina un sitio conectado, utiliza ILM para gestionar los datos de objetos de dicho sitio. Antes de poder iniciar el proceso de decomisionar un sitio conectado, debes eliminar el sitio de todas las reglas de ILM y activar una nueva política de ILM. Los procesos de ILM para migrar los datos de objetos y los procesos internos para eliminar un sitio pueden realizarse al mismo tiempo, pero la mejor práctica es permitir que los pasos de ILM se completen antes de iniciar el procedimiento de decomisionamiento propiamente dicho.
- Decomisionar un sitio desconectado te permite eliminar un sitio averiado del sistema StorageGRID. Por ejemplo, puedes llevar a cabo el decomisionamiento de un sitio desconectado para eliminar un sitio que haya quedado destruido por un incendio o una inundación.

Cuando StorageGRID elimina un sitio desconectado, considera que todos los nodos son irrecuperables y no intenta conservar los datos. Sin embargo, antes de poder iniciar el proceso de decomisionar un sitio desconectado, debes eliminar el sitio de todas las reglas de ILM y activar una nueva política de ILM.



Antes de realizar un procedimiento de descomisionamiento de un sitio desconectado, debes ponerte en contacto con tu representante de cuenta de NetApp. NetApp revisará tus requisitos antes de habilitar todos los pasos en el asistente Decommission Site. No deberías intentar descomisionar un sitio desconectado si crees que podría ser posible recuperar el sitio o recuperar los 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 puedes decomisionar un sitio que incluya el nodo de administración principal.
- No puedes decomisionar un sitio si alguno de los nodos tiene una interfaz que pertenece a un grupo de alta disponibilidad (HA). Debes editar el grupo de alta disponibilidad para quitar la interfaz del nodo o eliminar todo el grupo de alta disponibilidad.
- No puedes decomisionar un sitio si contiene una mezcla de nodos conectados (🟢) y desconectados (🔴 o 🌙).
- No puedes decomisionar un sitio si algún nodo de cualquier otro sitio está desconectado (🔴 o 🌙).
- No puedes iniciar el procedimiento de descomisionamiento del sitio si hay una operación de reparación de ec-nodo en curso. Consulta "[Comprobar los trabajos de reparación de datos](#)" para hacer un seguimiento de las reparaciones de los datos con código de borrado.
- Mientras se está llevando a cabo el procedimiento de decomisionar el sitio:
 - No puedes crear reglas de ILM que hagan referencia al sitio que se va a descomisionar. Tampoco puedes editar una regla de ILM existente para que haga referencia al sitio.
 - No puedes realizar otros procedimientos de mantenimiento, como la expansión o la actualización.



Si necesitas realizar otro procedimiento de mantenimiento durante el proceso de descomisionamiento de un sitio conectado, puedes "[pausa el procedimiento mientras se eliminan los Storage Nodes](#)". El botón **Pausar** solo está habilitado cuando se alcanzan las fases de evaluación de ILM o de descomisionamiento de datos con código de borrado; sin embargo, la evaluación de ILM (migración de datos) seguirá ejecutándose en segundo plano. Una vez completado el segundo procedimiento de mantenimiento, puedes reanudar el descomisionamiento.

- Si necesitas recuperar algún nodo tras iniciar el procedimiento de decomisionar el sitio, debes ponerte en contacto con soporte técnico.
- No puedes decomisionar 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 tu sistema StorageGRID, debes eliminar todas las relaciones de confianza de las partes dependientes del sitio de los Servicios de federación de Active Directory (AD FS).

Requisitos para la gestión del ciclo de vida de la información (ILM)

Como parte del proceso de decomisionar un sitio, debes actualizar tu configuración de ILM. El asistente Decommission Site te guía a través de una serie de pasos previos necesarios para garantizar lo siguiente:

- Ninguna política de ILM hace referencia a este sitio. Si es así, debes modificar las políticas o crear y activar políticas con nuevas reglas de ILM.
- Ninguna regla de ILM hace referencia al sitio, aunque dichas reglas no se utilicen en ninguna política. Debes eliminar o editar todas las reglas que hagan referencia al sitio.

Cuando StorageGRID decomisione el sitio, desactivará automáticamente cualquier perfil de código de borrado no utilizado que haga referencia al sitio y eliminará automáticamente cualquier grupo de almacenamiento no utilizado que haga referencia al sitio. Si existe el grupo de almacenamiento All Storage Nodes (StorageGRID 11.6 y versiones anteriores), se elimina porque utiliza todos los sitios.



Antes de poder eliminar un sitio, es posible que tengas que crear nuevas reglas de ILM y activar una nueva política de ILM. Estas instrucciones dan por hecho que comprendes bien cómo funciona ILM y que estás familiarizado con la creación de storage pools, perfiles de erasure-coding, reglas de ILM, y con la simulación y activación de una política de ILM. Consulta ["Gestiona objetos con ILM"](#).

Aspectos a tener en cuenta respecto a los datos de los objetos en un sitio conectado

Si vas a descomisionar un sitio conectado, debes decidir qué hacer con los datos de los objetos existentes en el sitio al crear nuevas reglas de ILM y una nueva política de ILM. Puedes hacer una o ambas de las siguientes cosas:

- Mueve los datos de los objetos del sitio seleccionado a uno o varios sitios de tu grid.

Ejemplo de traslado de datos: Supón que quieres decomisionar un sitio en Raleigh porque añadiste un sitio nuevo en Sunnyvale. En este ejemplo, quieres mover todos los datos de objetos del sitio antiguo al nuevo. Antes de actualizar tus reglas y políticas de ILM, debes revisar la capacidad en ambos sitios. Debes asegurarte de que el sitio de Sunnyvale tenga suficiente capacidad para alojar los datos de objetos del sitio de Raleigh y que quede capacidad adecuada en Sunnyvale para el crecimiento futuro.



Para garantizar que se dispone de la capacidad adecuada, es posible que tengas que ["expandir una grid"](#) añadiendo volúmenes de almacenamiento o Storage Nodes a un sitio existente o añadiendo un nuevo sitio antes de realizar este procedimiento.

- Eliminar copias de objetos del sitio seleccionado.

Ejemplo de eliminación de datos: Supongamos que actualmente utilizas una regla ILM de 3 copias para replicar datos de objetos en tres sitios. Antes de decomisionar un sitio, puedes crear una regla ILM equivalente de 2 copias para almacenar los datos solo en dos sitios. Cuando activas una nueva política de ILM que usa la regla de 2 copias, StorageGRID elimina las copias del tercer sitio porque ya no cumplen los requisitos de ILM. Sin embargo, los datos de los objetos seguirán protegidos y la capacidad de los dos

sitios restantes se mantendrá igual.



Nunca crees una regla ILM de copia única para permitir la eliminación de un sitio. Una regla ILM que crea solo una copia replicada durante cualquier periodo 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 Storage Node falla o tiene un error grave. También pierdes temporalmente el acceso al objeto durante procedimientos de mantenimiento como las actualizaciones.

Requisitos adicionales para decomisionar un sitio conectado

Antes de que StorageGRID pueda eliminar un sitio conectado, debes asegurarte de lo siguiente:

- Todos los nodos de tu sistema StorageGRID deben tener un estado de conexión **Conectado** (✓); sin embargo, los nodos pueden tener alertas activas.



Puedes completar los pasos 1 a 4 del asistente para descomisionar el sitio aunque uno o varios nodos estén desconectados. Sin embargo, no puedes completar el paso 5 del asistente, que inicia el proceso de decomisionar, a menos que todos los nodos estén conectados.

- Si el sitio que planeas eliminar contiene un nodo Gateway o un nodo Admin que se usa para el balanceo de carga, puede que necesites "expandir una grid" añadir un nuevo nodo equivalente en otro sitio. Asegúrate de que los clientes puedan conectarse al nodo de reemplazo antes de empezar el procedimiento para decomisionar el sitio.
- Si el sitio que planeas eliminar contiene algún Gateway Node o Admin Nodes que estén en un grupo de alta disponibilidad (HA), puedes completar los pasos 1-4 del asistente Decommission Site. Sin embargo, no puedes completar el paso 5 del asistente, que inicia el proceso de decomisionar, hasta que elimines estos nodos de todos los grupos de HA. Si los clientes existentes se conectan a un grupo de HA que incluye nodos del sitio, debes asegurarte 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 del sitio que tienes previsto eliminar, debes asegurarte de que puedan conectarse a los nodos de almacenamiento de otros sitios antes de iniciar el procedimiento para decomisionar el sitio.
- Debes disponer de espacio suficiente en los sitios restantes para alojar cualquier dato de objeto que se vaya a trasladar debido a cambios en cualquier política de ILM activa. En algunos casos, es posible que tengas que "expandir una grid" añadiendo Storage Nodes, volúmenes de almacenamiento o nuevos sitios antes de poder completar el decomisionado de un sitio conectado.
- Debes prever el tiempo suficiente para que se complete el procedimiento de decomisionar. Los procesos de StorageGRID ILM pueden tardar días, semanas o incluso meses en trasladar o eliminar los datos de objetos del sitio antes de que este pueda ser decomisionado.



Trasladar o eliminar datos de objetos de un sitio puede llevar días, semanas o incluso meses, dependiendo de la cantidad de datos que haya en el sitio, la carga del sistema, la latencia de red y la naturaleza de los cambios de ILM necesarios.

- Siempre que sea posible, debes completar los pasos 1 a 4 del asistente para decomisionar el sitio lo antes que puedas. El procedimiento de decomisionado se completará más rápido y con menos interrupciones e impactos en el rendimiento si permites que los datos se trasladen del sitio antes de iniciar el procedimiento de decomisionado propiamente dicho (seleccionando **Start Decommission** en el paso 5 del asistente).

Requisitos adicionales para decomisionar un sitio desconectado

Antes de que StorageGRID pueda eliminar un sitio desconectado, debes asegurarte de lo siguiente:

- Te has puesto en contacto con tu representante de cuenta de NetApp. NetApp revisará tus requisitos antes de habilitar todos los pasos del asistente para decomisionar el sitio.



No deberías intentar decomisionar un sitio desconectado si crees que podría ser posible recuperar el sitio o recuperar cualquier dato de objeto del sitio. Consulta ["Cómo el soporte técnico recupera un sitio"](#).

- Todos los nodos del sitio deben tener un Estado de conexión que sea uno de los siguientes:
 - **Desconocido** (🔌): Por una razón desconocida, un nodo se ha desconectado o los servicios del nodo han dejado de funcionar de forma inesperada. Por ejemplo, es posible que se haya detenido un servicio del nodo o que el nodo haya perdido la conexión de red debido a un corte de energía o a una interrupción inesperada.
 - **Fuera de servicio por motivos administrativos** (🌙): El nodo no está conectado a la grid por una razón prevista. Por ejemplo, el nodo o los servicios en el nodo se han apagado de forma controlada.
- Todos los nodos de los demás sitios deben tener un estado de conexión **Conectado** (✅); sin embargo, estos otros nodos pueden tener alertas activas.
- Debes tener en cuenta que ya no podrás utilizar StorageGRID para ver ni recuperar ningún dato de objeto que se almacenaba en ese sitio. Cuando StorageGRID realiza este procedimiento, no intenta conservar ningún dato del sitio desconectado.



Si tus reglas y políticas de ILM se diseñaron para protegerte frente a la pérdida de un único sitio, seguirán existiendo copias de tus objetos en los sitios restantes.

- Debes tener en cuenta que si el sitio contenía la única copia de un objeto, el objeto se pierde y no se puede recuperar.

Aspectos a tener en cuenta para la coherencia al eliminar un sitio

La consistencia de un bucket S3 determina si StorageGRID replica íntegramente los metadatos de los objetos en todos los nodos y sitios antes de decirle a un cliente que la incorporación del objeto fue exitosa. La consistencia ofrece un equilibrio entre la disponibilidad de los objetos y la consistencia de esos objetos en los diferentes Storage Nodes y sitios.

Cuando StorageGRID elimina un sitio, debe asegurarse de que no se escriban datos en el sitio que se va a eliminar. Por ello, anula temporalmente la consistencia de cada bucket o contenedor. Una vez que inicias el proceso de decomisionar el sitio, StorageGRID utiliza temporalmente una consistencia de sitio estricta para evitar que se escriban metadatos de objetos en el sitio que se va a eliminar.

Como consecuencia de esta anulación temporal, ten en cuenta que cualquier operación de escritura, actualización o eliminación realizada por un cliente durante el proceso de decomisionar un sitio puede fallar si varios nodos dejan de estar disponibles en los sitios restantes.

Reúne los materiales necesarios para decomisionar el sitio de StorageGRID

Antes de decomisionar un sitio, debes conseguir los siguientes materiales.

Artículo	Notas
Archivo del paquete de recuperación .zip	Debes descargar el paquete de recuperación más reciente .zip archivo (sgws-recovery-package-id-revision.zip). Puedes utilizar el archivo del paquete de recuperación para restaurar el sistema en caso de que se produzca un fallo. "Descargar el paquete de recuperación"
Passwords.txt archivo	Este archivo contiene las contraseñas necesarias para acceder a los nodos de la grid desde la línea de comandos y se incluye en el paquete de recuperación.
Contraseña de aprovisionamiento	La frase de contraseña se crea y se documenta al instalar el sistema StorageGRID por primera vez. La frase de contraseña de aprovisionamiento no está en el archivo Passwords.txt.
Descripción de la topología del sistema StorageGRID antes de decomisionar	Si está disponible, consigue toda la documentación que describa la topología actual del sistema.

Información relacionada

["Requisitos del navegador web"](#)

Selecciona un sitio para decomisionar en StorageGRID

Para determinar si se puede descomisionar un sitio, empieza por acceder al asistente de descomisionamiento de sitios.

Antes de empezar

- Ya has conseguido todo el material necesario.
- Ya has revisado las consideraciones para eliminar un sitio.
- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de acceso root o los permisos de mantenimiento e ILM"](#).

Pasos

1. Selecciona **Mantenimiento > Tareas > Decomisionar**.
2. Selecciona **Decomisionar Site**.

Aparece el paso 1 (Seleccionar sitio) del asistente para descomisionar sitios. Este paso incluye una lista alfabética de los sitios de tu 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

- Consulta los valores de 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 desconectados, la Capacidad de almacenamiento utilizada es el último valor conocido para el sitio.

- Para decomisionar un sitio conectado, este valor representa cuántos datos de objetos tendrán que moverse a otros sitios o ser eliminados por ILM antes de que puedas decomisionar este sitio de forma segura.
- En el caso de la descomisionación de un sitio desconectado, este valor indica qué parte del almacenamiento de datos de tu sistema quedará inaccesible cuando decomisiones este sitio.



Si tu política de ILM se diseñó para proteger contra la pérdida de un solo sitio, las copias de tus datos de objetos deberían seguir existiendo en los sitios restantes.

- Revisa los motivos en la columna **Decommission Possible** para determinar qué sitios pueden decomisionarse actualmente.



Si hay más de un motivo por el que no se puede decomisionar un sitio, se muestra el motivo más crítico.

Decomisionar posible motivo	Descripción	Siguiente paso
Marca de verificación verde ()	Puedes decomisionar este sitio.	Vaya a el siguiente paso .

Decomisionar posible motivo	Descripción	Siguiente paso
No. Este sitio contiene el nodo de administración principal.	No puedes decomisionar un sitio que contenga el nodo de administración principal.	Ninguno. No puedes realizar este procedimiento.
No. Este sitio contiene uno o varios Archive Nodes.	No puedes decomisionar un sitio que contenga un Archive Node.	Ninguno. No puedes realizar este procedimiento.
No. Todos los nodos de este sitio están desconectados. Ponte en contacto con tu representante de cuenta de NetApp.	No puedes decomisionar un sitio conectado a menos que todos los nodos del sitio estén conectados (✓).	Si quieres realizar la descomisión de un sitio desconectado, debes ponerte en contacto con tu representante de cuenta de NetApp, quien revisará tus requisitos y habilitará el resto del asistente para descomisionar sitios. IMPORTANTE: Nunca desconectes los nodos en línea para eliminar un sitio. Perderás datos.

El ejemplo muestra un sistema StorageGRID con tres sitios. La marca de verificación verde (✓) junto a los sitios Raleigh y Sunnyvale indica que puedes decomisionar esos sitios. Sin embargo, no puedes decomisionar el sitio Vancouver porque contiene el nodo de administración principal.

1. Si es posible decomisionar el sitio, selecciona el botón de opción para el sitio.

El botón **Siguiente** está activo.

2. Selecciona **Siguiente**.

Aparece el paso 2 (Ver detalles).

Revisa los detalles del sitio antes de decomisionar en StorageGRID

Desde el paso 2 (Ver detalles) del asistente para decomisionar un sitio, puedes revisar qué nodos están incluidos en el sitio, ver cuánto espacio se ha utilizado en cada Storage Node y evaluar cuánto espacio libre hay disponible en los demás sitios de tu grid.

Antes de empezar

Antes de decomisionar un sitio, debes revisar cuántos datos de objetos existen en el sitio.

- Si vas a descomisionar un sitio conectado, debes conocer la cantidad de datos de objetos que hay actualmente en el sitio antes de actualizar ILM. En función de las capacidades del sitio y de tus necesidades de protección de datos, puedes crear nuevas reglas de ILM para mover datos a otros sitios o para eliminar datos de objetos del sitio.
- Si es posible, realiza las ampliaciones necesarias del nodo de almacenamiento antes de iniciar el procedimiento de decomisionar.

- Si vas a descomisionar un sitio desconectado, debes tener en cuenta qué cantidad de datos de objetos quedará inaccesible de forma permanente al eliminar el sitio.

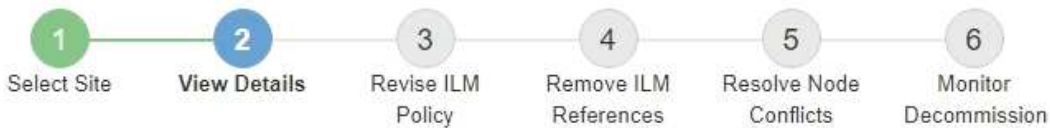


Si estás llevando a cabo la descomisionación de un sitio desconectado, ILM no puede mover ni eliminar los datos de los objetos. Cualquier dato que permanezca en el sitio se perderá. Sin embargo, si tu política de ILM se diseñó para proteger contra la pérdida de un solo sitio, seguirán existiendo copias de los datos de tus objetos en los sitios restantes. Consulta ["Activar la protección contra la pérdida del sitio"](#).

Pasos

1. En el paso 2 (Ver detalles), revisa las advertencias relacionadas con el sitio que seleccionaste para 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.

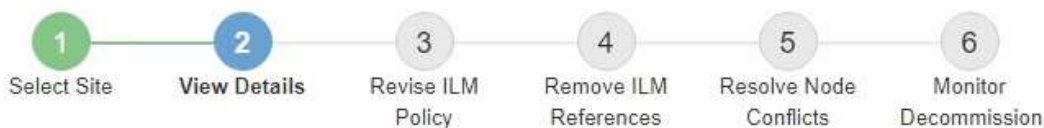
⚠ This site contains a mixture of connected and disconnected nodes. Before you can remove this site, you must bring all offline (blue or gray) nodes back online. Contact technical support if you need assistance.

En estos casos aparece un aviso:

- El sitio incluye un nodo Gateway. Si actualmente hay clientes de S3 conectados a este nodo, debes configurar un nodo equivalente en otro sitio. Asegúrate de que los clientes puedan conectarse al nodo de reemplazo antes de continuar con el procedimiento de descomisionar.
- El sitio contiene una combinación de nodos conectados (✅) y nodos desconectados (🌑 o 🔄). Antes de poder eliminar este sitio, debes volver a poner en línea todos los nodos que están fuera de línea.

2. Revisa los detalles sobre el sitio que has seleccionado para eliminar.

Decommission Site



Raleigh Details

Number of Nodes: 3
Used Space: 3.93 MB

Free Space: 475.38 GB
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](#)

Se incluye la siguiente información 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 decomisionar un sitio conectado, el valor de **Espacio utilizado** representa cuántos datos de objetos deben moverse a otros sitios o eliminarse con ILM.
 - Para decomisionar un sitio desconectado, el valor de **Espacio utilizado** indica cuántos datos de objetos se volverán inaccesibles cuando elimines el sitio.
- Nombres de nodo, tipos y estados de conexión:
 -  (Conectado)
 -  (Fuera de servicio por motivos administrativos)
 -  (Desconocido)
- Detalles sobre cada nodo:
 - Para cada nodo de almacenamiento, la cantidad de espacio que se ha utilizado para los datos de

objetos.

- Para los nodos de administración y los nodos de puerta de enlace, si el nodo se está usando actualmente en un grupo de alta disponibilidad (HA). No puedes decomisionar un nodo de administración ni un nodo de puerta de enlace que se use en un grupo de alta disponibilidad. Antes de empezar el decomisionamiento, edita los grupos de alta disponibilidad para quitar todos los nodos del sitio o elimina el grupo de alta disponibilidad si solo incluye nodos de este sitio. Para ver las instrucciones, consulta ["Administra grupos de alta disponibilidad \(HA\)"](#).

3. En la sección Detalles de otros emplazamientos de la página, comprueba cuánto espacio hay disponible en los demás emplazamientos de tu grid.

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 estás descomisionando un sitio conectado y planeas usar ILM para mover los datos de objetos del sitio seleccionado (en vez de simplemente eliminarlos), debes asegurarte de que los otros sitios tengan suficiente capacidad para alojar los datos movidos y que quede capacidad adecuada para el crecimiento futuro.



Aparecerá una advertencia si el **Espacio utilizado** del sitio que deseas eliminar es mayor que el **Espacio libre total para otros sitios**. Para asegurarte de que dispones de suficiente capacidad de almacenamiento tras la eliminación del sitio, es posible que tengas que realizar una expansión antes de llevar a cabo este procedimiento.

4. Selecciona **Siguiente**.

Aparece el paso 3 (Revisar la política de ILM).

Revisa las políticas de ILM para decomisionar sitios en StorageGRID

Desde el paso 3 (Revisar políticas de ILM) del asistente para decomisionar un sitio, puedes determinar si alguna política de ILM hace referencia a dicho sitio.

Antes de empezar

Tienes un buen conocimiento de cómo ["gestionar objetos con ILM"](#). Estás familiarizado con la creación de grupos de almacenamiento y reglas de ILM y con la simulación y activación de una política de ILM.

Acercas de esta tarea

StorageGRID no puede decomisionar un sitio si alguna regla de ILM de cualquier política (activa o inactiva) hace referencia a ese sitio.

Si alguna política de ILM hace referencia al sitio que deseas descomisionar, debes eliminar dichas políticas o modificarlas para que cumplan estos requisitos:

- Protege por completo todos los datos de los objetos.
- No hagas referencia al sitio que vas a descomisionar.
- No utilices grupos de almacenamiento que hagan referencia al sitio ni utilices la opción All Sites.
- No utilices perfiles de código de borrado que hagan referencia al sitio.
- No utilices la regla «Make 2 Copies» de las instalaciones de StorageGRID 11.6 o anteriores.



Nunca crees una regla ILM de copia única para permitir la eliminación de un sitio. Una regla ILM que crea solo una copia replicada durante cualquier periodo 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 Storage Node falla o tiene un error grave. También pierdes temporalmente el acceso al objeto durante procedimientos de mantenimiento como las actualizaciones.



Si vas a llevar a cabo un *decomisionar de un sitio conectado*, debes tener en cuenta cómo debe gestionar StorageGRID los datos de objetos que se encuentran actualmente en el sitio que deseas eliminar. En función de tus requisitos de protección de datos, las nuevas reglas pueden mover los datos de objetos existentes a otros sitios o eliminar cualquier copia adicional de objetos que ya no sea necesaria.

Ponte en contacto con el soporte técnico si necesitas ayuda para diseñar una nueva política.

Pasos

1. A partir del paso 3 (Revisar las políticas de ILM), comprueba si alguna de las políticas de ILM hace referencia al sitio que seleccionaste para decomisionar.
2. Si no aparece ninguna póliza en la lista, selecciona **Siguiente** para ir a ["Paso 4: Eliminar las referencias a ILM"](#).
3. Si aparecen una o más políticas de ILM *activas*, clona cada una de las políticas existentes o crea nuevas políticas que no hagan referencia al sitio que se va a decomisionar:
 - a. Selecciona el enlace de la política en la columna Nombre de la política.

La página de detalles de la política de ILM correspondiente a dicha política se abre en una nueva pestaña del navegador. La página de Decommission Site permanecerá abierta en la otra pestaña.

- b. Sigue estas directrices e instrucciones según sea necesario:

- Trabaja con las reglas de ILM:
 - ["Crear uno o varios grupos de almacenamiento"](#) que no hagan referencia al sitio.
 - ["Editar o sustituir reglas"](#) que hacen referencia al sitio.



No selecciones la regla **Crear 2 copias** porque esa regla usa el grupo de almacenamiento **Todos los nodos de almacenamiento**, lo cual no está permitido.

- Trabaja con políticas de ILM:
 - ["Clonar una política de ILM existente"](#) o ["Crea una nueva política de ILM"](#).
 - Asegúrate de que la regla predeterminada y el resto de reglas no hagan referencia al sitio.



Debes comprobar que las reglas de ILM estén en el orden correcto. Cuando se activa la política, los objetos nuevos y existentes se evalúan según las reglas en el orden indicado, empezando por la parte superior.

c. Introduce objetos de prueba y simula la política para asegurarte de que se aplican las reglas correctas.



Los errores en una política de ILM pueden provocar una pérdida irrecuperable de datos. Revisa detenidamente y simula la política antes de activarla para confirmar que funcionará como esperas.



Al activar una nueva política de ILM, StorageGRID la utiliza para gestionar todos los objetos, tanto los ya existentes como los recién incorporados. Antes de activar una nueva política de ILM, revisa cualquier cambio en la ubicación de los objetos replicados y con código de borrado ya existentes. Cambiar la ubicación de un objeto existente podría provocar problemas temporales de recursos mientras se evalúan y se implementan las nuevas ubicaciones.

d. Activa las nuevas políticas y asegúrate de que las antiguas ya estén inactivas.

Si quieres activar varias políticas, "[Sigue los pasos para crear etiquetas de política de ILM](#)".

Si estás llevando a cabo la descomisión de un sitio conectado, StorageGRID comienza a eliminar los datos de objetos del sitio seleccionado tan pronto como activas la nueva política de ILM. Mover o eliminar todas las copias de los objetos puede tardar semanas. Aunque puedes iniciar con seguridad la descomisión de un sitio mientras aún existan datos de objetos en el sitio, el procedimiento de descomisión se completará más rápido y con menos interrupciones e impactos en el rendimiento si permites que los datos se trasladen del sitio antes de iniciar el procedimiento de descomisión (seleccionando **Start Decommission** en el paso 5 del asistente).

4. Para cada política *inactiva*, éditala o elimínala seleccionando primero el enlace de cada política como se describió en los pasos anteriores.
 - "[Editar la política](#)" por lo que no se refiere al sitio que se va a decomisionar.
 - "[Eliminar una política](#)".
5. Cuando termines de hacer cambios en las reglas y políticas de ILM, no debería haber más políticas listadas en el paso 3 (Revisar políticas de ILM). Selecciona **Siguiente**.

Aparece el paso 4 (Remove ILM References).

Eliminar referencias de ILM a un sitio en StorageGRID

Desde el paso 4 (Eliminar referencias de ILM) del asistente para decomisionar el sitio, debes eliminar o modificar cualquier regla de ILM en desuso que haga referencia al sitio, incluso si dichas reglas no se utilizan en ninguna política de ILM.

Pasos

1. Comprueba si hay alguna regla de ILM no utilizada que se refiera al sitio.

Si aparece alguna regla de ILM, dichas reglas siguen haciendo referencia al sitio pero no se utilizan en ninguna política.



Cuando StorageGRID decomisiona el sitio, desactivará automáticamente cualquier perfil de código de borrado no utilizado que haga referencia al sitio y eliminará automáticamente cualquier grupo de almacenamiento no utilizado que haga referencia al sitio. El grupo de almacenamiento All Storage Nodes (StorageGRID 11.6 y versiones anteriores) se elimina porque utiliza el sitio All Sites.

2. Edita o elimina cada regla que no se utilice:

- Para editar una regla, ve a la página de reglas de ILM y actualiza todas las ubicaciones que utilicen un perfil de código de borrado o un grupo de almacenamiento que haga referencia al sitio. Luego, vuelve a **Paso 4 (Eliminar referencias de ILM)**.
- Para eliminar una regla, selecciona el icono de la papelera  y selecciona **OK**.



Debes eliminar la regla **Hacer 2 copias** antes de poder decomisionar un sitio.

3. Comprueba que no haya ninguna regla de ILM sin utilizar asociada al sitio y que el botón **Siguiente** esté activo.

4. Selecciona **Siguiente**.



Cualquier grupo de almacenamiento y perfil de código de borrado restantes que hagan referencia al sitio dejarán de ser válidos cuando se elimine el sitio. Cuando StorageGRID decomisione el sitio, desactivará automáticamente cualquier perfil de código de borrado no utilizado que haga referencia al sitio y eliminará automáticamente cualquier grupo de almacenamiento no utilizado que haga referencia al sitio. El grupo de almacenamiento All Storage Nodes (StorageGRID 11.6 y versiones anteriores) se elimina porque utiliza el sitio All Sites.

Aparece el paso 5 (Resolver conflictos entre nodos).

Resuelve conflictos de nodos e inicia la descomisión de sitios en StorageGRID

Desde el paso 5 (Resolver conflictos entre nodos) del asistente para descomisionar un sitio, puedes determinar si algún nodo de tu sistema StorageGRID está desconectado o si algún nodo del sitio seleccionado pertenece a un grupo de alta disponibilidad (HA). Después de resolver cualquier conflicto entre nodos, inicias el procedimiento de decomisionar desde esta página.

Antes de empezar

Debes asegurarte de que todos los nodos de tu sistema StorageGRID estén en el estado correcto, como se indica a continuación:

- Todos los nodos de tu sistema StorageGRID deben estar conectados (.



Si vas a descomisionar un sitio desconectado, todos los nodos del sitio que vas a eliminar deben estar desconectados, y todos los nodos de los demás sitios deben estar conectados.



El proceso de decomisionar no se iniciará si uno o más volúmenes están sin conexión (desmontados) o si están en línea (montados) pero en estado de error.



Si uno o más volúmenes se desconectan mientras se está llevando a cabo el proceso de decomisionar, el proceso de decomisionar finaliza después de que estos volúmenes hayan vuelto a estar en línea.

- Ningún nodo del sitio que vas a eliminar puede tener una interfaz que pertenezca a un grupo de alta disponibilidad (HA).

Acerca de esta tarea

Si aparece algún nodo en el paso 5 (Resolver conflictos entre nodos), debes solucionar el problema antes de poder iniciar el decomisionar.

Antes de iniciar el procedimiento de decomisionar el sitio desde esta página, ten en cuenta las siguientes consideraciones:

- Debes prever el tiempo suficiente para que se complete el procedimiento de decomisionar.



Trasladar o eliminar datos de objetos de un sitio puede llevar días, semanas o incluso meses, dependiendo de la cantidad de datos que haya en el sitio, la carga del sistema, la latencia de red y la naturaleza de los cambios de ILM necesarios.

- Mientras se está llevando a cabo el procedimiento de decomisionar el sitio:
 - No puedes crear reglas de ILM que hagan referencia al sitio que se va a descomisionar. Tampoco puedes editar una regla de ILM existente para que haga referencia al sitio.
 - No puedes realizar otros procedimientos de mantenimiento, como la expansión o la actualización.



Si necesitas realizar otro procedimiento de mantenimiento durante el proceso de decomisionar un sitio conectado, puedes pausar el procedimiento mientras se eliminan los Storage Nodes. El botón **Pause** está habilitado durante la etapa «Decommissioning Replicated and Erasure-Coded Data».

- Si necesitas recuperar algún nodo tras iniciar el procedimiento de decomisionar el sitio, debes ponerte en contacto con soporte técnico.

Pasos

1. Consulta la sección sobre nodos desconectados del Paso 5 (Resolver conflictos entre nodos) para determinar si algún nodo de tu 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 hay algún nodo desconectado, vuelve a ponerlo en línea.

Consulta la "[Procedimientos de nodo](#)". Ponte en contacto con el soporte técnico si necesitas ayuda.

3. Cuando todos los nodos desconectados hayan vuelto a estar en línea, revisa la sección de grupos de alta disponibilidad del paso 5 (Resolver conflictos entre nodos).

Esta tabla muestra todos los nodos del 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 aparece algún nodo en la lista, haz una de las siguientes cosas:

- Edita cada grupo de alta disponibilidad afectado para eliminar la interfaz del nodo.
- Elimina un grupo de alta disponibilidad (HA) que solo incluya nodos de este sitio. Consulta las instrucciones para administrar StorageGRID.

Si todos los nodos están conectados y ningún nodo del sitio seleccionado forma parte de un grupo de HA, el campo **Contraseña de aprovisionamiento** se habilita.

5. Introduce la contraseña de aprovisionamiento.

El botón **Start Decommission** queda activo.

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 estás listo para iniciar el procedimiento de decomisionar el sitio, selecciona **Start Decommission**.

En un aviso se enumeran el sitio y los nodos que se van a eliminar. Te recordamos que la eliminación completa del sitio puede tardar días, semanas o incluso meses.

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. Lee la advertencia. Si estás listo para empezar, selecciona **OK**.

Aparece un mensaje mientras se genera la nueva configuración de la grid. Este proceso puede tardar un tiempo, dependiendo del tipo y el número de nodos de la grid que se hayan decomisionado.

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 

Cuando se ha generado la nueva configuración de la grid, aparece el paso 6 (Monitor Decommission).



El botón **Anterior** permanece desactivado hasta que se complete el proceso de decomisionar.

Supervisa el progreso de la descomisión de instalaciones en StorageGRID

Desde el paso 6 (Monitor Decommission) del asistente de la página Decommission Site, puedes supervisar 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

La eliminación de cada Gateway Node o Admin Node puede llevar solo unos minutos o una hora; sin embargo, los Storage Nodes pueden tardar días o semanas.

Pasos

1. En cuanto se haya generado un nuevo paquete de recuperación, descarga 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.



Descarga el paquete de recuperación lo antes posible para asegurarte de que puedas recuperar tu grid si algo sale mal durante el procedimiento de descomisionar.

- a. Haz clic en el enlace del mensaje o selecciona **Mantenimiento > Sistema > Paquete de recuperación**.
- b. Descarga el archivo `.zip`.

Consulta las instrucciones para "[descargar el paquete de recuperación](#)".

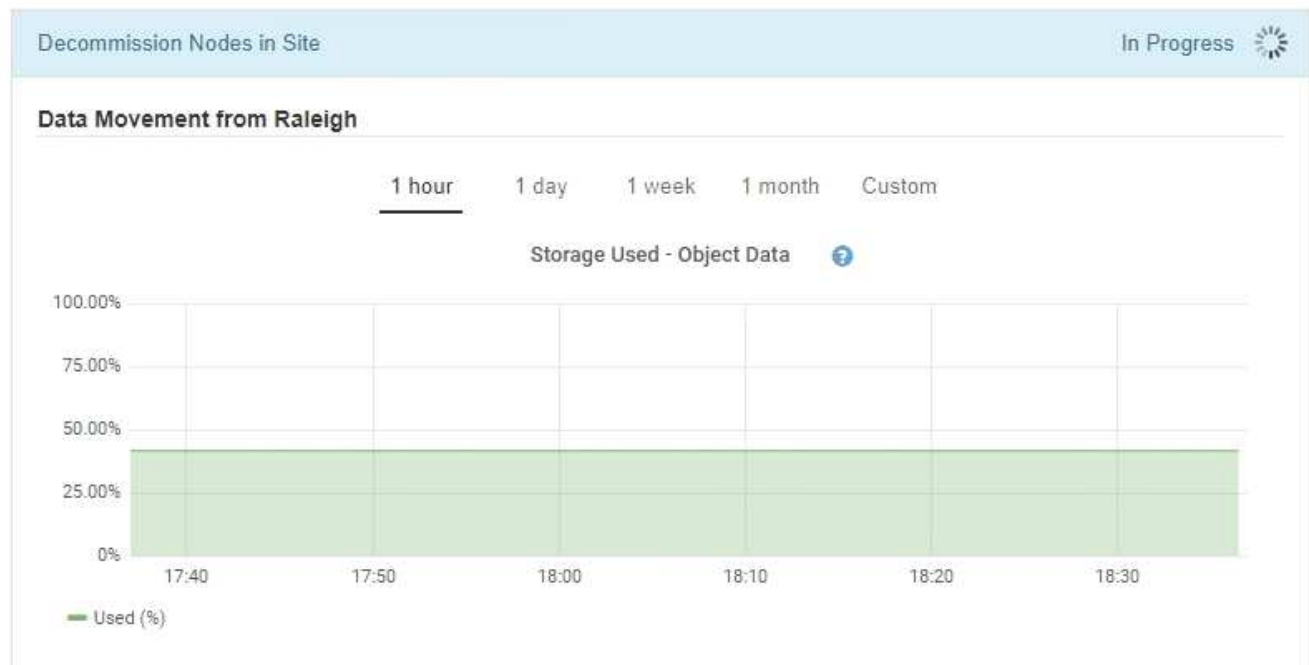


El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

2. Utiliza el gráfico de movimiento de datos para supervisar el movimiento de los datos de objetos desde este sitio a otros sitios.

La transferencia de datos comenzó cuando activaste la nueva política de ILM en el paso 3 (Revisar ILM Policy). La transferencia de datos ocurrirá durante todo el procedimiento de decomisionar.

Decommission Site Progress



3. En la sección Progreso de los nodos de la página, supervisa el progreso del procedimiento de decomisionar 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 se producen rápidamente o incluso de forma imperceptible, es posible que tengas que esperar días o incluso semanas a que se completen otras etapas, en función de la cantidad de datos que haya que mover. Se requiere tiempo adicional para gestionar los datos con código de borrado y volver a evaluar 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 estás supervisando el progreso de la descomisionación de un sitio conectado, consulta esta tabla para conocer las fases de la descomisionación de un Storage Node:

Escenario	Duración estimada
Pending	Un minuto o menos
Esperar bloqueos	Minutos
Preparar tarea	Un minuto o menos
Marcando LDR descomisionado	Minutos
Decomisionar datos replicados y con código de borrado	Horas, días o semanas en función de la cantidad de datos Nota: Si necesitas realizar otras tareas de mantenimiento, puedes pausar el decomisionamiento del sitio durante esta etapa.
Estado del conjunto LDR	Minutos
Vaciar las colas de auditoría	De unos minutos a unas horas, dependiendo del número de mensajes y la latencia de red.
Completo	Minutos

Si estás supervisando el progreso del proceso de decomisionar un sitio desconectado, consulta esta tabla para entender las etapas de decomisionar un Storage Node:

Escenario	Duración estimada
Pending	Un minuto o menos
Esperar bloqueos	Minutos
Preparar tarea	Un minuto o menos
Desactivar servicios externos	Minutos
Revocación de certificados	Minutos
Cancelar el registro del nodo	Minutos
Cancelar el registro de Storage Grade	Minutos
Eliminación de grupo de almacenamiento	Minutos
Eliminación de entidades	Minutos

Escenario	Duración estimada
Completo	Minutos

4. Después de que todos los nodos hayan alcanzado la etapa Complete, espera a que finalicen las operaciones restantes de decomisionar el sitio.
 - Durante el paso **Reparar Cassandra**, StorageGRID realiza las reparaciones necesarias en los clústeres de Cassandra que permanecen en tu grid. Estas reparaciones pueden tardar varios días o más, dependiendo de cuántos nodos de almacenamiento queden en tu grid.

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 de código de borrado que hacían referencia al sitio.
 - Se eliminan todos los grupos de almacenamiento que hacían referencia a ese sitio.



El grupo de almacenamiento All Storage Nodes (StorageGRID 11.6 y versiones anteriores) también se elimina porque utiliza el sitio All Sites.

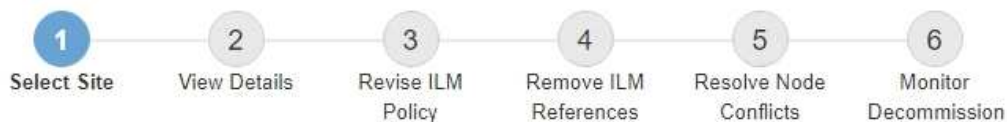
- Por último, durante el paso **Eliminar configuración**, se eliminan del resto de la grid todas las referencias restantes al sitio y a sus nodos.

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. Cuando el procedimiento de decomisionar ha finalizado, la página Decommission Site 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 que termines

Realiza estas tareas una vez que hayas completado el procedimiento para decomisionar el sitio:

- Asegúrate de que las unidades de todos los Storage Nodes en el sitio decomisionado se borren por completo. Usa una herramienta o un servicio de borrado de datos disponible en el mercado para eliminar de forma permanente y segura los datos de las unidades.
- Si el sitio incluye uno o varios nodos de administración y el inicio de sesión único (SSO) está habilitado para tu sistema StorageGRID, elimina todas las relaciones de confianza de las partes dependientes para ese sitio de Active Directory Federation Services (AD FS).
- Una vez que los nodos se hayan apagado automáticamente de forma controlada como parte del procedimiento de descomisionamiento del sitio conectado, elimina las máquinas virtuales asociadas.

Cambiar el nombre de una grid, un sitio o un nodo

Usa el procedimiento de cambio de nombre de StorageGRID

Si lo necesitas, puedes cambiar los nombres que se muestran en todo el Grid Manager para toda la grid, cada sitio y cada nodo. Puedes actualizar los nombres de pantalla de forma segura y cuando lo necesites.

¿En qué consiste el procedimiento de cambio de nombre?

Al instalar StorageGRID por primera vez, especificas un nombre para la grid, cada sitio y cada nombre de nodo. Estos nombres iniciales se conocen como *nombres del sistema* y son los nombres que aparecen inicialmente en todo StorageGRID.

Los nombres de sistema son obligatorios para las operaciones internas de StorageGRID y no se pueden cambiar. Sin embargo, puedes usar el procedimiento de cambio de nombre para definir nuevos *nombres de visualización* para la grid, cada sitio y cada nombre de nodo. Estos nombres de visualización aparecen en varias ubicaciones de StorageGRID en lugar de (o, en algunos casos, además de) los nombres de sistema subyacentes.

Utiliza el procedimiento de cambio de nombre para corregir errores tipográficos, aplicar una convención de nomenclatura diferente o indicar que un sitio y todos sus nodos se han reubicado. A diferencia de los nombres del sistema, los nombres de visualización se pueden actualizar siempre que sea necesario y sin que ello afecte al funcionamiento de StorageGRID.

¿Dónde aparecen los nombres del sistema y los nombres de visualización?

La siguiente tabla resume dónde aparecen los nombres del sistema y los nombres de visualización en la interfaz de usuario de StorageGRID y en los archivos de StorageGRID.

Ubicación	Nombre del sistema	Nombre para mostrar
Páginas de Grid Manager	Se muestra a menos que se cambie el nombre del elemento	Si se cambia el nombre de un elemento, se mostrará en lugar del nombre del sistema en estas ubicaciones: • Consola • Página de nodos • Páginas de configuración para grupos de alta disponibilidad, puntos finales de balanceadores de carga, interfaces VLAN, servidores de gestión de claves, contraseñas de grid y control de firewall • Alertas • Definiciones de grupos de almacenamiento • Página de consulta de metadatos de objetos • Páginas relacionadas con los procedimientos de mantenimiento, incluyendo actualización, corrección urgente, actualización del sistema operativo SANtricity, decomisionar, ampliación, recuperación y comprobación de existencia de objetos • Páginas de soporte (registros y diagnósticos) • Página de inicio de sesión único, junto al nombre de host del Admin Node en la tabla de detalles del Admin Node
Nodos > pestaña Resumen de un nodo	Siempre visible	Se muestra únicamente si se ha cambiado el nombre del elemento

Ubicación	Nombre del sistema	Nombre para mostrar
API node-health	Siempre devuelto	Solo se devuelve si se cambia el nombre del elemento
Mensaje que aparece al usar SSH para acceder a un nodo	Aparece como nombre principal, a menos que se haya cambiado el nombre del elemento: <pre>admin@SYSTEM-NAME: ~ \$</pre> Se incluye entre paréntesis cuando se cambia el nombre del elemento: <pre>admin@DISPLAY-NAME (SYSTEM-NAME): ~ \$</pre>	Aparece 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 aparece en la segunda columna	Cuando se cambia el nombre del elemento, se muestra en la cuarta columna
topology-display-names.json, incluido con los datos de AutoSupport	No incluido	Vacío a menos que se haya cambiado el nombre de los elementos; de lo contrario, asigna los ID de cuadrícula, sitio y nodo a sus nombres de visualización.

Requisitos para el nombre que se muestra

Antes de usar este procedimiento, revisa los requisitos para los nombres para mostrar.

Nombres de visualización de los nodos

Los nombres que se muestran para los nodos deben cumplir las siguientes reglas:

- Debe ser único en todo tu sistema StorageGRID.
- No puede coincidir con el nombre de sistema de ningún otro elemento de tu sistema StorageGRID.
- Debe contener al menos 1 y no más de 32 caracteres.
- Puede contener números, guiones (-) y letras mayúsculas y minúsculas.
- Puede empezar o terminar con una letra o un número, pero no puede empezar ni terminar con un guión.
- No puede ser solo números.
- No distinguen entre mayúsculas y minúsculas. Por ejemplo, DC1-ADM y dc1-adm se consideran duplicados.

Puedes cambiar el nombre de un nodo por un nombre de visualización que ya haya utilizado anteriormente otro nodo, siempre y cuando el cambio no dé lugar a un nombre de visualización o un nombre de sistema duplicado.

Nombres para la cuadrícula y los sitios

Los nombres para la grid y los sitios siguen las mismas reglas, con estas excepciones:

- Puede incluir espacios.
- Puede incluir estos caracteres especiales: = - _ : , . @ !
- Puede empezar y terminar con caracteres especiales, incluidos los guiones.
- Puede estar compuesto únicamente por números o caracteres especiales.

Mejores prácticas para el nombre para mostrar

Si tienes pensado cambiar el nombre de varios elementos, define tu esquema general de nomenclatura antes de seguir este procedimiento. Crea un sistema que garantice que los nombres sean únicos, coherentes y fáciles de entender a simple vista.

Puedes utilizar cualquier convención de nomenclatura que se adapte a los requisitos de tu organización. Ten en cuenta estas sugerencias básicas sobre qué incluir:

- **Indicador de sitio:** si tienes varios sitios, añade un código de sitio al nombre de nodo.
- **Tipo de nodo:** Los nombres de los nodos suelen indicar su tipo. Puedes utilizar abreviaturas como *s*, *adm* y *gw* (Storage Node, Admin Node y Gateway Node).
- **Número de nodo:** Si un sitio contiene más de un nodo de un tipo concreto, añade un número único al nombre de cada nodo.

Piénsatelo dos veces antes de añadir detalles específicos a los nombres que puedan cambiar con el tiempo. Por ejemplo, no incluyas direcciones IP en los nombres de nodo porque estas direcciones pueden cambiar. Del mismo modo, las ubicaciones de rack o los números de modelo de los dispositivos pueden cambiar si mueves el equipo o actualizas el hardware.

Ejemplos de nombres para mostrar

Supongamos que tu sistema StorageGRID cuenta con tres centros de datos y que cada uno de ellos tiene nodos de diferentes tipos. Tus nombres de visualización podrían ser tan sencillos como estos:

- **Grid:** StorageGRID Deployment

- **Primer sitio:** Data Center 1

- dc1-adm1
- dc1-s1
- dc1-s2
- dc1-s3
- dc1-gw1

- **Segundo sitio:** Data Center 2

- dc2-adm2
- dc2-s1
- dc2-s2
- dc2-s3

- **Tercer sitio:** Data Center 3

- dc3-s1
- dc3-s2
- dc3-s3

Agrega o actualiza los nombres de visualización de StorageGRID

Puedes usar este procedimiento para añadir o actualizar los nombres de visualización que se usan para tu grid, tus sitios y tus nodos. Puedes cambiar el nombre de un solo elemento, de varios elementos o incluso de todos los elementos al mismo tiempo. Definir o actualizar un nombre de visualización no afecta en nada el funcionamiento de StorageGRID.

Antes de empezar

- Desde cualquier nodo de administración, inicias sesión en Grid Manager usando una ["navegador web compatible"](#).
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- Tienes la frase de contraseña de aprovisionamiento.
- Conoces los requisitos y las prácticas recomendadas para los nombres de visualización. Consulta ["Cambiar el nombre de la grid, los sitios y los nodos"](#).

Cómo cambiar el nombre de una grid, sitios o nodos

Puedes cambiar el nombre de tu sistema StorageGRID, de uno o varios sitios o de uno o varios nodos.

Puedes utilizar un nombre de visualización que haya sido utilizado anteriormente por otro nodo, siempre y cuando el cambio de nombre no dé lugar a un nombre de visualización o un nombre de sistema duplicado.

Selecciona los elementos que deseas renombrar

Para empezar, selecciona los elementos que quieres renombrar.

Pasos

1. Selecciona **Mantenimiento > Tareas > Cambiar nombre de la cuadrícula, los sitios y los nodos**.
2. En el paso **Seleccionar nombres**, selecciona los elementos a los que quieras cambiar el nombre.

Elemento que hay que modificar	Instrucción
Los nombres de todo (o casi todo) en tu sistema	a. Selecciona Seleccionar todo . b. Opcionalmente, desmarca cualquier elemento que no quieras renombrar.
Nombre de la grid	Selecciona la casilla para la cuadrícula.
Nombre de un sitio y de algunos o todos sus nodos	a. Marca la casilla de selección en el encabezado de la tabla para el sitio. b. Si lo deseas, desmarca los nodos que no quieras renombrar.
Nombre de un sitio	Marca la casilla correspondiente al sitio.
Nombre de un nodo	Marca la casilla de verificación del nodo.

3. Selecciona **Continuar**.
4. Revisa la tabla, que incluye los elementos que seleccionaste.
 - La columna **Nombre de visualización** muestra el nombre actual de cada elemento. Si nunca se ha cambiado el nombre del elemento, su nombre de visualización es el mismo que su nombre de sistema.
 - La columna **Nombre del sistema** muestra el nombre que introdujiste para cada elemento durante la instalación. Los nombres de los sistemas se utilizan para operaciones internas de StorageGRID y no se pueden cambiar. Por ejemplo, el nombre del sistema de un nodo podría ser su hostname.
 - La columna **Tipo** indica el tipo del elemento: Grid, Site o el tipo específico de nodo.

Proponer nuevos nombres

En el paso **Proponer nuevos nombres**, puedes introducir un nombre de visualización para cada elemento de forma individual o puedes cambiar los nombres de los elementos de forma masiva.

Renombrar elementos uno por uno

Sigue estos pasos para introducir un nombre de visualización para cada elemento al que quieras cambiar el nombre.

Pasos

1. En el campo **Nombre para mostrar**, introduce un nombre propuesto para cada elemento de la lista.

Consulta "[Cambiar el nombre de la grid, los sitios y los nodos](#)" para conocer los requisitos de nomenclatura.

2. Para eliminar los elementos que no quieras renombrar, selecciona  en la columna **Eliminar de la lista**.

Si no vas a proponer un nuevo nombre para un elemento, debes eliminarlo de la tabla.

3. Cuando hayas propuesto nuevos nombres para todos los elementos de la tabla, selecciona **Renombrar**.

Aparece un mensaje de éxito. Los nuevos nombres de visualización ya se utilizan en todo Grid Manager.

Renombrar elementos de forma masiva

Utiliza la herramienta de renombrado masivo si los nombres de los elementos contienen una cadena común que quieras sustituir por otra diferente.

Pasos

1. En el paso **Proponer nuevos nombres**, selecciona **Usar la herramienta de renombrado masivo**.

La **Vista previa de cambio de nombre** incluye todos los elementos que se mostraron en el paso **Proponer nuevos nombres**. Puedes utilizar la vista previa para ver cómo quedarán los nombres de visualización después de que reemplaces una cadena compartida.

2. En el campo **Cadena actual**, introduce la cadena compartida que deseas sustituir. Por ejemplo, si la cadena que deseas sustituir es `Data-Center-1`, introduce **Data-Center-1**.

A medida que escribes, tu texto se resalta dondequiera que se encuentre en los nombres de la izquierda.

3. Selecciona  para eliminar los elementos que no quieras renombrar con esta herramienta.

Por ejemplo, supón que quieres cambiar el nombre de todos los nodos que contienen la cadena `Data-Center-1`, pero no quieres cambiar el nombre del sitio `Data-Center-1` en sí. Selecciona  para quitar el sitio de la vista previa del 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**, introduce la cadena de sustitución que quieras utilizar en su lugar. Por ejemplo, introduce **DC1**.

Consulta "[Cambiar el nombre de la grid, los sitios y los nodos](#)" para conocer los requisitos de nomenclatura.

A medida que introduces la cadena de sustitución, los nombres de la izquierda se van actualizando, así que puedes comprobar que los nuevos nombres serán correctos.

1353

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 estés satisfecho con los nombres que aparecen en la vista previa, selecciona **Add names** para añadir los nombres a la tabla para el paso **Proponer nuevos nombres**.
6. Realiza los cambios adicionales que sean necesarios o selecciona **X** para eliminar los elementos que no quieras renombrar.
7. Cuando estés listo para cambiar el nombre de todos los elementos de la tabla, selecciona **Renombrar**.

Aparece un mensaje de éxito. Los nuevos nombres de visualización ya se usan en todo Grid Manager.

Descarga el paquete de recuperación

Cuando hayas terminado de cambiar los nombres de los elementos, descarga y guarda un nuevo paquete de recuperación. Los nuevos nombres de visualización de los elementos cuyos nombres has cambiado se incluyen en el `Passwords.txt` archivo.

Pasos

1. Introduce la contraseña de aprovisionamiento.
2. Selecciona **Descargar paquete de recuperación**.

La descarga comienza de inmediato.
3. Cuando finalice la descarga, abre el `Passwords.txt` archivo para ver el nombre del servidor de todos los nodos y los nombres de visualización de los nodos a los que se les haya cambiado el nombre.
4. Copia el archivo `sgws-recovery-package-id-revision.zip` en dos ubicaciones seguras y distintas.



El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

5. Selecciona **Finalizar** para volver al primer paso.

Restablecer los nombres que aparecen en pantalla a los nombres del sistema

Puedes restablecer el nombre de sistema original de una grid, un sitio o un nodo al que se le haya cambiado el nombre. Cuando restableces el nombre de sistema de un elemento, las páginas de Grid Manager y otras ubicaciones de StorageGRID ya no muestran un **Nombre para mostrar** para ese elemento. Solo se muestra el nombre de sistema del elemento.

Pasos

1. Selecciona **Mantenimiento > Tareas > Cambiar nombre de la cuadrícula, los sitios y los nodos**.
2. En el paso **Seleccionar nombres**, selecciona cualquier elemento que quieras revertir a los nombres del sistema.
3. Selecciona **Continuar**.
4. En el paso **Proponer nuevos nombres**, restablece los nombres de visualización a los nombres del sistema de forma individual o en bloque.

Restablecer la nomenclatura del sistema de forma individual

- a. Copia el nombre original del sistema de cada elemento y pégalo en el campo **Nombre para mostrar**, o selecciona  para eliminar los elementos que no quieras restaurar.

Para restablecer un nombre de visualización, el nombre del sistema debe aparecer en el campo **Nombre de visualización**, pero el nombre no distingue entre mayúsculas y minúsculas.

- b. Selecciona **Renombrar**.

Aparece un mensaje de éxito. Los nombres de visualización de estos elementos ya no se usan.

Restablecer la nomenclatura del sistema en lote

- a. En el paso **Proponer nuevos nombres**, selecciona **Usar la herramienta de renombrado masivo**.
- b. En el campo **Cadena actual**, introduce la cadena del nombre para mostrar que deseas reemplazar.
- c. En el campo **Nueva cadena**, introduce la cadena de nombre del sistema que quieras utilizar en su lugar.
- d. Selecciona **Add names** para añadir los nombres a la tabla en el paso **Propose new names**.
- e. Comprueba que cada entrada del campo **Nombre para mostrar** coincida con el nombre del campo **Nombre del sistema**. Realiza los cambios que desees o selecciona  para eliminar los elementos que no quieras revertir.

Para restablecer un nombre de visualización, el nombre del sistema debe aparecer en el campo **Nombre de visualización**, pero el nombre no distingue entre mayúsculas y minúsculas.

- f. Selecciona **Renombrar**.

Aparece un mensaje de éxito. Los nombres que se muestran para estos elementos ya no se usan.

5. [Descargar y guardar un nuevo paquete de recuperación](#).

Los nombres que se muestran para los elementos que has revertido ya no se incluyen en el archivo `Passwords.txt`.

Procedimientos de nodo

Procedimientos de mantenimiento de nodos StorageGRID

Es posible que tengas que llevar a cabo procedimientos de mantenimiento relacionados con nodos específicos de la red o con servicios de los nodos.

Mover ADC

El "[Servicio ADC](#)" se encuentra en algunos nodos de almacenamiento. En determinadas circunstancias de decomisionar y conversión de nodos, necesitas mover el servicio ADC a otro nodo de almacenamiento en el mismo sitio.

Convertir nodo de almacenamiento en nodo de solo datos

Puedes convertir los nodos de almacenamiento que no contengan el servicio ADC en nodos de almacenamiento solo para datos.

Reinicio, apagado y alimentación del nodo

Estos procedimientos sirven para reiniciar uno o varios nodos, para apagar y reiniciar nodos, o para apagar y volver a encender los nodos.

Reasignación de puertos

Puedes utilizar los procedimientos de reasignación de puertos para eliminar las reasignaciones de puertos de un nodo, por ejemplo, si quieres configurar un endpoint de balanceador de carga usando un puerto que se había reasignado antes.

Administrador de servidores

El Administrador de servidores se ejecuta en cada nodo de la red para supervisar el inicio y la detención de los servicios y garantizar que estos se incorporen y se retiren correctamente del sistema StorageGRID. El Administrador de servidores también supervisa los servicios en cada nodo de la red e intentará reiniciar automáticamente cualquier servicio que notifique fallos.

Para llevar a cabo los procedimientos del Administrador de servidores, normalmente necesitas acceder a la línea de comandos del nodo.



Solo debes acceder al Administrador de servidores si el soporte técnico te lo ha indicado.

Mover el servicio ADC en StorageGRID

Puedes trasladar el servicio ADC a otro nodo de almacenamiento en el mismo sitio.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- El nodo de origen contiene el servicio ADC.
- El nodo de destino no contiene el servicio ADC.
- El nodo de destino es un nodo que contiene solo metadatos o un nodo combinado (metadatos y datos de objeto).
- El nodo de origen y el nodo de destino están en el mismo sitio.

Acerca de esta tarea

Utiliza el procedimiento Move ADC cuando desees:

- Decomisionar un nodo de almacenamiento que aloja el servicio ADC
- Convertir un nodo de almacenamiento que aloja el servicio ADC en un nodo de almacenamiento solo para datos

Cuando quieras decomisionar un Storage Node o ["Convertir un nodo de almacenamiento en un nodo solo de datos"](#), primero puede que necesites usar el procedimiento Move ADC. Tendrás que asegurarte de que ["Se mantiene el quórum del ADC"](#).

Este procedimiento traslada los servicios ADC, IDNT, ACCT y RSM de un Storage Node a otro en el mismo sitio. Los servicios RSM, IDNT y ACCT dependen del servicio ADC, así que se trasladan automáticamente

cuando se traslada el servicio ADC.

Pasos

1. Anota los ID de los nodos de origen y de destino.

En la Grid Management API, el ID del nodo de origen se denomina `sourceNodeId`. El ID del nodo de destino se denomina `targetNodeId`.

2. En la parte superior del Grid Manager, selecciona el icono de ayuda y selecciona **API documentation**.
3. Selecciona **Ir a la documentación privada de la API**.
4. Selecciona la POST `/private/move-adc/start` operación. Consulta ["Realizar solicitudes a la API"](#) para más información.

Durante el procedimiento, los dos nodos se reiniciarán de forma secuencial. El nodo de origen se reinicia primero, seguido del nodo de destino.

5. Puedes usar GET `/private/move-adc` para supervisar el procedimiento. Si ocurren errores, selecciona POST `/private/move-adc/retry` para volver a intentar el procedimiento.
6. ["Descargar un paquete de recuperación"](#) una vez finalizado este procedimiento.

Convertir un nodo de almacenamiento StorageGRID en un nodo solo de datos

Para mejorar el rendimiento, puedes convertir los nodos de almacenamiento sin ADC, que son más lentos, en nodos de almacenamiento solo de datos.

Utilizar un nodo de almacenamiento exclusivamente para datos puede tener sentido si tus nodos de almacenamiento presentan características de rendimiento diferentes. Por ejemplo, para aumentar potencialmente el rendimiento, podrías tener nodos de almacenamiento destinados solo a datos, de gran capacidad y con discos giratorios, acompañados de nodos de almacenamiento destinados solo a metadatos y de alto rendimiento.

Además, puedes aumentar la capacidad de metadatos eliminando de Cassandra los nodos con poca memoria RAM, lo que incrementa el límite de capacidad de metadatos por nodo. Consulta ["Gestiona el almacenamiento de metadatos de objetos"](#).

Al convertir nodos de solo datos, la grid debe contener un mínimo de tres nodos de almacenamiento combinados o de solo metadatos por sitio.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- El nodo de almacenamiento que deseas convertir no contiene el servicio ADC, o has ["Se movió el servicio ADC"](#) a otro nodo.
- El nodo de almacenamiento no es un nodo solo de metadatos ni un nodo solo de datos.
- El nodo de almacenamiento que deseas convertir no contiene el servicio ADC, o has ["Se movió el servicio ADC"](#) a otro nodo.
- Hay suficiente espacio para metadatos en otros nodos del sitio (o has ["has ampliado tu grid"](#)) para alojar los metadatos que se migrarán desde el nodo de almacenamiento que estás convirtiendo.



- Si los metadatos que se migran a otros nodos en el mismo sitio superan el tamaño de ["espacio reservado de metadatos"](#), la grid se volverá inestable.
- Después de que inicies la conversión, no podrás expandir la grid.

Acerca de esta tarea

Sigue este procedimiento para convertir uno o varios nodos de almacenamiento combinados que no contengan el servicio ADC en nodos exclusivos de datos.

Además de convertir el nodo de almacenamiento, este procedimiento decomisiona Cassandra del nodo. Todos los metadatos migrarán a nodos de almacenamiento combinados o solo de metadatos. Dependiendo de la cantidad de metadatos que necesiten migrar, este procedimiento podría tardar hasta varios días por nodo en completarse.



Por lo general, puedes convertir hasta 10 nodos a la vez si el uso de metadatos por nodo es inferior a 1 TB. Si el uso de metadatos por nodo supera 1 TB, convierte hasta 5 nodos por procedimiento.

Pasos

1. Anota los ID de los nodos de almacenamiento que no sean de ADC y que quieras convertir.
2. En la parte superior del Grid Manager, selecciona el icono de ayuda y selecciona **API documentation**.
3. Selecciona **Ir a la documentación privada de la API**.
4. Selecciona la operación `POST /private/convert-to-data-only-node/start`. Consulta ["Realizar solicitudes a la API"](#) para más información.

Cada nodo se reiniciará durante el procedimiento.

5. Puedes usar `GET /private/convert-to-data-only-node` para monitorear el procedimiento. Si ocurren errores, selecciona `POST /private/convert-to-data-only-node/retry` para volver a intentar el procedimiento.
6. ["Descargar un paquete de recuperación"](#) una vez finalizado este procedimiento.

Procedimientos de reinicio, apagado y encendido

Realiza un reinicio progresivo de StorageGRID

Puedes realizar un reinicio progresivo para reiniciar varios nodos de la red sin provocar una interrupción del servicio.

Antes de empezar

- Has iniciado sesión en Grid Manager en el nodo de administración principal y estás utilizando un ["navegador web compatible"](#).



Debes haber iniciado sesión en el nodo de administración principal para llevar a cabo este procedimiento.

- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).

Acerca de esta tarea

Utiliza este procedimiento si necesitas reiniciar varios nodos al mismo tiempo. Por ejemplo, puedes usar este procedimiento después de cambiar el modo FIPS para el "[Política de seguridad de TLS y SSH](#)" de la grid. Cuando cambia el modo FIPS, debes reiniciar todos los nodos para que el cambio tenga efecto.



Si solo necesitas reiniciar un nodo, puedes "[reinicia el nodo desde la pestaña Tareas](#)".

Cuando StorageGRID reinicia los nodos de la red, ejecuta el comando `reboot` en cada nodo, lo que provoca que el nodo se apague y se reinicie. Todos los servicios se reinician automáticamente.

- Al reiniciar un nodo de VMware, se reinicia la máquina virtual.
- Al reiniciar un nodo de Linux, se reinicia el contenedor.
- Reiniciar un nodo del dispositivo StorageGRID reinicia el controlador de cálculo.

El procedimiento de reinicio progresivo permite reiniciar varios nodos al mismo tiempo, con las siguientes 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 su lugar, estos nodos se reinician de forma secuencial para garantizar que los grupos de alta disponibilidad, los datos de los objetos y los servicios críticos de los nodos permanezcan siempre disponibles.

Al reiniciar el nodo de administración principal, tu navegador pierde temporalmente el acceso al Grid Manager, por lo que ya no puedes supervisar el procedimiento. Por esta razón, el nodo de administración principal se reinicia al final.

Realiza un reinicio progresivo

Selecciona los nodos que desees reiniciar, revisa tu selección, inicia el procedimiento de reinicio y supervisa el progreso.

Selecciona nodos

Como primer paso, accede a la página Rolling reboot y selecciona los nodos que quieras reiniciar.

Pasos

1. Selecciona **Mantenimiento > Tareas > Reinicio progresivo**.
2. Revisa el estado de la conexión y los iconos de alerta en la columna **Node name**.



No puedes reiniciar un nodo si está desconectado de la grid. Las casillas de selección están desactivadas para los nodos con estos iconos:  o .

3. Si algún nodo tiene alertas activas, revisa la lista de alertas en la columna **Alert summary**.



Para ver todas las alertas actuales de un nodo, también puedes seleccionar el **Nodos > pestaña «Descripción general»**.

4. Opcionalmente, realiza las acciones recomendadas para resolver cualquier alerta actual.
5. Opcionalmente, si todos los nodos están conectados y quieres reiniciarlos todos, marca la casilla en la cabecera de la tabla y selecciona **Seleccionar todo**. De lo contrario, selecciona cada nodo que quieras

reiniciar.

Puedes utilizar las opciones de filtrado de la tabla para ver subconjuntos de nodos. Por ejemplo, puedes ver y seleccionar solo los Storage Nodes o todos los nodos de una ubicación determinada.

6. Selecciona **Revisar selección**.

Revisar selección

En este paso, puedes calcular cuánto tiempo podría durar el procedimiento total de reinicio y confirmar que seleccionaste los nodos correctos.

1. En la página de selección de revisión, revisa el resumen, que indica cuántos nodos se van a reiniciar y el tiempo total estimado para que todos los nodos se reinicien.
2. Si lo deseas, para eliminar un nodo específico de la lista de reinicio, selecciona **Remove**.
3. Si lo deseas, para añadir más nodos, selecciona **Paso anterior**, selecciona los nodos adicionales y selecciona **Revisar selección**.
4. Cuando estés listo para iniciar el procedimiento de reinicio progresivo de todos los nodos seleccionados, selecciona **Reiniciar nodos**.
5. Si has seleccionado reiniciar el nodo de administración principal, lee el mensaje informativo y selecciona **Yes**.



El nodo de administración principal será el último en reiniciarse. Mientras este nodo se esté reiniciando, se perderá la conexión de tu navegador. Cuando el nodo de administración principal vuelva a estar disponible, debes volver a cargar la página de reinicio progresivo.

Supervisa un reinicio progresivo

Mientras se está ejecutando el procedimiento de reinicio progresivo, puedes supervisararlo desde el nodo de administración principal.

Pasos

1. Revisa el progreso general de la operación, que incluye la siguiente información:
 - Número de nodos reiniciados
 - Número de nodos que se están reiniciando
 - Número de nodos que quedan por reiniciar
2. Consulta la tabla para cada tipo de nodo.

Las tablas muestran una barra de progreso de la operación en cada nodo y muestran la fase de reinicio de ese nodo, que puede ser una de estas:

- Esperando para reiniciar
- Detener servicios
- Reinicio del sistema
- Iniciando servicios
- Reinicio completado

Detener el procedimiento de reinicio progresivo

Puedes detener el procedimiento de reinicio progresivo desde el nodo de administración principal. Al detener el procedimiento, los nodos que tengan el estado "Deteniendo servicios", "Reiniciando sistema" o "Iniciando servicios" completarán la operación de reinicio. Sin embargo, estos nodos ya no se rastrearán como parte del procedimiento.

Pasos

1. Selecciona **Mantenimiento > Tareas > Reinicio progresivo**.
2. En el paso **Monitor reboot**, selecciona **Detener el procedimiento de reinicio**.

Reinicia el nodo StorageGRID desde la pestaña Tareas

Puedes reiniciar un nodo individual de la grid desde la pestaña Tareas en la página Nodos.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- Tienes la frase de contraseña de aprovisionamiento.
- Si vas a reiniciar el nodo de administración principal o cualquier nodo de almacenamiento, has revisado las siguientes consideraciones:
 - Al reiniciar el nodo de administración principal, tu navegador pierde temporalmente el acceso al Grid Manager.
 - Si reinicias dos o más nodos de almacenamiento en una ubicación determinada, es posible que no puedas acceder a ciertos objetos mientras dure el reinicio. Este problema puede ocurrir si alguna regla de ILM utiliza la opción de ingesta **Dual commit** (o si una regla específica **Balanced** y no es posible crear inmediatamente todas las copias necesarias). En este caso, StorageGRID confirmará los objetos recién incorporados en dos nodos de almacenamiento del mismo sitio y evaluará ILM más tarde.
 - Para garantizar que puedas acceder a todos los objetos mientras se reinicia un nodo de almacenamiento, deja de introducir 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, ejecuta el comando `reboot` en dicho nodo, lo que provoca que este se apague y se reinicie. Todos los servicios se reinician automáticamente.

- Al reiniciar un nodo de VMware, se reinicia la máquina virtual.
- Al reiniciar un nodo de Linux, se reinicia el contenedor.
- Reiniciar un nodo del dispositivo StorageGRID reinicia el controlador de cálculo.



Si necesitas reiniciar más de un nodo, puedes usar la ["procedimiento de reinicio progresivo"](#).

Pasos

1. Selecciona **Nodos**.
2. Selecciona el nodo de la grid que quieras reiniciar.
3. Selecciona la pestaña **Tareas**.

4. Selecciona **Reiniciar**.

Aparecerá un cuadro de diálogo de confirmación. Si vas a reiniciar el nodo de administración principal, el cuadro de diálogo de confirmación te recordará que la conexión de tu navegador con el Grid Manager se interrumpirá temporalmente cuando se detengan los servicios.

5. Introduce la contraseña de aprovisionamiento y selecciona **OK**.

6. Espera a que el nodo se reinicie.

Es posible que los servicios tarden un tiempo en dejar de funcionar.

Cuando el nodo se está reiniciando, aparece el icono gris (Administrativamente Down) para el nodo en la página Nodes. Cuando todos los servicios se han iniciado de nuevo y el nodo está conectado correctamente a la grid, la página Nodes debería mostrar un estado normal (sin iconos a la izquierda del nombre de nodo), lo que indica que no hay alertas activas y que el nodo está conectado a la grid.

Reinicia el nodo StorageGRID desde el intérprete de comandos

Si necesitas supervisar más de cerca el proceso de reinicio o si no puedes acceder al Grid Manager, puedes iniciar sesión en el nodo de la red y ejecutar el comando de reinicio de Server Manager desde la línea de comandos.

Antes de empezar

Tienes el archivo `Passwords.txt`.

Pasos

1. Inicia sesión en el nodo de la grid:

- Introduce el siguiente comando: `ssh admin@grid_node_IP`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.
- Introduce el siguiente comando para pasar a ser usuario root: `su -`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Si lo deseas, detén los servicios: `service servermanager stop`

Detener los servicios es un paso opcional, aunque recomendable. El proceso de apagado de los servicios puede tardar hasta 15 minutos, por lo que quizá te interese iniciar sesión en el sistema de forma remota para supervisar dicho proceso antes de reiniciar el nodo en el siguiente paso.

3. Reinicia el nodo de grid: `reboot`

4. Cierra la sesión del intérprete de comandos: `exit`

Apaga el nodo StorageGRID

Puedes apagar un nodo de la grid desde la línea de comandos del propio nodo.

Antes de empezar

- Tienes el archivo `Passwords.txt`.

Acerca de esta tarea

Antes de llevar a cabo este procedimiento, ten en cuenta las siguientes consideraciones:

- En general, no deberías apagar más de un nodo a la vez para evitar interrupciones.
- No apagues un nodo durante un procedimiento de mantenimiento a menos que así lo indique expresamente la documentación o el soporte técnico.
- El proceso de apagado depende de dónde esté instalado el nodo, como se indica a continuación:
 - Al apagar un nodo de VMware, se apaga la máquina virtual.
 - Al apagar un nodo de Linux, se apaga el contenedor.
 - Al apagar un nodo de un dispositivo StorageGRID, se apaga el controlador de cómputo.
- Si tienes previsto apagar más de un nodo de almacenamiento en una ubicación, deja de introducir objetos en esa ubicación durante aproximadamente una hora antes de apagar los nodos.

Si alguna regla de ILM utiliza la opción de ingesta **Dual commit** (o si una regla utiliza la opción **Balanced** y no es posible crear inmediatamente todas las copias necesarias), StorageGRID confirma de inmediato cualquier objeto recién ingerido en dos nodos de almacenamiento del mismo sitio y evalúa el ILM más tarde. Si se apagan más de un nodo de almacenamiento en un sitio, es posible que no puedas acceder a los objetos recién ingeridos mientras dure el apagón. Las operaciones de escritura también podrían fallar si quedan muy pocos nodos de almacenamiento disponibles en el sitio. Consulta ["Gestiona objetos con ILM"](#).

Pasos

1. Inicia sesión en el nodo de la grid:

- Introduce el siguiente comando: `ssh admin@grid_node_IP`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.
- Introduce el siguiente comando para pasar a ser usuario root: `su -`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Detén todos los servicios: `service servermanager stop`

El apagado de los servicios puede tardar hasta 15 minutos, por lo que quizá te interese iniciar sesión en el sistema de forma remota para supervisar el proceso de apagado.

3. Si el nodo se está ejecutando en una máquina virtual de VMware o se trata de un nodo de dispositivo, ejecuta el comando de apagado: `shutdown -h now`

Realiza este paso independientemente del resultado del comando `service servermanager stop`.



Después de que ejecutes el comando `shutdown -h now` en un nodo del dispositivo, debes apagar y volver a encender el dispositivo para reiniciar el nodo.

En el caso del appliance, este comando apaga el controlador, pero el appliance sigue encendido. Debes completar el siguiente paso.

4. Si vas a apagar un nodo del appliance, sigue los pasos correspondientes a tu appliance.

SG6160

- a. Desconecta la alimentación del controlador de almacenamiento SG6100-CN.
- b. Espera a que se apague el LED azul de alimentación del controlador de almacenamiento SG6100-CN.

SGF6112

- a. Apaga la alimentación del aparato.
- b. Espera a que se apague el LED azul de alimentación.

SG6000

- a. Espera a que se apague el LED verde «Cache Active» situado en la parte trasera de los controladores de almacenamiento.

Este LED se enciende cuando es necesario escribir datos almacenados en la caché en las unidades. Debes esperar a que este LED se apague antes de apagar la alimentación.

- b. Desconecta el aparato de la corriente y espera a que se apague el LED azul de encendido.

SG5800

- a. Espera a que se apague el LED verde «Cache Active» situado en la parte trasera del controlador de almacenamiento.

Este LED se enciende cuando es necesario escribir datos almacenados en la caché en las unidades. Debes esperar a que este LED se apague antes de apagar la alimentación.

- b. En la página de inicio de SANtricity System Manager, selecciona **Ver operaciones en curso**.
- c. Asegúrate de que todas las operaciones hayan finalizado antes de continuar con el siguiente paso.
- d. Apaga los dos interruptores de encendido del shelf del controlador y espera a que se apaguen todos los LED del shelf del controlador.

SG5700

- a. Espera a que se apague el LED verde «Cache Active» situado en la parte trasera del controlador de almacenamiento.

Este LED se enciende cuando es necesario escribir datos almacenados en la caché en las unidades. Debes esperar a que este LED se apague antes de apagar la alimentación.

- b. Apaga el aparato y espera a que se detenga toda la actividad de los LED y de la pantalla de siete segmentos.

SG100 o SG1000

- a. Apaga la alimentación del aparato.
- b. Espera a que se apague el LED azul de alimentación.

Apaga un host StorageGRID

Antes de apagar un host, debes detener los servicios en todos los nodos de grid de ese host.

Pasos

1. Inicia sesión en el nodo de la grid:

- a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
- b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
- d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

2. Detén todos los servicios que se estén ejecutando en el nodo: `service servermanager stop`

El apagado de los servicios puede tardar hasta 15 minutos, por lo que quizá te interese iniciar sesión en el sistema de forma remota para supervisar el proceso de apagado.

3. Repite los pasos 1 y 2 para cada nodo en el host.

4. Si tienes un host Linux:

- a. Inicia sesión en el sistema operativo del host.
- b. Detén el nodo: `storagegrid node stop`
- c. Apaga el sistema operativo del host.

5. Si el nodo se está ejecutando en una máquina virtual de VMware o se trata de un nodo de dispositivo, ejecuta el comando de apagado: `shutdown -h now`

Realiza este paso independientemente del resultado del comando `service servermanager stop`.



Después de que ejecutes el comando `shutdown -h now` en un nodo del dispositivo, debes apagar y volver a encender el dispositivo para reiniciar el nodo.

En el caso del appliance, este comando apaga el controlador, pero el appliance sigue encendido. Debes completar el siguiente paso.

6. Si vas a apagar un nodo del appliance, sigue los pasos correspondientes a tu appliance.

SG6160

- a. Desconecta la alimentación del controlador de almacenamiento SG6100-CN.
- b. Espera a que se apague el LED azul de alimentación del controlador de almacenamiento SG6100-CN.

SGF6112

- a. Apaga la alimentación del aparato.
- b. Espera a que se apague el LED azul de alimentación.

SG6000

- a. Espera a que se apague el LED verde «Cache Active» situado en la parte trasera de los controladores de almacenamiento.

Este LED se enciende cuando es necesario escribir datos almacenados en la caché en las unidades. Debes esperar a que este LED se apague antes de apagar la alimentación.

- b. Desconecta el aparato de la corriente y espera a que se apague el LED azul de encendido.

SG5800

- a. Espera a que se apague el LED verde «Cache Active» situado en la parte trasera del controlador de almacenamiento.

Este LED se enciende cuando es necesario escribir datos almacenados en la caché en las unidades. Debes esperar a que este LED se apague antes de apagar la alimentación.

- b. En la página de inicio de SANtricity System Manager, selecciona **Ver operaciones en curso**.
- c. Asegúrate de que todas las operaciones hayan finalizado antes de continuar con el siguiente paso.
- d. Apaga los dos interruptores de encendido del shelf del controlador y espera a que se apaguen todos los LED del shelf del controlador.

SG5700

- a. Espera a que se apague el LED verde «Cache Active» situado en la parte trasera del controlador de almacenamiento.

Este LED se enciende cuando es necesario escribir datos almacenados en la caché en las unidades. Debes esperar a que este LED se apague antes de apagar la alimentación.

- b. Apaga el aparato y espera a que se detenga toda la actividad de los LED y de la pantalla de siete segmentos.

SG110 o SG1100

- a. Apaga la alimentación del aparato.
- b. Espera a que se apague el LED azul de alimentación.

SG100 o SG1000

- a. Apaga la alimentación del aparato.
- b. Espera a que se apague el LED azul de alimentación.

7. Cierra la sesión del intérprete 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 servicios SG110 y SG1100"](#)
- ["Aparatos de servicios SG100 y SG1000"](#)

Apaga y enciende todos los nodos StorageGRID

Es posible que tengas que apagar todo tu sistema StorageGRID, por ejemplo, si vas a trasladar un centro de datos. Estos pasos ofrecen una descripción a grandes rasgos de la secuencia recomendada para llevar a cabo un apagado y un arranque controlados.

Cuando apagas todos los nodos de un sitio o grid, no podrás acceder a los objetos ingeridos mientras los Storage Nodes estén fuera de línea.

Detén los servicios y apaga los nodos de la red

Antes de apagar un sistema StorageGRID, debes detener todos los servicios que se estén ejecutando en cada nodo de la red y luego apagar todas las máquinas virtuales de VMware, los motores de contenedores y los dispositivos StorageGRID.

Acerca de esta tarea

Detén primero los servicios en los nodos de administración y los nodos de puerta de enlace, y después detén los servicios en los nodos de almacenamiento.

Este enfoque te 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 único host incluye más de un nodo de la grid, no apagues el host hasta que hayas detenido todos los nodos de ese host. Si el host incluye el nodo de administración principal, apaga ese host al final.



Si es necesario, puedes ["migrar nodos de un host Linux a otro"](#) para realizar tareas de mantenimiento del host sin afectar la funcionalidad ni la disponibilidad de tu grid.

Pasos

1. El acceso externo por SSH está bloqueado de forma predeterminada. Si es necesario, ["permitir el acceso de forma temporal"](#).
2. Impide que todas las aplicaciones cliente accedan a la grid.
3. Inicia sesión en cada Gateway Node:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.

c. Introduce el siguiente comando para pasar a ser usuario root: `su -`

d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

4. Detén todos los servicios que se están ejecutando en el nodo: `service servermanager stop`

El apagado de los servicios puede tardar hasta 15 minutos, por lo que quizá te interese iniciar sesión en el sistema de forma remota para supervisar el proceso de apagado.

5. Repite los dos pasos anteriores para detener los servicios en todos los Storage Nodes y en los Admin Nodes que no sean primarios.

Puedes detener los servicios de estos nodos en cualquier orden.



Si ejecutas el comando `service servermanager stop` para detener los servicios en un nodo de almacenamiento del dispositivo, deberás apagar y volver a encender el dispositivo para reiniciar el nodo.

6. Para el nodo de administración principal, repite los pasos para [iniciar sesión en el nodo](#) y [detener todos los servicios en el nodo](#).
7. Para los nodos que se ejecutan en hosts Linux:
- a. Inicia sesión en el sistema operativo del host.
 - b. Detén el nodo: `storagegrid node stop`
 - c. Apaga el sistema operativo del host.

8. Para los nodos que se ejecutan en máquinas virtuales de VMware y para los Storage Nodes de los dispositivos, ejecuta el comando de apagado: `shutdown -h now`

Realiza este paso independientemente del resultado del comando `service servermanager stop`.

En el dispositivo, este comando apaga el controlador de cálculo, pero el dispositivo sigue encendido. Debes completar el siguiente paso.

9. Si tienes nodos de appliance, sigue los pasos para tu appliance.

SG110 o SG1100

- a. Apaga la alimentación del aparato.
- b. Espera a que se apague el LED azul de alimentación.

SG100 o SG1000

- a. Apaga la alimentación del aparato.
- b. Espera a que se apague el LED azul de alimentación.

SG6160

- a. Desconecta la alimentación del controlador de almacenamiento SG6100-CN.
- b. Espera a que se apague el LED azul de alimentación del controlador de almacenamiento SG6100-CN.

SGF6112

- a. Apaga la alimentación del aparato.
- b. Espera a que se apague el LED azul de alimentación.

SG6000

- a. Espera a que se apague el LED verde «Cache Active» situado en la parte trasera de los controladores de almacenamiento.

Este LED se enciende cuando es necesario escribir datos almacenados en la caché en las unidades. Debes esperar a que este LED se apague antes de apagar la alimentación.

- b. Desconecta el aparato de la corriente y espera a que se apague el LED azul de encendido.

SG5800

- a. Espera a que se apague el LED verde «Cache Active» situado en la parte trasera del controlador de almacenamiento.

Este LED se enciende cuando es necesario escribir datos almacenados en la caché en las unidades. Debes esperar a que este LED se apague antes de apagar la alimentación.

- b. En la página de inicio de SANtricity System Manager, selecciona **Ver operaciones en curso**.
- c. Asegúrate de que todas las operaciones hayan finalizado antes de continuar con el siguiente paso.
- d. Apaga los dos interruptores de encendido del shelf del controlador y espera a que se apaguen todos los LED del shelf del controlador.

SG5700

- a. Espera a que se apague el LED verde «Cache Active» situado en la parte trasera del controlador de almacenamiento.

Este LED se enciende cuando es necesario escribir datos almacenados en la caché en las unidades. Debes esperar a que este LED se apague antes de apagar la alimentación.

- b. Apaga el aparato y espera a que se detenga toda la actividad de los LED y de la pantalla de siete segmentos.

10. Si es necesario, cierra la sesión del intérprete de comandos: `exit`

La grid StorageGRID ya se ha apagado.

11. Si has permitido el acceso SSH externo, "[bloquear el acceso](#)" cuando hayas terminado de apagar los nodos.

Iniciar los nodos de la red



Si toda la grid ha estado inactiva durante más de 15 días, debes ponerte en contacto con soporte técnico antes de poner en marcha cualquier nodo de la grid. No intentes los procedimientos de recuperación que reconstruyen los datos de Cassandra. Hacerlo podría provocar la pérdida de datos.

Si es posible, enciende los nodos de la red en este orden:

- Enciende primero los nodos de administración.
- Conecta los nodos de Gateway al final.



Si un host incluye varios nodos de grid, los nodos volverán a estar en línea automáticamente cuando enciendas el host.

Pasos

1. Enciende los hosts para el nodo de administración principal y cualquier nodo de administración no principal.



No podrás iniciar sesión en los nodos de administración hasta que se hayan reiniciado los nodos de almacenamiento.

2. Enciende los hosts de todos los nodos de almacenamiento.

Puedes encender estos nodos en cualquier orden.

3. Enciende los hosts de todos los nodos de Gateway.

4. Inicia sesión en Grid Manager.

5. Selecciona **Nodos** y supervisa el estado de los nodos de la red. Comprueba que no haya iconos de alerta junto a los nombres de los nodos.

Información relacionada

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

Procedimientos de reasignación de puertos

Eliminar las reasignaciones de puertos en los dispositivos StorageGRID

Si deseas configurar un endpoint para el servicio Load Balancer y quieres usar un puerto que ya se haya configurado como el Mapped-To Port de una reasignación de puertos, primero debes eliminar la reasignación de puertos existente o el endpoint no será efectivo. Debes ejecutar un script en cada Admin Node y Gateway Node 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 necesitas conservar algunas de las reasignaciones, ponte en contacto con el soporte técnico.

Para obtener información sobre cómo configurar los puntos de conexión del equilibrador de carga, consulta ["Configurar los puntos de conexión del equilibrador de carga"](#).



Si la reasignación de puertos permite el acceso de los clientes, reconfigura el cliente para que use un puerto diferente como punto final del equilibrador de carga para evitar la pérdida de servicio. De lo contrario, eliminar la asignación de puertos resultará en la pérdida de acceso de los clientes y debe programarse adecuadamente.



Este procedimiento no funciona en un sistema StorageGRID implementado como contenedor en hosts «bare metal». Consulta las instrucciones para ["Eliminando las reasignaciones de puertos en hosts bare metal"](#).

Pasos

1. El acceso externo por SSH está bloqueado de forma predeterminada. Si es necesario, ["permitir el acceso de forma temporal"](#).
2. Inicia sesión en el nodo.
 - a. Introduce 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 contenedores en el que se ejecuta StorageGRID.

- b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
- d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

3. Ejecuta el siguiente script: `remove-port-remap.sh`
4. Reinicia el nodo: `reboot`
5. Cierra la sesión del intérprete de comandos: `exit`
6. Repite estos pasos en cada Admin Node y Gateway Node que tenga puertos reasignados en conflicto.
7. Si has permitido el acceso SSH externo, ["bloquear el acceso"](#) cuando hayas terminado de eliminar las

reasignaciones de puertos.

Eliminar la reasignación de puertos StorageGRID en hosts bare metal

Si deseas configurar un endpoint para el servicio Load Balancer y quieres usar un puerto que ya se haya configurado como el Mapped-To Port de una reasignación de puertos, primero debes eliminar la reasignación de puertos existente o el endpoint no será efectivo.

Acerca de esta tarea

Si estás ejecutando StorageGRID en hosts bare metal, sigue este procedimiento en lugar del procedimiento general para eliminar las reasignaciones de puertos. Debes editar el archivo de configuración de cada Admin Node y Gateway Node 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 necesitas conservar algunas de las reasignaciones, ponte en contacto con el soporte técnico.

Para obtener información sobre cómo configurar los puntos finales del equilibrador de carga, consulta las instrucciones para la administración de StorageGRID.



Este procedimiento puede provocar una interrupción temporal del servicio mientras se reinician los nodos.

Pasos

1. Inicia sesión en el host que aloja el nodo. Inicia sesión como root o con una cuenta que tenga permisos de sudo.
2. Ejecuta el siguiente comando para desactivar temporalmente el nodo: `sudo storagegrid node stop node-name`
3. Utilizando un editor de texto como vim o pico, edita el archivo de configuración del nodo.

El archivo de configuración del nodo se encuentra en `/etc/storagegrid/nodes/node-name.conf`.

4. Busca la sección del archivo de configuración del nodo que contiene las reasignaciones de puertos.

Fíjate en 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. Edita las entradas PORT_REMAP y PORT_REMAP_INBOUND para eliminar las reasignaciones de puertos.

```

PORT_REMAP =
PORT_REMAP_INBOUND =

```

6. Ejecuta el siguiente comando para validar los cambios realizados en el archivo de configuración del nodo:


```
sudo storagegrid node validate node-name
```

Soluciona cualquier error o advertencia antes de pasar al siguiente paso.

7. Ejecuta el siguiente comando para reiniciar el nodo sin reasignaciones de puertos:

```
sudo storagegrid node start node-name
```
8. Inicia sesión en el nodo como admin usando la contraseña que aparece en el archivo `Passwords.txt`.
9. Comprueba 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. Espera hasta que todos los servicios tengan el estado «En ejecución» o «Verificado».
- c. Salir de la pantalla de estado:Ctrl+C

10. Repite estos pasos en cada Admin Node y Gateway Node que tenga puertos reasignados en conflicto.

Procedimientos de Administrador de servidores

Ver el estado y la versión de StorageGRID Administrador de servidores

Para cada nodo de la red, puedes consultar el estado actual y la versión de Administrador de servidores que se está ejecutando en ese nodo de la red. También puedes consultar el estado actual de todos los servicios que se están ejecutando en ese nodo de la red.

Antes de empezar

Tienes el archivo `Passwords.txt`.

Pasos

1. Inicia sesión en el nodo de la grid:

- a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
- b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
- d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

2. Consulta el estado actual del Administrador de servidores en el nodo de la red: **service servermanager status**

Se muestra el estado actual del Administrador de servidores en el nodo de la red (en ejecución o no). Si el estado del Administrador de servidores es `running`, se indica el tiempo que lleva en ejecución desde la última vez que se inició. Por ejemplo:

```
servermanager running for 1d, 13h, 0m, 30s
```

3. Ver la versión actual del Administrador de servidores que se está ejecutando en un nodo de la red: **service servermanager version**

Se indica la versión actual. Por ejemplo:

```
11.1.0-20180425.1905.39c9493
```

4. Cierra la sesión del intérprete de comandos: **exit**

Ver el estado actual de todos los servicios de StorageGRID

Puedes consultar en cualquier momento el estado actual de todos los servicios que se están ejecutando en un nodo de la red.

Antes de empezar

Tienes el archivo `Passwords.txt`.

Pasos

1. Inicia sesión en el nodo de la grid:

- a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
- b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
- d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Ver el estado de todos los servicios que se están ejecutando en el nodo de la red: `storagegrid-status`

Por ejemplo, la salida correspondiente al nodo de administración principal muestra que el estado actual de los servicios AMS, CMN y NMS es En ejecución. Esta salida se actualiza de inmediato si cambia el estado de un servicio.

```
Host Name          190-ADM1
IP Address
Operating System Kernel 4.9.0      Verified
Operating System Environment Debian 9.4   Verified
StorageGRID Webscale Release 11.1.0     Verified
Networking          Verified
Storage Subsystem    Verified
Database Engine      5.5.9999+default Running
Network Monitoring   11.1.0     Running
Time Synchronization 1:4.2.8p10+dfsg Running
ams                  11.1.0     Running
cmn                  11.1.0     Running
nms                  11.1.0     Running
ssm                  11.1.0     Running
mi                   11.1.0     Running
dynip                11.1.0     Running
nginx                1.10.3     Running
tomcat               8.5.14     Running
grafana              4.2.0      Running
mgmt api              11.1.0     Running
prometheus           1.5.2+ds   Running
persistence          11.1.0     Running
ade exporter         11.1.0     Running
attrDownPurge        11.1.0     Running
attrDownSamp1        11.1.0     Running
attrDownSamp2        11.1.0     Running
node exporter        0.13.0+ds  Running
```

3. Vuelve a la línea de comandos, pulsa **Ctrl+C**.
4. Si lo deseas, puedes consultar un informe estático de todos los servicios que se están ejecutando 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. Cierra la sesión del intérprete de comandos: `exit`

Inicia el Administrador de servidores StorageGRID y todos los servicios

Es posible que tengas que iniciar el Administrador de servidores, lo que también inicia todos los servicios del nodo de la grid.

Antes de empezar

Tienes el archivo `Passwords.txt`.

Acerca de esta tarea

Iniciar el Administrador de servidores en un nodo de la red donde ya se está ejecutando provoca un reinicio del Administrador de servidores y de todos los servicios en el nodo de la red.

Pasos

1. Inicia sesión en el nodo de la grid:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.
2. Inicia el Administrador de servidores: `service servermanager start`
3. Cierra la sesión del intérprete de comandos: `exit`

Reinicia el Administrador de servidores StorageGRID y todos los servicios

Es posible que tengas que reiniciar el Administrador de servidores y todos los servicios que se están ejecutando en un nodo de grid.

Antes de empezar

Tienes el archivo `Passwords.txt`.

Pasos

1. Inicia sesión en el nodo de la grid:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Reinicia el Administrador de servidores y todos los servicios del nodo de la red: `service servermanager restart`

El Administrador de servidores y todos los servicios del nodo de la red se detienen y luego se reinician.



Usar el comando `restart` es lo mismo que usar el comando `stop` seguido del comando `start`.

3. Cierra la sesión del intérprete de comandos: `exit`

Detén StorageGRID Administrador de servidores y todos los servicios

Administrador de servidores está diseñado para estar siempre en ejecución, pero es posible que tengas que detener Administrador de servidores y todos los servicios que se ejecutan en un nodo de la red.

Antes de empezar

Tienes el archivo `Passwords.txt`.

Pasos

1. Inicia sesión en el nodo de la grid:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Detén el Administrador de servidores y todos los servicios que se estén ejecutando en el nodo de la red:
`service servermanager stop`

El Administrador de servidores y todos los servicios que se ejecutan en el nodo de la red se cierran de forma controlada. Los servicios pueden tardar hasta 15 minutos en cerrarse.

3. Cierra la sesión del intérprete de comandos: `exit`

Ver el estado actual de un servicio StorageGRID

Puedes ver el estado actual de un servicio que se está ejecutando en un nodo de la grid en cualquier momento.

Antes de empezar

Tienes el archivo `Passwords.txt`.

Pasos

1. Inicia sesión en el nodo de la grid:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`

- b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
- d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Ver el estado actual de un servicio que se está ejecutando en un nodo de la grid: ``service servicename status`` Se muestra el estado actual del servicio solicitado que se está ejecutando en el nodo de la grid (en ejecución o no). Por ejemplo:

```
cmn running for 1d, 14h, 21m, 2s
```

3. Cierra la sesión del intérprete de comandos: **`exit`**

Detén un servicio StorageGRID

Algunos procedimientos de mantenimiento requieren que detengas un único servicio mientras los demás servicios del nodo de la grid siguen en funcionamiento. Solo detén servicios individuales cuando un procedimiento de mantenimiento te lo indique.

Antes de empezar

Tienes el archivo `Passwords.txt`.

Acerca de esta tarea

Si sigues estos pasos para «detener administrativamente» un servicio, Administrador de servidores no reiniciará automáticamente dicho servicio. Debes iniciar el servicio manualmente o reiniciar Administrador de servidores.

Si necesitas detener el servicio LDR en un nodo de almacenamiento, ten en cuenta que puede tardar un rato en detenerse si hay conexiones activas.

Pasos

1. Inicia sesión en el nodo de la grid:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Detener un servicio concreto: `service servicename stop`

Por ejemplo:

```
service ldr stop
```



Los servicios pueden tardar hasta 11 minutos en detenerse.

3. Cierra la sesión del intérprete de comandos: `exit`

Información relacionada

["Forzar la finalización del servicio"](#)

Forzar que un servicio de StorageGRID se termine

Si necesitas detener un servicio de forma inmediata, puedes utilizar el comando `force-stop`.

Antes de empezar

Tienes el archivo `Passwords.txt`.

Pasos

1. Inicia sesión en el nodo de la grid:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador 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 cerrar el servicio.

3. Cierra la sesión del intérprete de comandos: `exit`

Iniciar o reiniciar un servicio de StorageGRID

Es posible que tengas que iniciar un servicio que se haya detenido, o que tengas que detener y reiniciar un servicio.

Antes de empezar

Tienes el archivo `Passwords.txt`.

Pasos

1. Inicia sesión en el nodo de la grid:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`

- b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
- d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Decide qué comando ejecutar, dependiendo de si el servicio está actualmente en ejecución o detenido.

- Si el servicio está actualmente detenido, utiliza el comando `start` para iniciar el servicio manualmente: `service servicename start`

Por ejemplo:

```
service ldr start
```

- Si el servicio se está ejecutando actualmente, usa el comando `restart` para detener el servicio y luego volver a iniciarlo: `service servicename restart`

Por ejemplo:

```
service ldr restart
```

+



Usar el comando `restart` es lo mismo que usar el comando `stop` seguido del comando `start`. Puedes ejecutar `restart` incluso si el servicio está detenido en este momento.

3. Cierra la sesión del intérprete de comandos: `exit`

Usa un archivo `StorageGRID DoNotStart`

Si estás realizando varios procedimientos de mantenimiento o configuración bajo la dirección del soporte técnico, es posible que te pidan que uses un archivo `DoNotStart` para evitar que los servicios se inicien cuando se inicia o reinicia el Administrador de servidores.



Solo debes añadir o eliminar un archivo `DoNotStart` solo si el soporte técnico te lo ha indicado.

Para impedir que se inicie un servicio, coloca un archivo `DoNotStart` en el directorio del servicio que quieres impedir que se inicie. Al iniciar, el Administrador de servidores busca el archivo `DoNotStart`. Si el archivo está presente, se impide que el servicio (y cualquier servicio dependiente de él) se inicie. Cuando se elimina el archivo `DoNotStart`, el servicio que se detuvo previamente se iniciará en el siguiente inicio o reinicio del Administrador de servidores. Los servicios no se inician automáticamente cuando se elimina el archivo `DoNotStart`.

La forma más eficaz de evitar que se reinicien todos los servicios es impedir que se inicie el servicio NTP. Todos los servicios dependen del servicio NTP y no pueden ejecutarse si el servicio NTP no está en funcionamiento.

Agrega un archivo DoNotStart para el servicio

Puedes impedir que se inicie un servicio concreto añadiendo un archivo DoNotStart al directorio de dicho servicio en un nodo de la red.

Antes de empezar

Tienes el archivo `Passwords.txt`.

Pasos

1. Inicia sesión en el nodo de la grid:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.Cuando inicias sesión como root, el indicador cambia de `$` a `#`.
2. Agrega un archivo DoNotStart: `touch /etc/sv/service/DoNotStart`

donde `service` es el nombre del servicio que quieres evitar que se inicie. Por ejemplo,

```
touch /etc/sv/ldr/DoNotStart
```

Se crea un archivo DoNotStart. No se necesita contenido en el archivo.

Cuando se reinicia el Administrador de servidores o el nodo de la grid, el Administrador de servidores se reinicia, pero el servicio no.

3. Cierra la sesión del intérprete de comandos: `exit`

Eliminar el archivo DoNotStart para el servicio

Cuando elimines un archivo DoNotStart que impide que se inicie un servicio, debes iniciar ese servicio.

Antes de empezar

Tienes el archivo `Passwords.txt`.

Pasos

1. Inicia sesión en el nodo de la grid:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.Cuando inicias sesión como root, el indicador cambia de `$` a `#`.
2. Elimina el archivo DoNotStart del directorio de servicios: `rm /etc/sv/service/DoNotStart`

donde `service` es el nombre del servicio. Por ejemplo,

```
rm /etc/sv/ldr/DoNotStart
```

3. Inicia el servicio: `service servicename start`
4. Cierra la sesión del intérprete de comandos: `exit`

Soluciona problemas del Administrador de servidores en StorageGRID

Si surge algún problema al utilizar el Administrador de servidores, comprueba su archivo de registro.

Los mensajes de error relacionados con el Administrador de servidores se registran en el archivo de registro del Administrador de servidores, que se encuentra en: `/var/local/log/servermanager.log`

Consulta este archivo para ver los mensajes de error relacionados con los fallos. Si es necesario, remite el problema al soporte técnico. Es posible que se te pida que envíes los archivos de registro al soporte técnico.

Servicio en estado de error

Si detectas que un servicio ha entrado en estado de error, intenta reiniciar el servicio.

Antes de empezar

Tienes el archivo `Passwords.txt`.

Acerca de esta tarea

El Administrador de servidores supervisa los servicios y reinicia aquellos que se hayan detenido de forma inesperada. Si un servicio falla, el Administrador de servidores intenta reiniciarlo. Si se producen tres intentos fallidos de iniciar un servicio en un plazo de cinco minutos, el servicio pasa a un estado de error. El Administrador de servidores no intenta otro reinicio.

Pasos

1. Inicia sesión en el nodo de la grid:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Comprueba el estado de error del servicio: `service servicename status`

Por ejemplo:

```
service ldr status
```

Si el servicio se encuentra en estado de error, se devuelve el siguiente mensaje: `servicename in error state`. Por ejemplo:

```
ldr in error state
```



Si el estado del servicio es `disabled`, consulta las instrucciones de ["eliminar un archivo DoNotStart de un servicio"](#).

3. Intenta solucionar el error reiniciando el servicio: `service servicename restart`

Si el servicio no se reinicia, ponte en contacto con el soporte técnico.

4. Cierra la sesión del intérprete de comandos: `exit`

Procedimientos de red

Actualiza las subredes para la red Grid de StorageGRID

StorageGRID mantiene una lista de las subredes de red que se usan para comunicar los nodos de la red Grid (eth0). Estas entradas incluyen las subredes que usa la red Grid en cada sitio de tu sistema StorageGRID, así como cualquier subred usada 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 agregas nodos de la red o un sitio nuevo en una ampliación, puede que necesites actualizar o agregar subredes a la red Grid.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- Tienes la frase de contraseña de aprovisionamiento.
- Dispones de las direcciones de red, en notación CIDR, de las subredes que desees configurar.

Acerca de esta tarea

Si estás llevando a cabo una actividad de ampliación que incluye la incorporación de una nueva subred, debes añadir dicha subred a la lista de subredes de Grid Network antes de iniciar el procedimiento de ampliación. De lo contrario, tendrás que cancelar la ampliación, añadir la nueva subred e iniciar de nuevo la ampliación.

No utilices subredes que contengan las siguientes direcciones IPv4 para la Grid Network, Admin Network o Client Network de ningún nodo:

- 192.168.130.101
- 192.168.130.121
- 192.168.131.101
- 192.168.131.121
- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 198.51.100.2
- 198.51.100.4



Por ejemplo, no utilices los siguientes rangos de subred para la Grid Network, Admin Network o Client Network 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. Selecciona **Mantenimiento > Red > Red de grid**.
2. Selecciona **Add another subnet** para añadir una nueva subred en notación CIDR.

Por ejemplo, escribe 10.96.104.0/22.

3. Introduce la contraseña de aprovisionamiento y selecciona **Guardar**.
4. Espera a que se apliquen los cambios y luego descarga un nuevo paquete de recuperación.
 - a. Selecciona **Mantenimiento > Sistema > Paquete de recuperación**.
 - b. Introduce la **frase de contraseña de aprovisionamiento**.



Debes proteger el archivo del paquete de recuperación porque contiene claves de cifrado y contraseñas que se pueden usar para obtener datos del sistema StorageGRID. También se utiliza para recuperar el nodo de administración primario.

Las subredes que has especificado se configuran automáticamente para tu sistema StorageGRID.

Editar una subred

Pasos

1. Selecciona **Mantenimiento > Red > Red de grid**.
2. Selecciona la subred que quieras editar y realiza los cambios necesarios.
3. Introduce la frase de contraseña de aprovisionamiento y selecciona **Guardar**.
4. Selecciona **Sí** en el cuadro de diálogo de confirmación.
5. Espera a que se apliquen los cambios y luego descarga un nuevo paquete de recuperación.
 - a. Selecciona **Mantenimiento > Sistema > Paquete de recuperación**.
 - b. Introduce la **frase de contraseña de aprovisionamiento**.

Eliminar una subred

Pasos

1. Selecciona **Mantenimiento > Red > Red de grid**.
2. Selecciona el icono de eliminación  junto a la subred.
3. Introduce la frase de contraseña de aprovisionamiento y selecciona **Guardar**.
4. Selecciona **Sí** en el cuadro de diálogo de confirmación.
5. Espera a que se apliquen los cambios y luego descarga un nuevo paquete de recuperación.
 - a. Selecciona **Mantenimiento > Sistema > Paquete de recuperación**.
 - b. Introduce la **frase de contraseña de aprovisionamiento**.

Configurar direcciones IP

Directrices de dirección IP de StorageGRID

Puedes realizar la configuración de red configurando las direcciones IP de los nodos de grid mediante la herramienta Change IP.

Debes utilizar la herramienta Change IP para realizar la mayoría de los cambios en la configuración de red que se estableció inicialmente durante el despliegue del grid. Es posible que los cambios realizados manualmente mediante comandos y archivos de red estándar de Linux no se propaguen a todos los servicios de StorageGRID y que no se mantengan tras las actualizaciones, reinicios o procedimientos de recuperación de nodos.



El procedimiento de cambio de IP puede ser un procedimiento disruptivo. Algunas partes de la grid podrían no estar disponibles hasta que se aplique la nueva configuración.



Si solo vas a realizar cambios en la lista de subredes de la Grid Network, utiliza el Grid Manager para añadir o modificar la configuración de red. De lo contrario, utiliza la herramienta Change IP si no puedes acceder al Grid Manager debido a un problema de configuración de red, o si estás realizando al mismo tiempo tanto un cambio en el enrutamiento de la Grid Network como otros cambios de red.



Si quieres cambiar la dirección IP de la red de la malla para todos los nodos de la malla, usa el ["procedimiento especial para cambios que afectan a toda la grid"](#).

Interfaces Ethernet

La dirección IP asignada a eth0 es siempre la dirección IP de la red Grid del nodo de la grid. La dirección IP asignada a eth1 es siempre la dirección IP de la red Admin del nodo de la grid. La dirección IP asignada a eth2 es siempre la dirección IP de la red Client del nodo de la grid.

Ten en cuenta que, en algunas plataformas, como los dispositivos StorageGRID, eth0, eth1 y eth2 pueden ser interfaces agregadas compuestas por puentes subordinados o enlaces de interfaces físicas o de VLAN. En estas plataformas, la pestaña **SSM > Resources** puede mostrar la dirección IP de la red Grid, Admin y Client asignada a otras interfaces además de eth0, eth1 o eth2.

DHCP

Solo puedes configurar DHCP durante la fase de implementación. No puedes configurar DHCP durante la configuración. Debes usar los procedimientos de cambio de dirección IP si quieres cambiar direcciones IP, máscaras de subred y puertas de enlace predeterminadas para un nodo de la red. Si usas la herramienta Change IP, las direcciones DHCP pasarán a ser estáticas.

Grupos de alta disponibilidad (HA)

- Si una interfaz de red de cliente está contenida en un grupo HA, no puedes cambiar la dirección IP de red de cliente de esa interfaz por una dirección que esté fuera de la subred configurada para el grupo HA.
- No puedes cambiar la dirección IP de la red de cliente por el valor de una dirección IP virtual existente asignada a un grupo de alta disponibilidad (HA) configurado en la interfaz de red de cliente.
- Si una interfaz de red Grid está contenida en un grupo HA, no puedes cambiar la dirección IP de red Grid de esa interfaz por una dirección que esté fuera de la subred configurada para el grupo HA.
- No puedes cambiar la dirección IP de la red Grid por el valor de una dirección IP virtual ya existente asignada a un grupo de alta disponibilidad (HA) configurado en la interfaz de red Grid.

Cambiar la configuración de la red de nodos en StorageGRID

Puedes cambiar la configuración de red de uno o varios nodos usando la herramienta Change IP. Puedes cambiar la configuración de la Grid Network, o añadir, cambiar o quitar las Admin o Client Networks.

Antes de empezar

Tienes el archivo `Passwords.txt`.

Acerca de esta tarea

Linux: Si vas a añadir un nodo a la Admin Network o a la Client Network por primera vez, y no configuraste previamente `ADMIN_NETWORK_TARGET` o `CLIENT_NETWORK_TARGET` en el archivo de configuración del nodo, debes hacerlo ahora. Consulta la StorageGRID ["instrucciones de instalación"](#) para tu sistema operativo Linux.

Dispositivos: En los dispositivos StorageGRID, si la red de cliente o de administración no se configuró en el instalador de StorageGRID durante la instalación inicial, no puedes añadir la red utilizando solo la herramienta Change IP. Primero debes ["Pon el aparato en modo de mantenimiento"](#), configurar los enlaces, devolver el dispositivo al modo de funcionamiento normal y luego usar la herramienta Change IP para modificar la configuración de red. Consulta el ["Procedimiento para configurar las conexiones de red"](#).

Puedes cambiar la dirección IP, la máscara de subred, la puerta de enlace o el valor de MTU de uno o varios nodos en cualquier red.

También puedes añadir o eliminar un nodo de una red de clientes o de una red de administración:

- Puedes añadir un nodo a una red de clientes o a una red de administración añadiendo una dirección IP/máscara de subred de esa red al nodo.
- Puedes eliminar un nodo de una red de cliente o de una red de administración borrando la dirección IP/máscara de subred de dicho nodo en esa red.

No se pueden eliminar nodos de la red Grid.



No se permite el intercambio de direcciones IP. Si necesitas intercambiar direcciones IP entre nodos de la red, debes usar una dirección IP intermedia temporal.



Si el inicio de sesión único (SSO) está habilitado en tu sistema StorageGRID y vas a cambiar la dirección IP de un nodo de administración, ten en cuenta que cualquier relación de confianza de parte dependiente que se haya configurado usando la dirección IP del nodo de administración (en lugar de su nombre de dominio completo, como se recomienda) dejará de ser válida. Ya no podrás iniciar sesión en el nodo. Justo después de cambiar la dirección IP, debes actualizar o reconfigurar la relación de confianza de la parte dependiente del nodo en Active Directory Federation Services (AD FS) con la nueva dirección IP. Consulta las instrucciones para ["configuración de SSO"](#).



Cualquier cambio que realices en la red mediante la herramienta «Change IP» se aplica al firmware del instalador de los dispositivos StorageGRID. De este modo, si se reinstala el software de StorageGRID en un dispositivo o si este se pone en modo de mantenimiento, la configuración de red será correcta.

Pasos

1. El acceso externo por SSH está bloqueado de forma predeterminada. Si es necesario, ["permitir el acceso de forma temporal"](#).
2. Inicia sesión en el nodo de administración principal:
 - a. Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

3. Inicia la herramienta «Change IP» introduciendo el siguiente comando: `change-ip`
4. Introduce la contraseña de aprovisionamiento cuando se te 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: █
```

5. Si lo deseas, selecciona **1** para elegir qué nodos actualizar. Luego selecciona una de las siguientes opciones:

- **1:** Un solo nodo: seleccionar por nombre
- **2:** Un solo nodo: selecciona primero por sitio y luego por nombre
- **3:** Un solo nodo: selecciona por la IP actual
- **4:** Todos los nodos de un sitio
- **5:** Todos los nodos de la red

Nota: Si quieres actualizar todos los nodos, deja «all» seleccionado.

Después de que hagas tu selección, aparece el menú principal y el campo **Nodos seleccionados** se actualiza para reflejar tu elección. Todas las acciones posteriores se realizan únicamente en los nodos mostrados.

6. En el menú principal, selecciona la opción **2** para editar la información de IP/máscara, puerta de enlace y MTU de los nodos seleccionados.

a. Selecciona la red en la que deseas realizar cambios:

- **1:** Red de grid
- **2:** Red de administración
- **3:** Red del cliente
- **4:** Todas las redes

Después de que hagas tu selección, la ventana de comando muestra el nombre de nodo, el nombre de la red (Grid, Admin o Client), el tipo de datos (IP/máscara, puerta de enlace o MTU) y el valor actual.

Si editas la dirección IP, la longitud del prefijo, la puerta de enlace o el MTU de una interfaz configurada mediante DHCP, la interfaz cambiará a estática. Cuando eliges cambiar una interfaz configurada por DHCP, se muestra una advertencia para informarte que la interfaz cambiará a estática.

Las interfaces configuradas como `fixed` no se pueden editar.

- b. Para establecer un nuevo valor, introdúcelo con el formato que se muestra para el valor actual.
- c. Para mantener el valor actual sin cambios, pulsa **Enter**.

- d. Si el tipo de datos es `IP/mask`, puedes eliminar la red de administración o la red de clientes del nodo introduciendo `d` o `0.0.0.0/0`.
- e. Una vez que hayas editado todos los nodos que quieras modificar, escribe `q` para volver al menú principal.

Tus cambios se mantienen en espera hasta que se borren o se apliquen.

7. Revisa tus cambios seleccionando una de las siguientes opciones:

- **5:** Muestra las modificaciones en la salida, aisladas para que solo se vea el elemento modificado. Los cambios aparecen resaltados en verde (añadidos) o en 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 las modificaciones en la salida que muestra la configuración completa. Los cambios aparecen resaltados en verde (añadidos) o en rojo (eliminaciones).



Es posible que algunas interfaces de línea de comandos muestren las adiciones y eliminaciones con formato tachado. La visualización correcta depende de que tu cliente de terminal admita las secuencias de escape VT100 necesarias.

8. Selecciona la opción **7** para validar todos los cambios.

Esta validación garantiza que no se incumplan las reglas para las redes Grid, Admin y Client, como la de no usar subredes que se solapen.

En este ejemplo, la validación detectó 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 se superó.

```
Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue
```

9. Una vez superada la validación, elige una de las siguientes opciones:

- **8:** Guarda los cambios no aplicados.

Esta opción te permite salir de la herramienta Change IP y volver a iniciarla más tarde, sin perder los cambios que aún no se hayan aplicado.

- **10:** Aplica la nueva configuración de red.

10. Si seleccionaste la opción **10**, elige una de las siguientes opciones:

- **aplicar:** Aplica los cambios de forma inmediata y reinicia automáticamente cada nodo si es necesario.

Si la nueva configuración de red no requiere ningún cambio físico en la red, puedes seleccionar **aplicar** para aplicar los cambios de inmediato. Los nodos se reiniciarán automáticamente, si es necesario. Se mostrarán los nodos que necesiten reiniciarse.

- **etapa:** Aplica los cambios la próxima vez que se reinicien manualmente los nodos.

Si necesitas realizar cambios en la configuración de red física o virtual para que la nueva configuración de red funcione, debes utilizar la opción **stage**, apagar los nodos afectados, realizar los cambios físicos necesarios en la red y reiniciar los nodos afectados. Si seleccionas **apply** sin haber realizado primero estos cambios en la red, los cambios suelen fallar.



Si utilizas la opción **stage**, debes reiniciar el nodo lo antes posible tras la preparación para minimizar las interrupciones.

- **cancelar:** No realices ningún cambio en la red por el momento.

Si no sabías que los cambios propuestos requieren reiniciar los nodos, puedes posponer los cambios para minimizar el impacto en los usuarios. Al seleccionar **cancel**, vuelves al menú principal y se conservan tus cambios para que puedas aplicarlos más tarde.

Al seleccionar **aplicar** o **preparar**, se genera un nuevo archivo de configuración de red, se lleva a cabo el aprovisionamiento y se actualizan los nodos con la nueva información operativa.

Durante el aprovisionamiento, la pantalla 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 que aplicas o preparas cambios, se genera un nuevo paquete de recuperación como resultado del cambio en la configuración de la grid.

11. Si has seleccionado **stage**, sigue estos pasos una vez finalizado el aprovisionamiento:

a. Realiza los cambios físicos o virtuales en la red que sean necesarios.

Cambios físicos en la red: Realiza los cambios físicos necesarios en la red, apagando el nodo de forma segura si es necesario.

Linux: Si vas a añadir el nodo a una red de administración o a una red de clientes por primera vez, asegúrate de haber añadido la interfaz tal y como se describe en "[Linux: Añadir interfaces a un nodo existente](#)".

a. Reinicia los nodos afectados.

12. Selecciona **0** para salir de la herramienta Cambiar IP una vez que hayas completado los cambios.

13. Descarga un nuevo paquete de recuperación desde el Grid Manager.

a. Selecciona **Mantenimiento > Sistema > Paquete de recuperación**.

b. Introduce la contraseña de aprovisionamiento.

14. Si has habilitado el acceso SSH externo, "[bloquear el acceso](#)" cuando hayas terminado de modificar la configuración de red del nodo.

Cambio temporal de la frecuencia de la PDU de LACP

Para realizar operaciones de mantenimiento en los componentes de red instalados en tu dispositivo, como actualizar el firmware de la NIC, puedes comprobar que la configuración actual de la velocidad de PDU de LACP cumple con los requisitos de sincronización de comunicación de la NIC. Puedes alternar de forma no persistente la velocidad de PDU de LACP entre rápida (espera de 1 segundo) y lenta (espera de 30 segundos), si es necesario.



Para realizar cambios permanentes en la tasa de PDU de LACP, consulta "[Configura conexiones de red](#)".

Antes de empezar

- El nodo de administración está instalado y en funcionamiento.
- Tienes el archivo `Passwords.txt`.

Pasos

1. Inicia sesión en el nodo de administración principal:

- Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.

c. Introduce el siguiente comando para pasar a ser usuario root: `su -`

d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Para comprobar la configuración actual de la tasa de PDU de LACP, introduce el siguiente comando:

```
run-each-node --parallel --port 8022 '/usr/sbin/set-lacp-rate.sh'
```

3. Para modificar temporalmente la frecuencia de PDU de LACP, introduce el siguiente comando:

```
run-each-node --parallel --port 8022 '/usr/sbin/set-lacp-rate.sh <speed>'
```

donde *<speed>* es `fast` o `slow`.

La tasa de PDU de LACP volverá a su configuración anterior en el próximo reinicio del dispositivo.

Añadir o cambiar listas de subredes en la red de administración en StorageGRID

Puedes añadir, eliminar o cambiar las subredes en la Lista de subredes de red de administración de uno o más nodos.

Antes de empezar

- Tienes el archivo `Passwords.txt`.

Puedes añadir, eliminar o cambiar subredes en todos los nodos de la lista de subredes de la red de administración.

No utilices subredes que contengan las siguientes direcciones IPv4 para la Grid Network, Admin Network o Client Network de ningún nodo:

- 192.168.130.101
- 192.168.130.121
- 192.168.131.101
- 192.168.131.121
- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 198.51.100.2
- 198.51.100.4



Por ejemplo, no utilices los siguientes rangos de subred para la Grid Network, Admin Network o Client Network 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. El acceso externo por SSH está bloqueado de forma predeterminada. Si es necesario, ["permitir el acceso de forma temporal"](#).
2. Inicia sesión en el nodo de administración principal:
 - a. Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

3. Inicia la herramienta «Change IP» introduciendo el siguiente comando: `change-ip`
4. Introduce la contraseña de aprovisionamiento cuando se te 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: █

```

5. Si lo deseas, limita las redes o los nodos en los que se realizan las operaciones. Elige una de las siguientes opciones:
 - Selecciona los nodos que deseas editar marcando **1** si quieres filtrar los nodos específicos en los que se va a realizar la operación. Selecciona una de las siguientes opciones:
 - **1:** Nodo único (seleccionar por nombre)
 - **2:** Un solo nodo (selecciona por sitio y luego por nombre)
 - **3:** Un solo nodo (seleccionar por la IP actual)
 - **4:** Todos los nodos de un sitio
 - **5:** Todos los nodos de la red
 - **0:** Volver
 - Deja «all» seleccionado. Una vez realizada la selección, aparece la pantalla del menú principal. El campo «Selected nodes» refleja tu nueva selección, y ahora todas las operaciones seleccionadas solo se realizarán en este elemento.
6. En el menú principal, selecciona la opción para editar las subredes de la Admin Network (opción **3**).
7. Elige uno de los siguientes:
 - Agrega una subred introduciendo este comando: `add CIDR`
 - Elimina una subred introduciendo este comando: `del CIDR`
 - Configura la lista de subredes introduciendo este comando: `set CIDR`



En todos los comandos, puedes introducir 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`



Puedes reducir la cantidad de texto que tienes que escribir utilizando la «flecha hacia arriba» para recuperar los valores introducidos anteriormente en el indicador de entrada actual y luego editarlos si es necesario.

El ejemplo de entrada que se muestra a continuación ilustra cómo añadir subredes a la lista de subredes de la Admin Network Subnet List:

```

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

```

8. Cuando estés listo, escribe **q** para volver a la pantalla del menú principal. Tus cambios se mantienen hasta que los borres o los apliques.



Si en el paso 3 has seleccionado alguno de los modos de selección de nodos «todos», pulsa **Intro** (sin **q**) para pasar al siguiente nodo de la lista.

9. Elige uno de los siguientes:

- Selecciona la opción **5** para mostrar los cambios en una salida aislada en la que solo se muestre el elemento modificado. Los cambios aparecen resaltados en verde (añadidos) o en rojo (eliminaciones), como se muestra en el ejemplo de salida siguiente:

```

=====
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

```

- Selecciona la opción **6** para mostrar los cambios en la salida que muestra la configuración completa. Los cambios aparecen resaltados en verde (añadidos) o en rojo (eliminaciones). **Nota:** Algunos emuladores de terminal pueden mostrar los añadidos y las eliminaciones con formato tachado.

Cuando intentas cambiar la lista de subredes, aparece 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 has asignado específicamente las subredes de los servidores NTP y DNS a una red, StorageGRID crea automáticamente una ruta de host (/32) para la conexión. Si, por ejemplo, prefieres tener una ruta /16 o /24 para la conexión saliente a un servidor DNS o NTP, debes eliminar la ruta /32 creada automáticamente y añadir las rutas que quieras. Si no eliminas la ruta de host creada automáticamente, se mantendrá después de que apliques cualquier cambio en la lista de subredes.



Aunque puedes utilizar estas rutas de host detectadas automáticamente, en general deberías configurar manualmente las rutas de DNS y NTP para asegurar la conectividad.

10. Selecciona la opción **7** para validar todos los cambios en espera.

Esta validación garantiza que se sigan las reglas para las redes Grid, Admin y Client, como usar subredes superpuestas.

11. Si lo prefieres, selecciona la opción **8** para guardar todos los cambios provisionales y volver más tarde para seguir haciendo cambios.

Esta opción te permite salir de la herramienta Change IP y volver a iniciarla más tarde, sin perder los cambios que aún no se hayan aplicado.

12. Debe realizar una de las siguientes acciones:

- Selecciona la opción **9** si quieres borrar todos los cambios sin guardar ni aplicar la nueva configuración de red.
- Selecciona la opción **10** si estás listo para aplicar los cambios y poner en marcha la nueva configuración de red. Durante la puesta en marcha, la pantalla 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
```

13. Descarga un nuevo paquete de recuperación desde el Grid Manager.

a. Selecciona **Mantenimiento > Sistema > Paquete de recuperación**.

b. Introduce la contraseña de aprovisionamiento.

14. Si has permitido el acceso SSH externo, ["bloquear el acceso"](#) cuando hayas terminado de añadir o modificar las listas de subredes.

Agrega o cambia las listas de subredes en Grid Network en StorageGRID

Puedes utilizar la herramienta Change IP para añadir o modificar subredes en la Grid Network.

Antes de empezar

- Tienes el archivo `Passwords.txt`.

Puedes añadir, eliminar o modificar subredes en la lista de subredes de la red de la grid. Los cambios afectarán al enrutamiento en todos los nodos de la grid.



Si solo vas a realizar cambios en la lista de subredes de la Grid Network, utiliza el Grid Manager para añadir o modificar la configuración de red. De lo contrario, utiliza la herramienta Change IP si no puedes acceder al Grid Manager debido a un problema de configuración de red, o si estás realizando al mismo tiempo tanto un cambio en el enrutamiento de la Grid Network como otros cambios de red.

No utilices subredes que contengan las siguientes direcciones IPv4 para la Grid Network, Admin Network o Client Network de ningún nodo:

- 192.168.130.101
- 192.168.130.121
- 192.168.131.101
- 192.168.131.121
- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 198.51.100.2
- 198.51.100.4



Por ejemplo, no utilices los siguientes rangos de subred para la Grid Network, Admin Network o Client Network 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. El acceso externo por SSH está bloqueado de forma predeterminada. Si es necesario, ["permitir el acceso"](#)

de forma temporal".

2. Inicia sesión en el nodo de administración principal:

- a. Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
- b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
- d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

3. Inicia la herramienta «Change IP» introduciendo el siguiente comando: `change-ip`

4. Introduce la contraseña de aprovisionamiento cuando se te 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: █
```

5. En el menú principal, selecciona la opción para editar las subredes para la Grid Network (opción **4**).



Los cambios en la lista de subredes de la red Grid son a nivel de grid.

6. Elige uno de los siguientes:

- Agrega una subred introduciendo este comando: `add CIDR`
- Elimina una subred introduciendo este comando: `del CIDR`
- Configura la lista de subredes introduciendo este comando: `set CIDR`



En todos los comandos, puedes introducir 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`



Puedes reducir la cantidad de texto que tienes que escribir utilizando la «flecha hacia arriba» para recuperar los valores introducidos anteriormente en el indicador de entrada actual y luego editarlos si es necesario.

El ejemplo de entrada que se muestra a continuación ilustra cómo configurar las subredes para la lista de

subredes de la Grid Network:

```
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
```

7. Cuando estés listo, escribe **q** para volver a la pantalla del menú principal. Tus cambios se mantienen hasta que los borres o los apliques.
8. Elige uno de los siguientes:
 - Selecciona la opción **5** para mostrar los cambios en una salida aislada en la que solo se muestre el elemento modificado. Los cambios aparecen resaltados en verde (añadidos) o en rojo (eliminaciones), como se muestra en el ejemplo de salida siguiente:

```
=====
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
```

- Selecciona la opción **6** para mostrar los cambios en la salida que muestra la configuración completa. Los cambios aparecen resaltados en verde (añadidos) o en rojo (eliminaciones).



Es posible que algunas interfaces de línea de comandos muestren las adiciones y eliminaciones con el formato de tachado.

9. Selecciona la opción **7** para validar todos los cambios en espera.

Esta validación garantiza que se sigan las reglas para las redes Grid, Admin y Client, como usar subredes superpuestas.

10. Si lo prefieres, selecciona la opción **8** para guardar todos los cambios provisionales y volver más tarde para seguir haciendo cambios.

Esta opción te permite salir de la herramienta Change IP y volver a iniciarla más tarde, sin perder los cambios que aún no se hayan aplicado.

11. Debe realizar una de las siguientes acciones:

- Selecciona la opción **9** si quieres borrar todos los cambios sin guardar ni aplicar la nueva configuración de red.
- Selecciona la opción **10** si estás listo para aplicar los cambios y poner en marcha la nueva configuración de red. Durante la puesta en marcha, la pantalla 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. Si seleccionaste la opción **10** al hacer cambios en la red de cuadrícula, elige una de las siguientes opciones:

- **aplicar**: Aplica los cambios de forma inmediata y reinicia automáticamente cada nodo si es necesario.

Si la nueva configuración de red va a funcionar simultáneamente con la antigua configuración de red sin ningún cambio externo, puedes usar la opción **apply** para un cambio de configuración totalmente automatizado.

- **stage**: Aplica los cambios la próxima vez que se reinicien los nodos.

Si necesitas realizar cambios en la configuración de red física o virtual para que la nueva configuración de red funcione, debes utilizar la opción **stage**, apagar los nodos afectados, realizar los cambios físicos necesarios en la red y reiniciar los nodos afectados.



Si utilizas la opción **stage**, reinicia el nodo lo antes posible tras la preparación para minimizar las interrupciones.

- **cancelar**: No realices ningún cambio en la red por el momento.

Si no sabías que los cambios propuestos requieren reiniciar los nodos, puedes posponer los cambios para minimizar el impacto en los usuarios. Al seleccionar **cancel**, vuelves al menú principal y se conservan tus cambios para que puedas aplicarlos más tarde.

Después de que aplicas o preparas cambios, se genera un nuevo paquete de recuperación como resultado del cambio en la configuración de la grid.

13. Si la configuración se detiene debido a errores, tienes las siguientes opciones disponibles:

- Para finalizar el procedimiento de cambio de IP y volver al menú principal, introduce **a**.
- Para volver a intentar la operación que falló, introduce **r**.
- Para continuar con la siguiente operación, introduce **c**.

La operación fallida se puede volver a intentar más tarde seleccionando la opción **10** (Aplicar cambios) en el menú principal. El procedimiento de cambio de IP no se completará hasta que todas las operaciones se hayan completado con éxito.

- Si has tenido que intervenir manualmente (por ejemplo, para reiniciar un nodo) y estás seguro de que

la acción que la herramienta considera fallida se ha completado correctamente, introduce **f** para marcarla como correcta y pasar a la siguiente operación.

14. Descarga un nuevo paquete de recuperación desde el Grid Manager.

- a. Selecciona **Mantenimiento > Sistema > Paquete de recuperación**.
- b. Introduce la contraseña de aprovisionamiento.



El archivo del paquete de recuperación debe protegerse porque contiene claves de cifrado y contraseñas que pueden usarse para obtener datos del sistema StorageGRID.

15. Si has permitido el acceso SSH externo, "[bloquear el acceso](#)" cuando hayas terminado de añadir o modificar las listas de subredes.

Cambiar las direcciones IP de todos los nodos en una grid de StorageGRID

Si necesitas cambiar la dirección IP de la Grid Network para todos los nodos de la grid, debes seguir este procedimiento especial. No puedes hacer un cambio de dirección IP de la Grid Network en toda la grid usando el procedimiento para cambiar nodos individuales.

Antes de empezar

- Tienes el archivo `Passwords.txt`.

Para garantizar que la red se ponga en marcha correctamente, debes realizar todos los cambios al mismo tiempo.



Este procedimiento solo se aplica a la red Grid. No puedes utilizar este procedimiento para cambiar las direcciones IP en las redes Admin o Client.

Si deseas modificar las direcciones IP y el MTU de los nodos de una única sede, sigue las "[Modificar la configuración de red del nodo](#)" instrucciones.

Pasos

1. Planifica con antelación los cambios que necesitas hacer fuera de la herramienta Change IP, como los cambios en el servidor DNS o el servidor NTP, y los cambios en la configuración del inicio de sesión único (SSO), si se usa.



Si la red no puede acceder a los servidores NTP actuales a través de las nuevas direcciones IP, añade los nuevos servidores NTP antes de llevar a cabo el procedimiento de cambio de IP.



Si la red no podrá acceder a los servidores DNS actuales con las nuevas direcciones IP, añade los nuevos servidores DNS antes de realizar el procedimiento de cambio de IP.



Si el inicio de sesión único (SSO) está habilitado para tu sistema StorageGRID y se configuraron relaciones de confianza de partes dependientes usando direcciones IP de nodos de administración (en lugar de dominios completos, como se recomienda), prepárate para actualizar o reconfigurar estas relaciones de confianza de partes dependientes en Active Directory Federation Services (AD FS) inmediatamente después de cambiar las direcciones IP. Consulta "[Configura el inicio de sesión único](#)".



Si es necesario, añade la nueva subred para las nuevas direcciones IP.

2. El acceso externo por SSH está bloqueado de forma predeterminada. Si es necesario, ["permitir el acceso de forma temporal"](#).
3. Inicia sesión en el nodo de administración principal:
 - a. Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

4. Inicia la herramienta «Change IP» introduciendo el siguiente comando: `change-ip`
5. Introduce la contraseña de aprovisionamiento cuando se te solicite.

Aparece el menú principal. Por defecto, el campo `Selected nodes` está configurado como `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: █
```

6. En el menú principal, selecciona **2** para editar la información de IP, máscara de subred, puerta de enlace y MTU de todos los nodos.
 - a. Selecciona **1** para realizar cambios en la Grid Network.

Después de que hagas tu selección, el mensaje muestra los nombres de nodo, el nombre de la Grid Network, el tipo de datos (IP/máscara, gateway o MTU) y los valores actuales.

Si editas la dirección IP, la longitud del prefijo, la puerta de enlace o el MTU de una interfaz configurada mediante DHCP, la interfaz cambiará a estática. Se muestra una advertencia antes de cada interfaz configurada mediante DHCP.

Las interfaces configuradas como `fixed` no se pueden editar.

- a. Para establecer un nuevo valor, introdúcelo con el formato que se muestra para el valor actual.
- b. Una vez que hayas editado todos los nodos que quieras modificar, escribe **q** para volver al menú principal.

Tus cambios se mantienen en espera hasta que se borren o se apliquen.

7. Revisa tus cambios seleccionando una de las siguientes opciones:

- **5:** Muestra las modificaciones en la salida, aisladas para que solo se vea el elemento modificado. Los cambios aparecen resaltados en verde (añadidos) o en 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 MTU [ 1400 ]: 0  
username-x Admin MTU [ 1400 ]: 0  
username-x Admin MTU [ 1400 ]: 0  
username-x Admin MTU [ 1400 ]: 0  
username-x Admin MTU [ 1400 ]: 0  
Press Enter to continue
```

- **6:** Muestra las modificaciones en la salida que muestra la configuración completa. Los cambios aparecen resaltados en verde (añadidos) o en rojo (eliminaciones).



Es posible que algunas interfaces de línea de comandos muestren las adiciones y eliminaciones con formato tachado. La visualización correcta depende de que tu cliente de terminal admita las secuencias de escape VT100 necesarias.

8. Selecciona la opción **7** para validar todos los cambios.

Esta validación garantiza que no se incumplan las reglas de la Grid Network, como la de no utilizar subredes que se solapen.

En este ejemplo, la validación detectó 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 se superó.


```
Validating new networking configuration... PASSED.  
Checking for Grid Network IP address swaps... PASSED.  
Press Enter to continue
```

9. Después de que la validación pase, selecciona **10** para aplicar la nueva configuración de red.
10. Selecciona **stage** para aplicar los cambios la próxima vez que se reinicien los nodos.



Debes seleccionar **stage**. No realices un reinicio progresivo, ni manualmente ni seleccionando **apply** en lugar de **stage**; la grid no se iniciará correctamente.

11. Después de que termines de hacer los cambios, selecciona **0** para salir de la herramienta Change IP.
12. Apaga todos los nodos a la vez.



Es necesario apagar toda la red, de modo que todos los nodos queden inactivos al mismo tiempo.

13. Realiza los cambios físicos o virtuales en la red que sean necesarios.
14. Comprueba que todos los nodos de la grid estén inactivos.
15. Enciende todos los nodos.
16. Después de que la red se inicie correctamente:
 - a. Si has añadido nuevos servidores NTP, elimina los valores del servidor NTP antiguo.
 - b. Si has añadido nuevos servidores DNS, elimina los valores del servidor DNS antiguo.
17. Descarga el nuevo paquete de recuperación desde el Grid Manager.
 - a. Selecciona **Mantenimiento > Sistema > Paquete de recuperación**.
 - b. Introduce la contraseña de aprovisionamiento.
18. Si has habilitado el acceso SSH externo, "[bloquear el acceso](#)" cuando hayas terminado de cambiar las direcciones IP.

Información relacionada

- ["Agrega o cambia listas de subredes en Grid Network"](#)
- ["Apagar nodo de la red"](#)

Agrega interfaces a un nodo existente

Agrega interfaces de Admin o Client a un nodo Linux en StorageGRID

Sigue estos pasos para añadir una interfaz en la red de administración o en la red de clientes a un nodo Linux después de que se haya instalado.

Si durante la instalación no has configurado ADMIN_NETWORK_TARGET ni CLIENT_NETWORK_TARGET en el archivo de configuración del nodo del host Linux, sigue este procedimiento para añadir la interfaz. Para obtener más información sobre el archivo de configuración del nodo, consulta "[Instalar StorageGRID en nodos basados en software](#)".

Realiza este procedimiento en el servidor Linux que aloja el nodo que necesita la nueva asignación de red, no dentro del nodo. Este procedimiento solo añade la interfaz al nodo; ocurre un error de validación si intentas especificar cualquier otro parámetro de red.

Para proporcionar la información de direccionamiento, debes usar la herramienta Change IP. Consulta ["Modificar la configuración de red del nodo"](#).

Pasos

1. Inicia sesión en el servidor Linux que aloja el nodo.
2. Edita el archivo de configuración del nodo: `/etc/storagegrid/nodes/node-name.conf`.



No especifiques ningún otro parámetro de red o se producirá un error de validación.

- a. Agrega una entrada para el nuevo destino de red. Por ejemplo:

```
CLIENT_NETWORK_TARGET = bond0.3206
```

- b. Opcional: Añade una entrada para la dirección MAC. Por ejemplo:

```
CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
```

3. Ejecuta el comando «node validate»:

```
sudo storagegrid node validate node-name
```

4. Soluciona todos los errores de validación.

5. Ejecuta el comando «node reload»:

```
sudo storagegrid node reload node-name
```

Agrega interfaces trunk o de acceso a un nodo Linux en StorageGRID

Puedes añadir interfaces trunk o de acceso adicionales a un nodo Linux después de que se haya instalado. Las interfaces que añadas se muestran en la página de interfaces VLAN y en la página de grupos HA.

Antes de empezar

- Tienes acceso a la ["Instrucciones para instalar StorageGRID"](#) en tu plataforma Linux.
- Tienes el archivo `Passwords.txt`.
- Tienes ["permisos de acceso específicos"](#).



No intentes añadir interfaces a un nodo mientras una actualización de software, un procedimiento de recuperación o un procedimiento de ampliación esté activo.

Acerca de esta tarea

Sigue estos pasos para añadir una o más interfaces adicionales a un nodo Linux una vez que se haya instalado el nodo. Por ejemplo, podrías querer añadir una interfaz troncal a un Admin Node o Gateway Node, para poder usar interfaces VLAN y segregar el tráfico que pertenece a diferentes aplicaciones o tenants. O podrías querer añadir una interfaz de acceso para usarla en un grupo de alta disponibilidad (HA).

Si añades una interfaz troncal, debes configurar una interfaz de VLAN en StorageGRID. Si añades una interfaz de acceso, puedes añadir la interfaz directamente a un grupo de HA; no necesitas configurar una interfaz de VLAN.

El nodo queda indisponible durante un breve periodo de tiempo al añadir interfaces. Deberías realizar este procedimiento en un solo nodo a la vez.

Pasos

1. Inicia sesión en el servidor Linux que aloja el nodo.
2. Utilizando un editor de texto como vim o pico, edita el archivo de configuración del nodo:

```
/etc/storagegrid/nodes/node-name.conf
```

3. Añade una entrada al archivo para especificar el nombre y, opcionalmente, la descripción de cada interfaz adicional que desees añadir al nodo. Utiliza este formato.

```
INTERFACE_TARGET_nnnn=value
```

Para *nnnn*, especifica un número único para cada entrada INTERFACE_TARGET que agregues.

Para *value*, especifica el nombre de la interfaz física en el host bare-metal. Luego, si quieres, añade una coma y proporciona una descripción de la interfaz, que se muestra en la página de interfaces VLAN y en la página de grupos HA.

Por ejemplo:

```
INTERFACE_TARGET_0001=ens256, Trunk
```



No especifiques ningún otro parámetro de red o se producirá un error de validación.

4. Ejecuta el siguiente comando para validar tus cambios en el archivo de configuración del nodo:

```
sudo storagegrid node validate node-name
```

Soluciona cualquier error o advertencia antes de pasar al siguiente paso.

5. Ejecuta el siguiente comando para actualizar la configuración del nodo:

```
sudo storagegrid node reload node-name
```

Después de que termines

- Si añadiste una o más interfaces de tronco, ve a ["configurar interfaces VLAN"](#) para configurar una o más interfaces VLAN para cada nueva interfaz principal.
- Si añadiste una o más interfaces de acceso, ve a ["configurar grupos de alta disponibilidad"](#) para agregar las nuevas interfaces directamente a los grupos HA.

Agrega interfaces trunk o de acceso a un nodo VMware en StorageGRID

Puedes añadir una interfaz troncal o de acceso a un nodo de máquina virtual una vez que se haya instalado dicho nodo. Las interfaces que añadas aparecerán en la página «Interfaces de VLAN» y en la página «Grupos de alta disponibilidad».

Antes de empezar

- Tienes acceso a las instrucciones de ["Instalar StorageGRID en tu plataforma VMware"](#).
- Tienes máquinas virtuales de VMware Admin Node y Gateway Node.
- Tienes una subred de red que no se está utilizando como Grid, Admin ni Client Network.
- Tienes el archivo `Passwords.txt`.
- Tienes ["permisos de acceso específicos"](#).



No intentes añadir interfaces a un nodo mientras una actualización de software, un procedimiento de recuperación o un procedimiento de ampliación esté activo.

Acerca de esta tarea

Sigue estos pasos para añadir una o más interfaces adicionales a un nodo de VMware una vez instalado el nodo. Por ejemplo, puede que quieras añadir una interfaz troncal a un Admin Node o Gateway Node, así puedes usar interfaces VLAN para segregar el tráfico de diferentes aplicaciones o tenants. O quizá quieras añadir una interfaz de acceso para usarla en un grupo de alta disponibilidad (HA).

Si añades una interfaz troncal, debes configurar una interfaz de VLAN en StorageGRID. Si añades una interfaz de acceso, puedes añadir la interfaz directamente a un grupo de HA; no necesitas configurar una interfaz de VLAN.

Es posible que el nodo no esté disponible durante un breve tiempo cuando añades interfaces.

Pasos

1. En vCenter, añade un nuevo adaptador de red (tipo VMXNET3) a una VM de Admin Node y a una VM de Gateway Node. Marca las casillas **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. Utiliza SSH para iniciar sesión en el nodo de administración o en el nodo de puerta de enlace.
3. Utiliza `ip link show` para confirmar que se detectó 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 que termines

- Si añadiste una o más interfaces de tronco, ve a ["configurar interfaces VLAN"](#) para configurar una o más interfaces VLAN para cada nueva interfaz principal.
- Si añadiste una o más interfaces de acceso, ve a ["configurar grupos de alta disponibilidad"](#) para agregar las nuevas interfaces directamente a los grupos HA.

Configura servidores DNS en StorageGRID

Puedes añadir, actualizar y eliminar servidores DNS, de modo que puedas utilizar nombres de host con 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, indica la dirección IP de cada servidor DNS que vayas a utilizar. Estas entradas se utilizan para AutoSupport, correos electrónicos de alerta, notificaciones SNMP, puntos finales de servicios de plataforma, Cloud Storage Pools y mucho más.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- Tienes las direcciones IP de los servidores DNS para configurar.

Acerca de esta tarea

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

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

Agrega un servidor DNS

Sigue estos pasos para añadir un servidor DNS.

Pasos

1. Selecciona **Mantenimiento > Red > servidores DNS**.
2. Selecciona **Add another server** para añadir un servidor DNS.
3. Selecciona **Guardar**.

Modificar un servidor DNS

Sigue estos pasos para modificar un servidor DNS.

Pasos

1. Selecciona **Mantenimiento > Red > servidores DNS**.
2. Selecciona la dirección IP del nombre de servidor que quieras editar y realiza los cambios necesarios.
3. Selecciona **Guardar**.

Eliminar un servidor DNS

Sigue estos pasos para eliminar la dirección IP de un servidor DNS.

Pasos

1. Selecciona **Mantenimiento > Red > servidores DNS**.
2. Selecciona el icono de eliminación  junto a la dirección IP.
3. Selecciona **Guardar**.

Modificar la configuración de DNS para un único nodo StorageGRID

En lugar de configurar el DNS de forma global para todo el despliegue, puedes ejecutar un script para configurar el DNS de forma diferente en cada nodo de la grid.

En general, debes utilizar la opción **Mantenimiento > Red > Servidores DNS** del Grid Manager para configurar los servidores DNS. Utiliza el siguiente script únicamente si necesitas usar servidores DNS diferentes para distintos nodos de la red.

Pasos

1. El acceso externo por SSH está bloqueado de forma predeterminada. Si es necesario, ["permitir el acceso de forma temporal"](#).
2. Inicia sesión en el nodo de administración principal:
 - a. Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

- e. Añade la clave privada SSH al agente SSH. Escribe: `ssh-add`
- f. Introduce la contraseña de acceso SSH que figura en el archivo `Passwords.txt`.
3. Inicia sesión en el nodo que quieras actualizar con una configuración DNS personalizada: `ssh node_IP_address`
4. Ejecuta el script de configuración del DNS: `setup_resolv.rb`.

El script muestra la lista de comandos compatibles.

```
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`]
```

5. Añade la dirección IPv4 de un servidor que proporcione el servicio de nombre de dominios para tu red:
`add <nameserver IP_address>`

6. Repite el comando `add nameserver` para añadir servidores de nombres.
7. Sigue las instrucciones que aparezcan para otros comandos.
8. Guarda los cambios y cierra la aplicación: `save`
9. Cerrar el shell de comandos del servidor: `exit`
10. Para cada nodo de la red, repite los pasos desde [iniciar sesión en el nodo](#) hasta [cerrar la línea de comandos](#).
11. Cuando ya no necesites el acceso sin contraseña a otros servidores, elimina la clave privada del agente SSH. Escribe: `ssh-add -D`
12. Si has habilitado el acceso SSH externo, ["bloquear el acceso"](#) cuando termines de modificar la configuración del DNS.

Administra los servidores NTP en StorageGRID

Puedes añadir, actualizar o eliminar servidores NTP para garantizar que los datos se sincronicen con precisión entre los nodos de la red en tu sistema StorageGRID.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- Tienes la frase de contraseña de aprovisionamiento.
- Tienes las direcciones IPv4 de los servidores NTP para configurar.

Cómo utiliza StorageGRID el NTP

El sistema StorageGRID utiliza el Protocolo de Tiempo de Red (NTP) para sincronizar la hora entre todos los nodos de la grid.

En cada sitio, al menos dos nodos del sistema StorageGRID se asignan con la función principal de NTP. 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 cliente NTP y se sincroniza con estos nodos NTP principales.

Los servidores NTP externos se conectan a los nodos a los que previamente les asignaste funciones NTP primarias. Por esta razón, se recomienda especificar al menos dos nodos con funciones NTP primarias.

Directrices para el servidor NTP

Sigue estas pautas para evitar problemas de sincronización:

- Los servidores NTP externos se conectan a los nodos a los que previamente les asignaste funciones NTP primarias. Por esta razón, se recomienda especificar al menos dos nodos con funciones NTP primarias.
- Asegúrate de que al menos dos nodos de cada emplazamiento puedan acceder a al menos cuatro fuentes NTP externas. Si solo un nodo de un emplazamiento puede acceder a las fuentes NTP, se producirán problemas de sincronización si ese nodo deja de funcionar. Además, designar dos nodos por emplazamiento como fuentes NTP primarias garantiza una sincronización precisa si un emplazamiento queda aislado del resto de la grid.
- Los servidores NTP externos especificados deben utilizar el protocolo NTP. Debes especificar referencias a servidores NTP de nivel Stratum 3 o superior para evitar problemas de desviación horaria.



Al especificar la fuente NTP externa para una instalación de StorageGRID en entorno de producción, no utilices el servicio Windows Time (W32Time) en versiones de Windows anteriores a Windows Server 2016. El servicio de hora en versiones anteriores de Windows no es lo suficientemente preciso y no está soportado por Microsoft para su uso en entornos de alta precisión, incluido StorageGRID. Para más detalles, consulta "[Límite de soporte para configurar el servicio de hora de Windows en entornos de alta precisión](#)".

Configurar servidores NTP

Sigue estos pasos para añadir, actualizar o eliminar servidores NTP.

Pasos

1. Selecciona **Mantenimiento > Red > servidores NTP**.
2. En la sección «Servidores», añade, actualiza o elimina entradas de servidor NTP, según sea necesario.

Debes incluir al menos cuatro servidores NTP, y puedes especificar hasta seis servidores.

3. Introduce la frase de contraseña de aprovisionamiento de tu sistema StorageGRID y, a continuación, selecciona **Guardar**.

La página está desactivada hasta que se completen las actualizaciones de configuración.



Si todos tus servidores NTP fallan en la prueba de conexión después de guardar los nuevos servidores NTP, no continúes. Ponte en contacto con soporte técnico.

Soluciona problemas con el servidor NTP

Si tienes problemas con la estabilidad o la disponibilidad de los servidores NTP especificados inicialmente durante la instalación, puedes actualizar la lista de fuentes NTP externas que utiliza el sistema StorageGRID añadiendo servidores adicionales o actualizando o eliminando servidores existentes.

Restaura la conectividad de red para nodos StorageGRID aislados

En determinadas circunstancias, uno o varios grupos de nodos podrían no poder contactar con el resto de la grid. Por ejemplo, los cambios en la dirección IP a nivel de sitio o de toda la grid pueden provocar nodos aislados.

Acerca de esta tarea

El aislamiento de un nodo se indica mediante:

- Alertas, como **No se puede establecer comunicación con el nodo (Alertas > Actuales)**
- Diagnósticos relacionados con la conectividad (**Soporte > Herramientas > Diagnósticos**)

Entre las consecuencias de tener nodos aislados se encuentran las siguientes:

- Si hay varios nodos aislados, es posible que no puedas iniciar sesión ni acceder al Grid Manager.
- Si hay varios nodos aislados, es posible que los valores de uso de almacenamiento y de cuota que se muestran en el panel de control de Tenant Manager no estén actualizados. Los totales se actualizarán cuando se restablezca la conectividad de red.

Para resolver el problema de aislamiento, ejecutas una utilidad de línea de comandos en cada nodo aislado o en un nodo de un grupo (todos los nodos de una subred que no contiene el nodo de administración principal) que está aislado del grid. La utilidad proporciona a los nodos la dirección IP de un nodo no aislado en el grid, lo que permite que el nodo o grupo de nodos aislados vuelva a contactar con todo el grid.



Si el sistema de nombres de dominio multicast (mDNS) está desactivado en las redes, es posible que tengas que ejecutar la utilidad de línea de comandos en cada nodo aislado.

Pasos

Este procedimiento no se aplica cuando solo algunos servicios están fuera de línea o presentan errores de comunicación.

1. Accede al nodo y consulta `/var/local/log/dynip.log` para ver los 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 estás utilizando la consola de VMware, aparecerá un mensaje indicando que el nodo podría estar aislado.

En las implementaciones de Linux, los mensajes de aislamiento aparecerían en archivos `/var/log/storagegrid/node/<nodename>.log`.

2. Si los mensajes de aislamiento son recurrentes y persistentes, ejecuta el siguiente comando:

```
add_node_ip.py <address>
```

donde `<address>` es la dirección IP de un nodo remoto 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. Comprueba lo siguiente para cada nodo que se haya aislado previamente:

- Los servicios del nodo se han iniciado.
- El estado del servicio de IP dinámica es "En ejecución" después de que ejecutes el comando `storagegrid-status`.
- En la página Nodos, el nodo ya no aparece desconectado del resto de la grid.



Si ejecutar el comando `add_node_ip.py` no soluciona el problema, puede que haya otros problemas de red que debas resolver.

Procedimientos de host y middleware

Migra un nodo StorageGRID a un nuevo host Linux

Puedes migrar uno o varios nodos de StorageGRID desde un host Linux (el *host de origen*) a otro host Linux (el *host de destino*) para realizar tareas de mantenimiento del host sin afectar la funcionalidad ni la disponibilidad de tu grid.

Por ejemplo, es posible que quieras migrar un nodo para aplicar parches al sistema operativo y reiniciarlo.

Antes de empezar

- Planeaste tu implementación de StorageGRID para incluir compatibilidad con la migración. Consulta ["Requisitos para la migración de contenedores de nodo"](#).
- El servidor de destino ya está preparado para usarlo con StorageGRID.
- El almacenamiento compartido se utiliza para todos los volúmenes de almacenamiento por nodo
- Las interfaces de red tienen nombres uniformes en todos los hosts.



En una implementación de producción, no ejecutes más de un nodo de almacenamiento en un solo host. Usar un host dedicado para cada nodo de almacenamiento proporciona un dominio de fallo aislado.

Se pueden implementar otros tipos de nodos, como Admin Nodes o Gateway Nodes, en el mismo host. Sin embargo, si tienes varios nodos del mismo tipo (dos Gateway Nodes, por ejemplo), no instales todas las instancias en el mismo host.

Exportar nodo desde el host de origen

Como primer paso, apaga el nodo de grid y expórtalo desde el host Linux de origen.

Ejecuta los siguientes comandos en el *host de origen*.

Pasos

1. Obtén el estado de todos los nodos que se están ejecutando 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. Identifica el nombre del nodo que deseas migrar y deténlo si su estado de ejecución es "Running".

```
sudo storagegrid node stop DC1-S3
```

Ejemplo de salida:

```
Stopping node DC1-S3
Waiting up to 630 seconds for node shutdown
```

3. Exporta 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. Toma nota del comando `import` sugerido en la salida.

Ejecutarás este comando en el servidor de destino en el siguiente paso.

Importar nodo en el host de destino

Después de exportar el nodo desde el host de origen, importas y validas el nodo en el host de destino. La validación confirma que el nodo tiene acceso a los mismos dispositivos de almacenamiento en bloque y de interfaz de red que tenía en el host de origen.

Ejecuta los siguientes comandos en el *host de destino*.

Pasos

1. Importa 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. Comprueba 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, corrígelo antes de iniciar el nodo migrado.

Para obtener información sobre la resolución de problemas, consulta la StorageGRID ["instrucciones de instalación"](#) para tu sistema operativo Linux.

Iniciar el nodo migrado

Después de validar el nodo migrado, inicias el nodo ejecutando un comando en el *host de destino*.

Pasos

1. Inicia el nodo en el nuevo host.

```
sudo storagegrid node start DC1-S3
```

2. Inicia sesión en Grid Manager y comprueba que el estado del nodo sea verde y que no haya ninguna alerta.



Comprobar que el estado del nodo sea verde garantiza que el nodo migrado se haya reiniciado por completo y se haya reincorporado a la grid. Si el estado no es verde, no migres ningún nodo adicional para que no haya más de un nodo fuera de servicio.

3. Si no puedes acceder al Grid Manager, espera 10 minutos y luego ejecuta el siguiente comando:

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

Confirma que el nodo migrado tenga un Run-State de Running.

Configura una máquina virtual VMware para reinicio automático en StorageGRID

Si la máquina virtual no se reinicia tras reiniciar VMware vSphere Hypervisor, es posible que tengas que configurar la máquina virtual para que se reinicie automáticamente.

Debes llevar a cabo este procedimiento si notas que una máquina virtual no se reinicia mientras recuperas un nodo de grid o realizas otro procedimiento de mantenimiento.

Pasos

1. En el árbol del cliente de VMware vSphere, selecciona la máquina virtual que no está iniciada.
2. Haz clic con el botón derecho del ratón sobre la máquina virtual y selecciona **Power on**.
3. Configura VMware vSphere Hypervisor para que la máquina virtual se reinicie automáticamente en el futuro.

Recuperar o sustituir nodos

Advertencias y consideraciones para la recuperación de nodos de StorageGRID

Si un nodo de la red falla, debes recuperarlo lo antes posible. Debes revisar todas las advertencias y consideraciones relativas a la recuperación de nodos antes de comenzar.



StorageGRID es un sistema distribuido compuesto por varios nodos que trabajan entre sí. No uses instantáneas de disco para restaurar nodos de la grid. En su lugar, consulta los procedimientos de recuperación y mantenimiento para cada tipo de nodo.



Si se ha producido un fallo en todo un sitio de StorageGRID, ponte en contacto con el soporte técnico. El soporte técnico colaborará contigo para desarrollar y ejecutar un plan de recuperación del sitio que maximice la cantidad de datos recuperados y se ajuste a tus objetivos empresariales. Consulta ["Cómo el soporte técnico recupera un sitio"](#).

Algunas de las razones para recuperar lo antes posible un nodo de grid que ha fallado incluyen las siguientes:

- Un nodo de la red que falle puede reducir la redundancia de los datos del sistema y de los objetos, lo que te expone al riesgo de una pérdida permanente de datos en caso de que falle otro nodo.
- Un nodo de la red que falle puede afectar la eficiencia de las operaciones diarias.
- Un nodo de grid que falle puede reducir tu capacidad para supervisar las operaciones del sistema.
- Un nodo de grid que falle puede provocar un error 500 de servidor interno si hay reglas estrictas de ILM en vigor.
- Si un nodo de la red no se recupera con rapidez, los tiempos de recuperación podrían aumentar. Por ejemplo, podrían formarse colas que habría que eliminar antes de que se complete la recuperación.

Sigue siempre el procedimiento de recuperación correspondiente al tipo específico de nodo de grid que estés recuperando. Los procedimientos de recuperación varían según se trate de nodos de administración primarios o no primarios, nodos de gateway, nodos de appliance y nodos de almacenamiento.

Condiciones previas para la recuperación de los nodos de la red

A la hora de recuperar nodos de la red, se asumen todas las condiciones siguientes:

- El hardware físico o virtual que presentaba un fallo ha sido reemplazado y configurado.
- La versión del instalador de StorageGRID Appliance del dispositivo de sustitución coincide con la versión de software de tu sistema StorageGRID, como se describe en ["Verifica y actualiza la versión de StorageGRID Appliance Installer"](#).
- Si estás recuperando un nodo de la red que no es el nodo de administración principal, hay conectividad entre el nodo de la red que se está recuperando y el nodo de administración que gestiona el procedimiento de recuperación.
- Si vas a recuperar un nodo de almacenamiento de un dispositivo Storage Node, debes especificar el mismo tipo de almacenamiento que el del dispositivo original (combinado, solo metadatos o solo datos) durante la instalación del dispositivo. Si especificas un tipo de almacenamiento diferente, la recuperación fallará y será necesario reinstalar el dispositivo especificando el tipo de almacenamiento correcto.

Orden de recuperación de nodos si falla un servidor que aloja más de un nodo de la red

Si falla un servidor que aloja más de un nodo de la red, puedes recuperar los nodos en cualquier orden. Sin embargo, si el servidor que ha fallado aloja el nodo de administración principal, debes recuperar ese nodo en primer lugar.

Direcciones IP de los nodos recuperados

No intentes recuperar un nodo utilizando una dirección IP que esté asignada actualmente a cualquier otro nodo. Cuando implementes el nuevo nodo, utiliza la dirección IP actual del nodo que ha fallado o una dirección IP sin usar.

Si utilizas una nueva dirección IP para implementar el nuevo nodo y luego recuperas el nodo, la nueva dirección IP seguirá utilizándose para el nodo recuperado. Si quieres volver a la dirección IP original, usa la herramienta Cambiar IP después de que termine la recuperación.

Reúne los materiales necesarios para la recuperación de nodos de grid de StorageGRID

Antes de llevar a cabo los procedimientos de mantenimiento, debes asegurarte de que dispones de los materiales necesarios para recuperar un nodo de la red que haya fallado.

Artículo	Notas
Archivo de instalación de StorageGRID	Si necesitas recuperar un nodo de la red, debes Descargar los archivos de instalación de StorageGRID para tu plataforma. Nota: No necesitas descargar archivos si estás recuperando volúmenes de almacenamiento con fallos en un Storage Node.
Portátil de servicio	El ordenador portátil de servicio debe tener lo siguiente: • Puerto de red • Cliente SSH (por ejemplo, PuTTY) • "Navegador web compatible"

Artículo	Notas
Archivo del paquete de recuperación .zip	Consigue una copia del archivo del paquete de recuperación más reciente .zip: <code>sgws-recovery-package-id-revision.zip</code> El contenido del archivo .zip se actualiza cada vez que se modifica el sistema. Debes guardar la versión más reciente del paquete de recuperación en un lugar seguro después de hacer esos cambios. Usa la copia más reciente para recuperarte de fallos en el grid. Una vez que hayas iniciado sesión en cualquier nodo de administración, utiliza el Grid Manager para descargar un paquete de recuperación. Selecciona Mantenimiento > Sistema > Paquete de recuperación. Si no puedes acceder al Grid Manager, puedes encontrar copias cifradas del paquete de recuperación en algunos nodos de almacenamiento que contienen el servicio ADC. En cada nodo de almacenamiento, revisa esta ubicación para el paquete de recuperación: <code>/var/local/install/sgws-recovery-package-grid-id-revision.zip.gpg</code> Usa el paquete de recuperación con el número de revisión más alto.
Passwords.txt archivo	Contiene las contraseñas necesarias para acceder a los nodos de grid desde la línea de comandos. Incluido en el paquete de recuperación.
Contraseña de aprovisionamiento	La frase de contraseña se crea y se documenta al instalar el sistema StorageGRID por primera vez. La frase de contraseña de aprovisionamiento no está en el archivo Passwords.txt.
Documentación actual para tu plataforma	Visita la página web del proveedor de la plataforma para consultar la documentación. Para conocer las versiones actuales compatibles con tu plataforma, consulta "Herramienta NetApp Interoperability Matrix Tool".

Descargar y descomprimir los archivos de instalación de StorageGRID

[[descargar y extraer los archivos de instalación de recuperación]]

Descarga el software y descomprime los archivos, a menos que seas "[Recuperar volúmenes de almacenamiento con fallo en un nodo de almacenamiento](#)".

Debes utilizar la versión de StorageGRID que se está ejecutando actualmente en la grid.

Pasos

1. Averigua qué versión del software tienes instalada actualmente. En la parte superior de Grid Manager, selecciona el icono de ayuda y selecciona **Acerca de**.
2. Ve a "[NetApp Página de descargas de StorageGRID](#)".
3. Selecciona la versión de StorageGRID que se está ejecutando actualmente en el grid.

Las versiones del software StorageGRID tienen este formato: 11.x.y.

4. Inicia sesión con el nombre de usuario y la contraseña de tu cuenta de NetApp.
5. Lee el Acuerdo de licencia de usuario final, marca la casilla de verificación y luego selecciona **Aceptar y continuar**.
6. En la columna **Instalar StorageGRID** de la página de descargas, selecciona el archivo .tgz o .zip correspondiente a tu plataforma.

La versión que figura en el archivo de instalación debe coincidir con la versión del software que está instalada actualmente.

Usa el archivo .zip si estás usando Windows.

Plataforma	Archivo de instalación
RHEL	StorageGRID-Webscale-version-RPM-uniqueID.zip StorageGRID-Webscale-version-RPM-uniqueID.tgz
Ubuntu o Debian o dispositivos preconfigurados	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. Descarga y descomprime el archivo comprimido.
8. Ve directamente a la sección correspondiente a tu plataforma para seleccionar los archivos que necesites, en función de tu plataforma y de los nodos de grid que debas recuperar.

Las rutas que figuran en el paso correspondiente a cada plataforma son relativas al directorio de nivel superior instalado por el archivo comprimido.

9. Si estás recuperando un "nodo basado en software", selecciona los archivos correspondientes:

RHEL

Ruta y nombre del archivo	Descripción
	Un archivo de texto que describe todos los archivos que contiene el archivo de descarga de StorageGRID.
	Una licencia gratuita que no da derecho a ningún tipo de asistencia técnica para el producto.
	Paquete RPM para instalar las imágenes de los nodos de StorageGRID en tus hosts RHEL.
	Paquete RPM para instalar el servicio de host de StorageGRID en tus hosts RHEL.
Herramienta de creación de scripts de implementación	Descripción
	Un script de Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Un script en Python que se utiliza para automatizar la configuración de los appliances StorageGRID.
	Un archivo de configuración de ejemplo para usar con el script <code>configure-storagegrid.py</code> .
	Un script de Python de ejemplo que puedes usar para iniciar sesión en la Grid Management API cuando el inicio de sesión único está habilitado. También puedes usar este script para la integración con Ping Federate.
	Un archivo de configuración en blanco para usar con el script <code>configure-storagegrid.py</code> .
	Ejemplo de rol y playbook de Ansible para configurar hosts de RHEL para el despliegue de contenedores de StorageGRID. Puedes personalizar el rol o el playbook según sea necesario.

Ruta y nombre del archivo	Descripción
	Un script de ejemplo en Python que puedes utilizar para iniciar sesión en la API de gestión de la red cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script auxiliar llamado por el script de Python compañero <code>storagegrid-ssoauth-azure.py</code> para realizar interacciones de inicio de sesión único con Azure.
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puedes utilizar estos esquemas para confirmar que cualquier código que hayas escrito para utilizar las API de gestión de StorageGRID será compatible con la nueva versión de StorageGRID si no tienes un entorno de StorageGRID que no sea de producción para pruebas de compatibilidad con la actualización.

Ubuntu o Debian

Ruta y nombre del archivo	Descripción
	Un archivo de texto que describe todos los archivos que contiene el archivo de descarga de StorageGRID.
	Un archivo de licencia de NetApp que no es de producción y que puedes utilizar para pruebas e implementaciones de prueba de concepto.
	Paquete DEB para instalar las imágenes de los nodos de StorageGRID en hosts Ubuntu o Debian.
	Suma de comprobación MD5 del archivo <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .
	Paquete DEB para instalar el servicio de host de StorageGRID en hosts con Ubuntu o Debian.
Herramienta de creación de scripts de implementación	Descripción

Ruta y nombre del archivo	Descripción
	Un script de Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Un script en Python que se utiliza para automatizar la configuración de los appliances StorageGRID.
	Un script de Python de ejemplo que puedes usar para iniciar sesión en la Grid Management API cuando el inicio de sesión único está habilitado. También puedes usar este script para la integración con Ping Federate.
	Un archivo de configuración de ejemplo para usar con el script <code>configure-storagegrid.py</code> .
	Un archivo de configuración en blanco para usar con el script <code>configure-storagegrid.py</code> .
	Ejemplo de rol y playbook de Ansible para configurar hosts de Ubuntu o Debian para el despliegue de contenedores de StorageGRID. Puedes personalizar el rol o el playbook según sea necesario.
	Un script de ejemplo en Python que puedes utilizar para iniciar sesión en la API de gestión de la red cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script auxiliar llamado por el script de Python compañero <code>storagegrid-ssoauth-azure.py</code> para realizar interacciones de inicio de sesión único con Azure.
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puedes utilizar estos esquemas para confirmar que cualquier código que hayas escrito para utilizar las API de gestión de StorageGRID será compatible con la nueva versión de StorageGRID si no tienes un entorno de StorageGRID que no sea de producción para pruebas de compatibilidad con la actualización.

VMware

Ruta y nombre del archivo	Descripción
	Un archivo de texto que describe todos los archivos que contiene el archivo de descarga de StorageGRID.
	Una licencia gratuita que no da derecho a ningún tipo de asistencia técnica para el producto.
	El archivo de disco de la máquina virtual que se utiliza como plantilla para crear máquinas virtuales de nodos de grid.
	El archivo de plantilla de Open Virtualization Format (.ovf) y el archivo de manifiesto (.mf) para implementar el nodo de administración primario.
	El archivo de plantilla (.ovf) y el archivo de manifiesto (.mf) para implementar nodos de administración no principales.
	El archivo de plantilla (.ovf) y el archivo de manifiesto (.mf) para implementar Gateway Nodes.
	El archivo de plantilla (.ovf) y el archivo de manifiesto (.mf) para desplegar nodos de almacenamiento basados en máquinas virtuales.
Herramienta de creación de scripts de implementación	Descripción
	Un script de Bash que se usa para automatizar el despliegue de nodos de grid virtuales.
	Un archivo de configuración de ejemplo para usarlo con el script <code>deploy-vsphere-ovftool.sh</code> .
	Un script de Python que se utiliza para automatizar la configuración de un sistema StorageGRID.
	Un script en Python que se utiliza para automatizar la configuración de los appliances StorageGRID.

Ruta y nombre del archivo	Descripción
	Un script de ejemplo en Python que puedes utilizar para iniciar sesión en la API de gestión de la red cuando está habilitado el inicio de sesión único (SSO). También puedes utilizar este script para la integración con Ping Federate.
	Un archivo de configuración de ejemplo para usar con el script <code>configure-storagegrid.py</code> .
	Un archivo de configuración en blanco para usar con el script <code>configure-storagegrid.py</code> .
	Un script de ejemplo en Python que puedes utilizar para iniciar sesión en la API de gestión de la red cuando el inicio de sesión único (SSO) está habilitado mediante Active Directory o Ping Federate.
	Un script auxiliar llamado por el script de Python compañero <code>storagegrid-ssoauth-azure.py</code> para realizar interacciones de inicio de sesión único con Azure.
	Esquemas de API para StorageGRID. Nota: Antes de realizar una actualización, puedes utilizar estos esquemas para confirmar que cualquier código que hayas escrito para utilizar las API de gestión de StorageGRID será compatible con la nueva versión de StorageGRID si no tienes un entorno de StorageGRID que no sea de producción para pruebas de compatibilidad con la actualización.

10. Si vas a restaurar un sistema basado en un dispositivo StorageGRID, selecciona los archivos correspondientes.



Para la instalación del dispositivo, estos archivos solo son necesarios si necesitas evitar el tráfico de red. El dispositivo puede descargar los archivos necesarios desde el nodo de administración donde realizas el procedimiento de recuperación.

Ruta y nombre del archivo	Descripción
	Paquete DEB para instalar las imágenes de los nodos de StorageGRID en tus dispositivos.

Ruta y nombre del archivo	Descripción
	Suma de comprobación MD5 para el archivo /debs/storagegridwebscale- images-version-SHA.deb.

Selecciona el procedimiento de recuperación del nodo StorageGRID

Debes seleccionar el procedimiento de recuperación adecuado para el tipo de nodo que ha fallado.

Nodo de grid	Procedimiento de recuperación
Más de un nodo de almacenamiento	Contacta al soporte técnico. Si han fallado más de un nodo de almacenamiento, el soporte técnico debe ayudarte con la recuperación para evitar inconsistencias en la base de datos que podrían provocar la pérdida de datos. Puede que se requiera un procedimiento de recuperación del sitio. "Cómo el soporte técnico recupera un sitio"
Un único nodo de almacenamiento	El procedimiento de recuperación del nodo de almacenamiento depende del tipo y la duración de la falla. "Recupérate de fallos en los nodos de almacenamiento"
Nodo de administración	El procedimiento para el nodo de administración depende de si necesitas recuperar el nodo de administración principal o un nodo de administración no principal. "Recupérate de fallos del nodo de administración"
Nodo de puerta de enlace	"Recupera ante fallos del nodo de puerta de enlace"
Nodo de archivo	"Recupera tras fallos en los nodos de archivo (sitio de documentación de StorageGRID 11.8)"



Si falla un servidor que aloja más de un nodo de la red, puedes recuperar los nodos en cualquier orden. Sin embargo, si el servidor que ha fallado aloja el nodo de administración principal, debes recuperar ese nodo primero. Recuperar primero el nodo de administración principal evita que las recuperaciones de otros nodos se detengan mientras esperan a contactar con el nodo de administración principal.

Recupérate de fallos en los nodos de almacenamiento

Recupera de fallos en el nodo de almacenamiento StorageGRID

El procedimiento para recuperar un nodo de almacenamiento que ha fallado depende del tipo de fallo y del tipo de nodo de almacenamiento que ha fallado.

Utiliza esta tabla para seleccionar el procedimiento de recuperación para un nodo de almacenamiento fallido.

Problema	Acción	Notas
Han fallado más de un nodo de almacenamiento.	Ponte en contacto con el soporte técnico.	La recuperación de más de un nodo de almacenamiento podría afectar la integridad de la base de datos de Cassandra, lo que puede causar la pérdida de datos. El soporte técnico puede determinar cuándo es seguro iniciar la recuperación de un segundo nodo de almacenamiento. Nota: Si en un sitio fallan varios nodos de almacenamiento que contienen el servicio ADC, pierdes cualquier solicitud de servicio de plataforma pendiente para ese sitio.
Han fallado más de un nodo de almacenamiento en una sede o ha fallado toda la sede.	Contacta al soporte técnico. Puede que sea necesario realizar un procedimiento de recuperación del sitio.	El soporte técnico evaluará tu situación y elaborará un plan de recuperación. Consulta "Cómo el soporte técnico recupera un sitio" .
Ha fallado un nodo de almacenamiento de appliance.	"Recuperar el nodo de almacenamiento del appliance"	El procedimiento de recuperación para los nodos de almacenamiento de appliance es el mismo para todos los fallos.
Uno o más volúmenes de almacenamiento han fallado, pero la unidad del sistema está intacta	"Recupérate de un fallo del volumen de almacenamiento cuando la unidad del sistema está intacta"	Este procedimiento se utiliza para los nodos de almacenamiento basados en software.
La unidad del sistema ha fallado.	"Recupera tu sistema tras un fallo de unidad"	El procedimiento de sustitución del nodo depende de la plataforma de implementación y de si también se ha producido algún fallo en los volúmenes de almacenamiento.



Algunos procedimientos de recuperación de StorageGRID utilizan Reaper para gestionar las reparaciones de Cassandra. Las reparaciones se llevan a cabo automáticamente en cuanto se han iniciado los servicios relacionados o necesarios. Es posible que veas en la salida del script menciones a "reaper" o "reparación de Cassandra". Si aparece un mensaje de error que indica que la reparación ha fallado, ejecuta el comando que se indica en dicho mensaje.

Recuperar el nodo de almacenamiento del appliance

Advertencias para recuperar los Storage Nodes del dispositivo StorageGRID

El procedimiento para recuperar un nodo de almacenamiento de un dispositivo StorageGRID que ha fallado es el mismo, tanto si se trata de una recuperación tras la pérdida de la unidad del sistema como si se trata únicamente de la pérdida de volúmenes de almacenamiento.



Si se ha producido un fallo en más de un nodo de almacenamiento (o está desconectado), ponte en contacto con soporte técnico. No realices el siguiente procedimiento de recuperación. Podría producirse una pérdida de datos. Para obtener más información, consulta ["Cómo el soporte técnico recupera un sitio"](#).



Si las reglas de ILM están configuradas para almacenar únicamente una copia replicada y dicha copia se encuentra en un volumen de almacenamiento que ha fallado, no podrás recuperar el objeto.



Para los procedimientos de mantenimiento del hardware, como las instrucciones para reemplazar un controlador o reinstalar SANtricity OS, consulta la ["Instrucciones de mantenimiento para tu dispositivo de almacenamiento"](#).

Prepara el nodo de almacenamiento del dispositivo StorageGRID para la reinstalación

Al recuperar un nodo de almacenamiento (Storage Node), primero debes preparar el dispositivo para la reinstalación del software StorageGRID.

Pasos

1. Inicia sesión en el nodo de almacenamiento que ha fallado:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Prepara el nodo de almacenamiento del dispositivo para la instalación del software StorageGRID.
`sgareinstall`
3. Cuando se te pida que continúes, introduce: `y`

El dispositivo se reinicia y tu sesión SSH finaliza. Normalmente, el instalador de StorageGRID Appliance

tarda unos 5 minutos en estar disponible, aunque en algunos casos puede que tengas que esperar hasta 30 minutos.



No intentes acelerar el reinicio apagando y volviendo a encender el dispositivo ni reiniciándolo de ninguna otra forma. Podrías interrumpir actualizaciones automáticas de la BIOS, el BMC u otro firmware.

El nodo de almacenamiento del dispositivo StorageGRID se ha reiniciado y ya no se puede acceder a los datos que contiene. Las direcciones IP configuradas durante el proceso de instalación original deberían permanecer intactas; no obstante, se recomienda que lo compruebes una vez finalizado el procedimiento.

Después de ejecutar el comando `sgareinstall`, se eliminan todas las cuentas, contraseñas y claves SSH aprovisionadas por StorageGRID, y se generan nuevas claves de host.

Inicia la instalación del dispositivo StorageGRID

Para instalar StorageGRID en un nodo de almacenamiento de un dispositivo, usas el StorageGRID Appliance Installer, que viene incluido en el dispositivo.

Antes de empezar

- El dispositivo se ha instalado en un rack, se ha conectado a tus redes y se ha encendido.
- Se han configurado las conexiones de red y las direcciones IP del dispositivo mediante el StorageGRID Appliance Installer.
- Conoces la dirección IP del nodo de administración principal de StorageGRID.
- Todas las subredes de la red Grid que aparecen en la página de Configuración de IP del StorageGRID Appliance Installer se han definido en la Grid Network Subnet List del nodo de administración principal.
- Has completado estas tareas previas siguiendo las instrucciones de instalación de tu dispositivo de almacenamiento. Consulta ["Guía de inicio rápido para la instalación del hardware"](#).
- Estás usando un ["navegador web compatible"](#).
- Conoces una de las direcciones IP asignadas al controlador de cálculo del dispositivo. Puedes usar la dirección IP para la red de administración (puerto de gestión 1 en el controlador), la red de Grid o la red de clientes.

Acercas de esta tarea

Para instalar StorageGRID en un nodo de almacenamiento de un appliance:

- Debes especificar o confirmar la dirección IP del nodo de administración principal y el nombre de host (nombre del sistema) del nodo.
- Inicia la instalación y espera a que se configuren los volúmenes y se instale el software.



Al recuperar un nodo de almacenamiento de un dispositivo Storage Node, reinstálalo con el mismo tipo de almacenamiento que el dispositivo original (combinado, solo metadatos o solo datos). Si especificas un tipo de almacenamiento diferente, la recuperación fallará y será necesario reinstalar el dispositivo especificando el tipo de almacenamiento correcto.

- A mitad del proceso, la instalación se detiene. Para reanudar la instalación, debes iniciar sesión en Grid Manager y configurar el nodo de almacenamiento pendiente como reemplazo del nodo que falló.
- Después de que hayas configurado el nodo, el proceso de instalación del dispositivo se completa y el dispositivo se reinicia.

Pasos

1. Abre un navegador e introduce una de las direcciones IP del controlador de cómputo en el appliance.

`https://Controller_IP:8443`

Aparece la página de inicio del instalador de StorageGRID Appliance.

2. En la sección «Conexión al nodo de administración principal», determina si necesitas especificar la dirección IP del nodo de administración principal.

El instalador de StorageGRID Appliance puede detectar esta dirección IP automáticamente, siempre que el nodo de administración principal, o al menos otro nodo de grid con ADMIN_IP configurado, esté presente en la misma subred.

3. Si esta dirección IP no aparece o necesitas cambiarla, indica la dirección:

Opción	Pasos
Introducción manual de la dirección IP	a. Desmarca la casilla Habilitar detección de nodos de administración. b. Introduce manualmente la dirección IP. Nota: Para la instalación, introduce manualmente la dirección IP del nodo de administración que deseas usar para instalar el nodo. Para la recuperación, usa la dirección IP del nodo de administración principal si está disponible; de lo contrario, usa la dirección IP de un nodo de administración que no sea el principal. a. Selecciona Guardar. b. Espera mientras el estado de conexión de la nueva dirección IP se vuelve "listo".
Detección automática de todos los nodos de administración principales conectados	a. Marca la casilla Habilitar detección de nodos de administración. b. En la lista de direcciones IP detectadas, selecciona el nodo de administración para la grid donde se va a implementar este nodo de almacenamiento de appliance. Nota: Para la recuperación, utiliza la dirección IP del nodo de administración principal si está disponible; de lo contrario, utiliza la dirección IP de un nodo de administración que no sea el principal. a. Selecciona Guardar. b. Espera mientras el estado de conexión de la nueva dirección IP se vuelve "listo".

4. En el campo **Nombre de nodo**, introduce el mismo nombre de host (nombre del sistema) que se utilizó para el nodo que estás recuperando y haz clic en **Guardar**.
5. En la sección «Instalación», comprueba que el estado actual sea «Listo para iniciar la instalación de *node name* en la grid con el Primary Admin Node *admin_ip*» y que el botón **Iniciar instalación** esté habilitado.

Si el botón **Iniciar instalación** no está habilitado, es posible que debas cambiar la configuración de red o los ajustes de puerto. Para obtener instrucciones, consulta las instrucciones de mantenimiento de tu dispositivo.

6. En la página de inicio del instalador de StorageGRID Appliance, haz clic en **Iniciar instalación**.

El estado actual cambia a «Instalación en curso» y se muestra la página «Supervisar la instalación».



Si necesitas acceder manualmente a la página «Instalación de Monitor», haz clic en **Instalación de Monitor** en la barra de menús. Consulta ["Supervisar la instalación del appliance"](#).

Supervisar la instalación del dispositivo StorageGRID

El instalador de StorageGRID Appliance muestra el estado hasta que la instalación se completa. Cuando la instalación del software se completa, el appliance se reinicia.

Pasos

1. Para supervisar el progreso de la instalación, haz clic en **Monitor Installation** en la barra de menús.

La página de instalación del monitor muestra el progreso de la instalación.

La barra de estado azul indica qué tarea está actualmente en progreso. Las barras de estado verdes indican las tareas que se han completado correctamente.



El instalador se asegura de que las tareas completadas en una instalación anterior no se vuelvan a ejecutar. Si vuelves a ejecutar una instalación, las tareas que no necesiten volver a ejecutarse se muestran con una barra de estado verde y el estado "Skipped".

2. Revisa el avance de las dos primeras fases de la instalación.

- **1. Configura el almacenamiento**

Durante esta fase, el instalador se conecta al controlador de almacenamiento, borra cualquier configuración existente, se comunica con SANtricity OS para configurar los volúmenes y configura los parámetros del host.

- **2. Instala el sistema operativo**

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

3. Sigue supervisando el progreso de la instalación hasta que la fase **Instalar StorageGRID** se detenga y aparezca un mensaje en la consola integrada en el que se te pida que apruebes este nodo en el Admin Node usando Grid Manager.
4. Vaya a ["Selecciona Iniciar recuperación para configurar el nodo de almacenamiento del appliance Storage Node"](#).

Selecciona Iniciar recuperación para configurar el nodo de almacenamiento del appliance StorageGRID

Debes seleccionar «Iniciar recuperación» en el Grid Manager para configurar un nodo de almacenamiento del appliance como sustituto del nodo que ha fallado.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un "navegador web compatible".
- Tienes el "Permiso de mantenimiento o acceso de usuario raíz".
- Tienes la frase de contraseña de aprovisionamiento.
- Has implementado un nodo de almacenamiento de recovery appliance.
- Dispones de la fecha de inicio de cualquier trabajo de reparación de datos con código de borrado.

Pasos

1. Desde el Grid Manager, selecciona **Maintenance > Tasks > Recovery**.
2. Selecciona el nodo de la grid que deseas recuperar en la lista Nodos pendientes.

Los nodos aparecen en la lista tras sufrir un fallo, pero no puedes seleccionar un nodo hasta que se haya reinstalado y esté listo para la recuperación.

3. Introduce la **frase de contraseña de aprovisionamiento**.
4. Haz 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. Supervisa el progreso de la recuperación en la tabla Recuperando nodo de grid.

Cuando el nodo de la grid llegue a la fase «Esperando pasos manuales», pasa al siguiente tema y realiza los pasos manuales para volver a montar y formatear los volúmenes de almacenamiento del appliance.

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, puedes hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparecerá un cuadro de diálogo en el que se indica que el nodo quedará en un estado indeterminado si restableces 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 deseas volver a intentar la recuperación tras reiniciar el procedimiento, debes restaurar el nodo del dispositivo a su estado de preinstalación ejecutando `sgareinstall` en dicho nodo.

Vuelve a montar y reformatea los volúmenes de almacenamiento del dispositivo StorageGRID (pasos manuales)

Debes ejecutar manualmente dos scripts para volver a montar los volúmenes de almacenamiento conservados y reformatear cualquier volumen de almacenamiento que haya fallado. El primer script vuelve a montar los volúmenes que están correctamente formateados como volúmenes de almacenamiento de StorageGRID. El segundo script reformatea cualquier volumen desmontado, reconstruye la base de datos de Cassandra, si es necesario, e inicia los servicios.

Antes de empezar

- Ya has sustituido el hardware de cualquier volumen de almacenamiento fallido que sabes que requiere reemplazo.

Ejecutar el `sn-remount-volumes` script podría ayudarte a identificar otros volúmenes de almacenamiento que hayan fallado.

- Has comprobado que no se está llevando a cabo el proceso de decomisionar un nodo de almacenamiento, o bien has pausado dicho proceso. (En Grid Manager, selecciona **Mantenimiento > Tareas > Decomisionar**.)
- Has comprobado que no hay ninguna expansión en curso. (En el Grid Manager, selecciona **Mantenimiento > Tareas > Expansión**.)



Ponte en contacto con el soporte técnico si hay más de un nodo de almacenamiento desconectado. No ejecutes el `sn-recovery-postinstall.sh` script.

Acerca de esta tarea

Para completar este procedimiento, debes realizar estas tareas a grandes rasgos:

- Inicia sesión en el nodo de almacenamiento recuperado.
- Ejecuta el `sn-remount-volumes` script para volver a montar los volúmenes de almacenamiento con el formato adecuado. Cuando se ejecuta este script, realiza lo siguiente:
 - Monta y desmonta cada volumen de almacenamiento para reproducir el journal de XFS.
 - Realiza una comprobación de la coherencia de archivos XFS.
 - Si el sistema de archivos es coherente, determina si el volumen de almacenamiento es un volumen de almacenamiento StorageGRID formateado correctamente.
 - Si el volumen de almacenamiento está formateado correctamente, vuelve a montar el volumen de almacenamiento. Los datos existentes en el volumen permanecen intactos.
- Revisa el resultado del script y resuelve cualquier problema.
- Ejecuta el `sn-recovery-postinstall.sh` script. Cuando se ejecuta este script, realiza lo siguiente.



No reinicies un nodo de almacenamiento durante la recuperación antes de ejecutar `sn-recovery-postinstall.sh` (paso 4) para reformatear los volúmenes de almacenamiento defectuosos y restaurar los metadatos de los objetos. Reiniciar el nodo de almacenamiento antes de que `sn-recovery-postinstall.sh` finalice provoca errores en los servicios que intentan iniciarse y hace que los nodos del dispositivo StorageGRID salgan del modo de mantenimiento.

- Reformatea cualquier volumen de almacenamiento que el `sn-remount-volumes` script no haya podido montar o que se haya detectado que está formateado incorrectamente.



Si se vuelve a formatear un volumen de almacenamiento, se perderán todos los datos que contenga. Debes realizar un procedimiento adicional para restaurar los datos de objetos desde otras ubicaciones en el grid, suponiendo que las reglas de ILM se hayan configurado para almacenar más de una copia de cada objeto.

- Reconstruye la base de datos de Cassandra en el nodo, si es necesario.
- Inicia los servicios en el nodo de almacenamiento.

Pasos

1. Inicia sesión en el nodo de almacenamiento recuperado:

- Introduce el siguiente comando: `ssh admin@grid_node_IP`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.
- Introduce el siguiente comando para pasar a ser usuario root: `su -`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Ejecuta el primer script para volver a montar los volúmenes de almacenamiento que estén correctamente formateados.



Si todos los volúmenes de almacenamiento son nuevos y hay que formatearlos, o si todos los volúmenes de almacenamiento han fallado, puedes saltarte este paso y ejecutar el segundo script para volver a formatear todos los volúmenes de almacenamiento desmontados.

a. Ejecuta el script: `sn-remount-volumes`

Es posible que este script tarde horas en ejecutarse en volúmenes de almacenamiento que contengan datos.

b. A medida que se ejecuta el script, revisa la salida y responde a cualquier mensaje.



Si lo necesitas, puedes usar el comando `tail -f` para supervisar el contenido del archivo de registro del script (`/var/local/log/sn-remount-volumes.log`). El archivo de registro contiene información más detallada que 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 resultado, un volumen de almacenamiento se volvió a montar correctamente y tres volúmenes de almacenamiento presentaron errores.

- `/dev/sdb` superó la comprobación de coherencia del sistema de archivos XFS y presentaba una estructura de volumen válida, por lo que se volvió a montar correctamente. Los datos de los dispositivos que el script vuelve a montar se conservan.
- `/dev/sdc` La comprobación de coherencia del sistema de archivos XFS falló porque el volumen de almacenamiento era nuevo o estaba dañado.
- `/dev/sdd` No se ha podido montar porque el disco no estaba inicializado o el superbloque del disco estaba dañado. Cuando el script no puede montar un volumen de almacenamiento, te pregunta si deseas ejecutar la comprobación de coherencia del sistema de archivos.
 - Si el volumen de almacenamiento está conectado a un disco nuevo, responde **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 ya existente, responde **Y** a la pregunta. Puedes 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` superó la comprobación de coherencia del sistema de archivos XFS y tenía una estructura de volumen válida; sin embargo, el ID del nodo LDR en el `volID` archivo no coincidía con el ID de este Storage Node (el `configured LDR noid` que aparece en la parte superior). Este mensaje indica que este volumen pertenece a otro Storage Node.

3. Revisa el resultado del script y resuelve cualquier problema.



Si un volumen de almacenamiento no ha superado la comprobación de coherencia del sistema de archivos XFS o no se ha podido montar, revisa detenidamente los mensajes de error que aparecen en la salida. Debes comprender las implicaciones de ejecutar el `sn-recovery-postinstall.sh` script en estos volúmenes.

- Comprueba que los resultados incluyan una entrada para todos los volúmenes que esperabas. Si falta algún volumen en la lista, vuelve a ejecutar el script.
- Revisa los mensajes de todos los dispositivos montados. Asegúrate de que no haya errores que indiquen que un volumen de almacenamiento no pertenece a este Storage Node.

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 indica que un volumen de almacenamiento pertenece a otro Storage Node, ponte en contacto con soporte técnico. Si ejecutas el `sn-recovery-postinstall.sh` script, el volumen de almacenamiento se reformateará, lo que podría provocar la pérdida de datos.

- Si no se ha podido montar algún dispositivo de almacenamiento, anota el nombre del dispositivo y repáralo o reemplázalo.



Debes reparar o sustituir cualquier dispositivo de almacenamiento que no se haya podido montar.

Utilizarás el nombre del dispositivo para buscar el ID del volumen, que es un dato obligatorio cuando

ejecutes el script `repair-data` para restaurar los datos de objetos en el volumen (el siguiente procedimiento).

- d. Después de reparar o reemplazar todos los dispositivos que no se pueden montar, ejecuta de nuevo el script `sn-remount-volumes` para confirmar que todos los volúmenes de almacenamiento que se pueden volver a montar han sido montados nuevamente.



Si no se puede montar un volumen de almacenamiento o está formateado incorrectamente, y continúas con el siguiente paso, el volumen y cualquier dato en el volumen se eliminarán. Si tenías dos copias de los datos de objetos, solo tendrás una copia hasta que completes el siguiente procedimiento (restaurar los datos de objetos).



No ejecutes el script `sn-recovery-postinstall.sh` si crees que los datos que quedan en un volumen de almacenamiento con fallo no se pueden reconstruir desde otra parte de la grid (por ejemplo, si tu política de ILM usa una regla que solo hace una copia o si los volúmenes han fallado en varios nodos). En su lugar, contacta al soporte técnico para ver cómo recuperar tus datos.

4. Ejecuta el `sn-recovery-postinstall.sh` script: `sn-recovery-postinstall.sh`

Este script reformatea cualquier volumen de almacenamiento que no se haya podido montar o que se haya detectado que está formateado incorrectamente; reconstruye la base de datos de Cassandra en el nodo, si es necesario; e inicia los servicios en el nodo de almacenamiento.

Ten en cuenta lo siguiente:

- Es posible que el script tarde horas en ejecutarse.
- En general, deberías dejar la sesión SSH sin tocar mientras el script está en ejecución.
- No pulses **Ctrl+C** mientras la sesión SSH esté activa.
- El script se ejecutará en segundo plano si se produce una interrupción de la red y se interrumpe la sesión SSH, pero puedes ver el progreso desde la página de recuperación.
- Si el nodo de almacenamiento utiliza el servicio RSM, puede parecer que el script se queda bloqueado durante 5 minutos mientras se reinician los servicios del nodo. Este retraso de 5 minutos es normal 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 gestionar las reparaciones de Cassandra. Las reparaciones se llevan a cabo automáticamente en cuanto se han iniciado los servicios relacionados o necesarios. Es posible que veas en la salida del script menciones a "reaper" o "reparación de Cassandra". Si aparece un mensaje de error que indica que la reparación ha fallado, ejecuta el comando que se indica en dicho mensaje.

5. Mientras se ejecuta el `sn-recovery-postinstall.sh` script, supervisa la página Recovery en el Grid Manager.

La barra de progreso y la columna «Etapa» de la página «Recuperación» ofrecen a grandes rasgos el estado del `sn-recovery-postinstall.sh` script.

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 que el `sn-recovery-postinstall.sh` script haya iniciado los servicios en el nodo, puedes restaurar los datos de objetos en cualquier volumen de almacenamiento que haya formateado el script.

El script te pregunta si deseas utilizar el proceso de restauración de volúmenes de Grid Manager.

- En la mayoría de los casos, debes **"restaura datos de objetos usando Grid Manager"**. Responde `y` para usar Grid Manager.
- En casos excepcionales, como cuando así lo indique el soporte técnico, o cuando sepas que el nodo de sustitución tiene menos volúmenes disponibles para el almacenamiento de objetos que el nodo original, debes **"restaurar los datos del objeto manualmente"** usando el script `repair-data`. Si se da alguno de estos casos, responde `n`.



Si respondes `n` al usar el proceso de restauración de volúmenes de Grid Manager (restaurar los datos de objetos manualmente):

- No puedes restaurar datos de objetos usando Grid Manager.
- Puedes supervisar el progreso de las tareas de restauración manual mediante Grid Manager.

Una vez realizada la selección, el script finaliza y se muestran los siguientes pasos para recuperar los datos del objeto. Tras revisar estos pasos, pulsa cualquier tecla para volver a la línea de comandos.

Restaurar datos de objetos en un volumen de almacenamiento para una StorageGRID appliance

Después de recuperar los volúmenes de almacenamiento para el nodo de almacenamiento del dispositivo, puedes restaurar los datos de objetos replicados o con código de borrado que se perdieron cuando falló el nodo de almacenamiento.

¿Qué procedimiento debo seguir?

Siempre que sea posible, restaura los datos de los objetos mediante la página **Restauración de volúmenes** en el Grid Manager.

- Si los volúmenes aparecen en **Mantenimiento > Restauración de volúmenes > Nodos para restaurar**,

restaura los datos de objetos mediante ["Página de restauración de volumen en el Grid Manager"](#).

- Si los volúmenes no aparecen en **Mantenimiento > Restauración de volúmenes > Nodos para restaurar**, sigue los pasos que se indican a continuación para usar el script `repair-data` para restaurar datos de objetos.

Si el nodo de almacenamiento recuperado contiene menos volúmenes que el nodo al que sustituye, debes usar el script `repair-data`.



El script `repair-data` está obsoleto y se eliminará en una futura versión. Cuando sea posible, utiliza el ["Procedimiento de restauración del volumen en el Grid Manager"](#).

Utiliza el script `repair-data` para restaurar los datos de los objetos

Antes de empezar

- Has comprobado que el nodo de almacenamiento recuperado presenta un estado de conexión **Conectado**  en la pestaña **Nodos > Resumen** del Grid Manager.

Acerca de esta tarea

Los datos de los objetos se pueden restaurar desde otros Storage Nodes o desde un Cloud Storage Pool, siempre que las reglas de ILM de la grid se hayan configurado de tal forma que haya copias de los objetos disponibles.

Ten en cuenta lo siguiente:

- Si se ha configurado una regla de ILM para almacenar únicamente una copia replicada y dicha copia se encontraba en un volumen de almacenamiento que ha fallado, no podrás recuperar el objeto.
- Si la única copia restante de un objeto se encuentra en un Cloud Storage Pool, StorageGRID debe enviar varias solicitudes al endpoint del Cloud Storage Pool para restaurar los datos del objeto. Antes de realizar este procedimiento, ponte en contacto con soporte técnico para que te ayuden a estimar el plazo de recuperación y los costes asociados.

Acerca del `repair-data` script

Para restaurar los datos de objetos, ejecutas el script `repair-data`. Este script inicia el proceso de restauración de datos de objetos y funciona con el escaneo de ILM para garantizar que se cumplan las reglas de ILM.

Selecciona **Datos replicados** o **Datos con código de borrado (EC)** a continuación para conocer las diferentes opciones del `repair-data` script, en función de si vas a restaurar datos replicados o datos con código de borrado. Si necesitas restaurar ambos tipos de datos, debes ejecutar ambos conjuntos de comandos.



Para obtener más información sobre el script `repair-data`, introduce `repair-data --help` desde la línea de comandos del nodo de administración primario.



El script `repair-data` está obsoleto y se eliminará en una futura versión. Cuando sea posible, utiliza el ["Procedimiento de restauración del volumen en el Grid Manager"](#).

Datos replicados

Hay dos comandos disponibles para restaurar datos replicados, dependiendo de si necesitas reparar todo el nodo o solo ciertos volúmenes en el nodo:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

Puedes realizar un seguimiento de las reparaciones de los datos replicados con este comando:

```
repair-data show-replicated-repair-status
```

Datos con código de borrado (EC)

Hay dos comandos disponibles para la restauración de datos con código de borrado, dependiendo de si necesitas reparar todo el nodo o solo determinados volúmenes del mismo:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Puedes realizar un seguimiento de las reparaciones de los datos con código de borrado con este comando:

```
repair-data show-ec-repair-status
```



Las reparaciones de datos con codificación de borrado pueden comenzar mientras algunos nodos de almacenamiento están sin conexión. Sin embargo, si no se pueden localizar todos los datos con codificación de borrado, la reparación no se podrá completar. La reparación se completará una vez que todos los nodos estén disponibles.



La tarea de reparación de EC reserva temporalmente una gran cantidad de almacenamiento. Es posible que se activen alertas de almacenamiento, pero se resolverán cuando finalice la reparación. Si no hay suficiente almacenamiento para la reserva, la tarea de reparación de EC fallará. Las reservas de almacenamiento se liberan cuando finaliza la tarea de reparación de EC, ya sea que la tarea haya fallado o tenido éxito.

Buscar el nombre de host para el nodo de almacenamiento

1. Inicia sesión en cualquier Admin Node:

- Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.
- Introduce el siguiente comando para pasar a ser usuario root: `su -`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

2. Usa el archivo `/etc/hosts` para buscar el nombre de host del nodo de almacenamiento para los volúmenes de almacenamiento restaurados. Para ver una lista de todos los nodos del grid, introduce lo

siguiente: `cat /etc/hosts`.

Repara los datos si todos los volúmenes han fallado

Si todos los volúmenes de almacenamiento han fallado, repara todo el nodo. Sigue las instrucciones para **datos replicados**, **datos con codificación de borrado (EC)** o ambos, según si usas datos replicados, datos con codificación de borrado (EC) o ambos.

Si solo se han dañado algunos volúmenes, ve a [Repara los datos si solo han fallado algunos volúmenes](#).



No puedes ejecutar operaciones de `repair-data` en más de un nodo al mismo tiempo. Para recuperar varios nodos, ponte en contacto con soporte técnico.

Datos replicados

Si tu grid incluye datos replicados, usa el comando `repair-data start-replicated-node-repair` con la opción `--nodes`, donde `--nodes` es el nombre de host (nombre del sistema), para reparar todo el Storage Node.

Este comando repara los datos replicados en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



A medida que se restauran los datos 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. Debes determinar la causa de la pérdida y si la recuperación es posible. Consulta "[Investiga los objetos que puedan haberse perdido](#)".

Datos con código de borrado (EC)

Si tu grid contiene datos con código de borrado, usa el comando `repair-data start-ec-node-repair` con la opción `--nodes`, donde `--nodes` es el hostname (nombre del sistema), para reparar todo el Storage Node.

Este comando repara los datos con código de borrado en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

La operación devuelve un identificador único `repair ID` que identifica esta `repair_data` operación. Usa este `repair ID` para seguir el progreso y el resultado de la `repair_data` operación. No se devuelve ningún otro comentario cuando finaliza el proceso de recuperación.

Las reparaciones de los datos con código de borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. La reparación se completará cuando todos los nodos estén disponibles.

Repara los datos si solo han fallado algunos volúmenes

Si solo algunos de los volúmenes han fallado, repara los volúmenes afectados. Sigue las instrucciones para **datos replicados**, **datos con código de borrado (EC)** o ambos, en función de si utilizas datos replicados, datos con código de borrado (EC) o ambos.

Si todos los volúmenes han fallado, ve a [Repara los datos si todos los volúmenes han fallado](#).

Introduce los ID de los volúmenes en formato hexadecimal. Por ejemplo, 0000 es el primer volumen y 000F es el decimosexto volumen. Puedes especificar un volumen, un rango de volúmenes o varios volúmenes que no estén en secuencia.

Todos los volúmenes deben estar en el mismo Storage Node. Si necesitas restaurar volúmenes de más de un Storage Node, ponte en contacto con el soporte técnico.

Datos replicados

Si tu grid contiene datos replicados, usa el comando `start-replicated-volume-repair` con la opción `--nodes` para identificar el nodo (donde `--nodes` es el nombre de host del nodo). Luego añade la opción `--volumes` o `--volume-range`, como se muestra en los siguientes ejemplos.

Un solo volumen: Este comando restaura los datos replicados en el volumen 0002 en un nodo de almacenamiento denominado 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 al 0009 en un Storage Node llamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Varios volúmenes no secuenciales: Este comando restaura los datos replicados en los volúmenes 0001, 0005 y 0008 en un Storage Node 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 objetos, se activa la alerta **Objects Lost** si el sistema StorageGRID no puede localizar los datos de objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Toma nota de la descripción de la alerta y de las acciones recomendadas para determinar la causa de la pérdida y si la recuperación es posible.

Datos con código de borrado (EC)

Si tu grid contiene datos con código de borrado, utiliza el comando `start-ec-volume-repair` con la opción `--nodes` para identificar el nodo (donde `--nodes` es el hostname del nodo). Luego añade la opción `--volumes` o `--volume-range`, como se muestra en los siguientes ejemplos.

Volumen único: este comando restaura datos con codificación de borrado en el volumen 0007 de un Storage Node llamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Rango de volúmenes: Este comando restaura los datos con código de borrado en todos los volúmenes comprendidos entre 0004 y 0006 en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Varios volúmenes no consecutivos: Este comando restaura datos con código de borrado en los volúmenes 000A, 000C y 000E de un Storage Node denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

La `repair-data` operación devuelve un `repair ID` único que identifica esta `repair_data` operación. Usa este `repair ID` para seguir el progreso y el resultado de la `repair_data` operación. No se devuelve ningún otro comentario cuando finaliza el proceso de recuperación.



Las reparaciones de los datos con código de borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. La reparación se completará cuando todos los nodos estén disponibles.

Supervisar reparaciones

Supervisa el estado de los trabajos de reparación, dependiendo de si utilizas **datos replicados**, **datos con código de borrado (EC)** o ambos.

También puedes supervisar el estado de las tareas de restauración de volúmenes en curso y consultar el historial de las tareas de restauración completadas en ["Grid Manager"](#).

Datos replicados

- Para obtener un porcentaje estimado de finalización de la reparación replicada, añade la opción `show-replicated-repair-status` al comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Para comprobar si las reparaciones se han completado:
 - a. Selecciona **Nodos > Nodo de almacenamiento en reparación > ILM**.
 - b. Revisa los atributos en la sección de evaluación. Cuando se completen las reparaciones, el atributo **Awaiting - All** indica 0 objetos.
- Para monitorear la reparación con más detalle:
 - a. Selecciona **Nodos**.
 - b. Selecciona **nombre de la cuadrícula > ILM**.
 - c. Coloca el cursor sobre el gráfico de la cola de ILM para ver el valor del atributo **Frecuencia de escaneo (objetos/seg)**, que es la velocidad a la que se escanean los objetos en el grid y se colocan en la cola de ILM.
 - d. En la sección Cola de ILM, fíjate en los siguientes atributos:
 - **Duración del escaneo - estimada:** El tiempo estimado para completar un escaneo ILM completo de todos los objetos.

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

- **Reparaciones intentadas:** el número total de operaciones de reparación de objetos intentadas para datos replicados que se consideran de alto riesgo. Los objetos de alto riesgo son aquellos a los que les queda una sola copia, ya sea porque así lo especifica la política de ILM o como resultado de la pérdida de copias. Este recuento se incrementa cada vez que un Storage Node intenta reparar un objeto de alto riesgo. Las reparaciones de ILM de alto riesgo se priorizan si el grid se ocupa.

La misma reparación de objetos podría volver a incrementarse si la replicación falló después de la reparación. + Estos atributos pueden ser útiles cuando estés monitorizando el progreso de la recuperación de volúmenes del Storage Node. Si el número de intentos de reparación ha dejado de aumentar y se ha completado un escaneo completo, es probable que la reparación haya finalizado.

- e. Como alternativa, envía una consulta de Prometheus para `storagegrid_ilm_scan_period_estimated_minutes` y `storagegrid_ilm_repairs_attempted`.

Datos con código de borrado (EC)

Para supervisar la reparación de los datos con código de borrado y volver a intentar cualquier solicitud que haya podido fallar:

1. Determina el estado de las reparaciones de los datos con código de borrado:
 - Selecciona **Support > Tools > Metrics** para ver el tiempo estimado hasta la finalización y el porcentaje de finalización del trabajo actual. Luego, selecciona **EC Overview** en la sección de Grafana. Consulta los paneles **Grid EC Job Estimated Time to Completion** y **Grid EC Job Percentage Completed**.

- Usa este comando para ver el estado de una operación `repair-data` específica:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Utiliza este comando para listar todas las reparaciones:

```
repair-data show-ec-repair-status
```

El resultado muestra información, incluida `repair ID`, sobre todas las reparaciones que se han realizado anteriormente y las que se están llevando a cabo actualmente.

2. Si el resultado indica que la operación de reparación ha fallado, utiliza la opción `--repair-id` para volver a intentar la reparación.

Este comando vuelve a intentar la reparación de un nodo que ha fallado, usando el ID de reparación 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando vuelve a intentar una reparación de volumen que ha fallado, usando el ID de reparación 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Comprueba el estado del almacenamiento después de recuperar un StorageGRID appliance Storage Node

Después de recuperar un nodo de almacenamiento del appliance, debes verificar que el estado deseado del nodo de almacenamiento del appliance esté configurado como en línea y asegurarte de que el estado será en línea de forma predeterminada cada vez que se reinicie el servidor del nodo de almacenamiento.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- El nodo de almacenamiento se ha recuperado y la recuperación de datos ha finalizado.

Pasos

1. Selecciona **Nodos > Storage Node > Tareas**.
2. Si la lista desplegable **Estado de almacenamiento** está configurada en **Solo lectura** o **Sin conexión**, selecciona **En línea**.
3. Selecciona **Guardar**.

Recupérate de un fallo del volumen de almacenamiento cuando la unidad del sistema está intacta

Recupera de un fallo de volumen de almacenamiento StorageGRID donde la unidad del sistema está intacta

Debes completar una serie de tareas para recuperar un nodo de almacenamiento

basado en software en el que hayan fallado uno o más volúmenes de almacenamiento, pero la unidad del sistema esté intacta. Si solo han fallado los volúmenes de almacenamiento, el nodo de almacenamiento sigue estando disponible para el sistema StorageGRID.



Este procedimiento de recuperación se aplica únicamente a los nodos de almacenamiento basados en software. Si se han producido fallos en los volúmenes de almacenamiento de un nodo de almacenamiento de un dispositivo, usa en su lugar el procedimiento correspondiente al dispositivo: ["Recuperar el nodo de almacenamiento del appliance"](#).

Este procedimiento de recuperación incluye las siguientes tareas:

- ["Revisa las advertencias relativas a la recuperación del volumen de almacenamiento"](#)
- ["Identifica y desmonta los volúmenes de almacenamiento que presentan fallos"](#)
- ["Recupera los volúmenes y reconstruye la base de datos de Cassandra"](#)
- ["Restaurar los datos de los objetos"](#)
- ["Comprueba el estado de almacenamiento"](#)

Advertencias para la recuperación de volúmenes de almacenamiento StorageGRID

Antes de recuperar volúmenes de almacenamiento que han fallado en un Storage Node, revisa las siguientes advertencias.

Los volúmenes de almacenamiento (o rangedbs) en un Storage Node se identifican por un número hexadecimal, que se conoce como el ID de volumen. Por ejemplo, 0000 es el primer volumen y 000F es el volumen dieciséis. El primer almacén de objetos (volumen 0) en cada Storage Node usa hasta 4 TB de espacio para metadatos de objetos y operaciones de la base de datos Cassandra; cualquier espacio restante en ese volumen se usa para datos de objetos. Todos los demás volúmenes de almacenamiento se usan exclusivamente para datos de objetos.

La base de datos Cassandra podría reconstruirse como parte del procedimiento de recuperación del volumen si:

- El volumen 0 falla y se recupera.
- La unidad del sistema y uno o varios volúmenes de almacenamiento fallan y se recuperan.

Cuando se reconstruye Cassandra, el sistema utiliza información de otros nodos de almacenamiento. Si Cassandra se ha reconstruido recientemente, es posible que los datos de Cassandra aún no sean consistentes en todo el grid. Si hay demasiados nodos de almacenamiento fuera de línea:

- Es posible que algunos datos de Cassandra no estén disponibles.
- Podría producirse una pérdida de datos.



Si se ha producido un fallo en más de un nodo de almacenamiento (o está desconectado), ponte en contacto con soporte técnico. No realices el siguiente procedimiento de recuperación. Podría producirse una pérdida de datos. Para obtener más información, consulta ["Cómo el soporte técnico recupera un sitio"](#).



Si las reglas de ILM están configuradas para almacenar únicamente una copia replicada y dicha copia se encuentra en un volumen de almacenamiento que ha fallado, no podrás recuperar el objeto.

Información relacionada

["Advertencias y consideraciones para la recuperación de nodos de la red"](#)

Identifica y desmonta volúmenes de almacenamiento fallidos en StorageGRID

Al recuperar un nodo de almacenamiento con volúmenes de almacenamiento defectuosos, debes identificar y desmontar los volúmenes defectuosos. Debes asegurarte de que solo los volúmenes de almacenamiento defectuosos se reformateen como parte del procedimiento de recuperación.

Antes de empezar

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

Acerca de esta tarea

Debes recuperar los volúmenes de almacenamiento que hayan fallado lo antes posible.

El primer paso del proceso de recuperación consiste en detectar los volúmenes que se han desconectado, que deben desmontarse o que presentan errores de E/S. Si los volúmenes defectuosos siguen conectados pero tienen un sistema de archivos dañado de forma aleatoria, es posible que el sistema no detecte ningún daño en las partes del disco que no se utilizan o que no están asignadas.



Debes terminar este procedimiento antes de realizar pasos manuales para recuperar los volúmenes, como añadir o volver a conectar los discos, detener el nodo, iniciar el nodo o reiniciar. De lo contrario, cuando ejecutes el `reformat_storage_block_devices.rb` script, podrías encontrarte con un error del sistema de archivos que haga que el script se quede colgado o falle.



Repara el hardware y conecta correctamente los discos antes de ejecutar el comando `reboot`.



Identifica con cuidado los volúmenes de almacenamiento defectuosos. Utilizarás esta información para comprobar qué volúmenes deben reformatearse. Una vez que se ha reformateado un volumen, los datos en el volumen no se pueden recuperar.

Para recuperar los volúmenes de almacenamiento que han fallado, necesitas conocer tanto los nombres de los dispositivos de los volúmenes que fallaron como sus IDs de volumen.

Durante la instalación, a cada dispositivo de almacenamiento se le asigna un identificador único universal (UUID) del sistema de archivos y se monta en un directorio `rangedb` del nodo de almacenamiento utilizando ese UUID del sistema de archivos asignado. El UUID del sistema de archivos y el directorio `rangedb` aparecen en el archivo `/etc/fstab`. El punto de montaje, el nombre del dispositivo y el tamaño del volumen se muestran en Grid Manager.

Pasos

1. Sigue los siguientes pasos para registrar los volúmenes de almacenamiento que han fallado y los nombres de sus dispositivos:
 - a. Selecciona **Nodos > site > Nodo de almacenamiento con fallo > Almacenamiento**.

b. Desplázate hacia abajo hasta encontrar las tablas Volúmenes y Almacenes de objetos y anota la siguiente información para cada volumen con estado Desconocido o Sin conexión.

- En la tabla de Volúmenes, anota el punto de montaje, el dispositivo y el tamaño.
- En la tabla de almacenes de objetos, anota el `object_store_ID`.

El `object_store_ID` es el ID del volumen de almacenamiento que ha fallado. Por ejemplo, especifica 0 en el comando para un almacén de objetos con ID 0000.

2. Inicia sesión en el nodo de almacenamiento que ha fallado:

- Introduce el siguiente comando: `ssh admin@grid_node_IP`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.
- Introduce el siguiente comando para pasar a ser usuario root: `su -`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

3. Ejecuta el siguiente script para desmontar un volumen de almacenamiento que ha fallado:

```
sn-unmount-volume object_store_ID
```

4. Si se te solicita, pulsa **y** para detener el servicio de Cassandra que depende del volumen de almacenamiento 0.



Si el servicio de Cassandra ya está detenido, no aparecerá ningún mensaje. El servicio de Cassandra solo se detiene para el volumen 0.

```
root@Storage-180:~/var/local/tmp/storage~ # sn-unmount-volume 0
Services depending on storage volume 0 (cassandra) aren't down.
Services depending on storage volume 0 must be stopped before running
this script.
Stop services that require storage volume 0 [y/N]? y
Shutting down services that require storage volume 0.
Services requiring storage volume 0 stopped.
Unmounting /var/local/rangedb/0
/var/local/rangedb/0 is unmounted.
```

En unos segundos, el volumen se desmonta. Aparecen mensajes que indican cada paso del proceso. El mensaje final indica que el volumen se desmonta.

5. Si el desmontaje falla porque el volumen está ocupado, puedes forzar el desmontaje utilizando la opción `--use-umountof`:



Forzar el desmontaje mediante la opción `--use-umountof` podría provocar que los procesos o servicios que utilizan el volumen se comporten de forma 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
```

Recupera volúmenes de almacenamiento fallidos y reconstruye la base de datos Cassandra en StorageGRID

Debes ejecutar un script que reformatee y vuelva a montar el almacenamiento en los volúmenes de almacenamiento que hayan fallado, y que reconstruya la base de datos de Cassandra en el Storage Node si el sistema determina que es necesario.

Antes de empezar

- Tienes el archivo `Passwords.txt`.
- Las unidades del sistema en el servidor están intactas.
- Se ha identificado la causa del fallo y, si es necesario, ya se ha adquirido el hardware de almacenamiento de repuesto.
- El tamaño total del almacenamiento de reemplazo es el mismo que el original.
- Has comprobado que no se está llevando a cabo el proceso de decomisionar un nodo de almacenamiento, o bien has pausado dicho proceso. (En Grid Manager, selecciona **Mantenimiento > Tareas > Decomisionar**.)
- Has comprobado que no hay ninguna expansión en curso. (En el Grid Manager, selecciona **Mantenimiento > Tareas > Expansión**.)
- Tienes ["has revisado las advertencias sobre la recuperación del volumen de almacenamiento"](#).

Pasos

1. Según sea necesario, reemplaza el almacenamiento físico o virtual defectuoso asociado con los volúmenes de almacenamiento defectuosos que identificaste y desmontaste antes.

No vuelvas a montar los volúmenes en este paso. El almacenamiento se vuelve a montar y se añade a `/etc/fstab` en un paso posterior.

2. En el Administrador de Grid, ve a **Nodos > appliance Storage Node > Hardware**. En la sección StorageGRID Appliance de la página, verifica que el modo RAID de almacenamiento esté en buen estado.
3. Inicia sesión en el nodo de almacenamiento que ha fallado:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

4. Utiliza un editor de texto (vi o vim) para eliminar los volúmenes con errores del archivo `/etc/fstab` y

luego guarda el archivo.



No basta con comentar un volumen defectuoso en el archivo `/etc/fstab`. El volumen debe eliminarse de `fstab` ya que el proceso de recuperación comprueba que todas las líneas del archivo `fstab` coincidan con los sistemas de archivos montados.

5. Reformatea cualquier volumen de almacenamiento que haya fallado y reconstruye la base de datos de Cassandra si es necesario. Introduce: `reformat_storage_block_devices.rb`

- Cuando se desmonte el volumen de almacenamiento 0, aparecerán avisos y mensajes que indicarán que se está deteniendo el servicio de Cassandra.
- Se te pedirá que vuelvas a crear la base de datos de Cassandra si es necesario.
 - Revisa las advertencias. Si ninguna de ellas es aplicable, vuelve a crear la base de datos de Cassandra. Introduce: **y**
 - Si hay más de un nodo de almacenamiento desconectado. Introduce: **n**

El script se cerrará sin reconstruir Cassandra. Ponte en contacto con soporte técnico.

- Para cada unidad `rangedb` del Storage Node, cuando se te pregunte: `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`, introduce una de las siguientes respuestas:
 - **y** para reformatear una unidad que presentaba errores. Esto reformatea el volumen de almacenamiento y añade el volumen reformateado al archivo `/etc/fstab`.
 - **n** si la unidad no presenta errores y no quieres volver a formatearla.



Si seleccionas **n**, se sale del script. Monta la unidad (si crees que los datos que contiene deben conservarse y se ha desmontado por error) o retírala. Luego, ejecuta de nuevo el comando `reformat_storage_block_devices.rb`.



Algunos procedimientos de recuperación de StorageGRID utilizan Reaper para gestionar las reparaciones de Cassandra. Las reparaciones se llevan a cabo automáticamente en cuanto se han iniciado los servicios relacionados o necesarios. Es posible que veas en la salida del script menciones a "reaper" o "reparación de Cassandra". Si aparece un mensaje de error que indica que la reparación ha fallado, ejecuta el comando que se indica en dicho mensaje.

En el siguiente ejemplo de salida, la unidad `/dev/sdf` debe volver a formatearse, y Cassandra no necesitó ser reconstruida:


```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? y
Successfully formatted /dev/sdf with UUID b951bfcb-4804-41ad-b490-
805dfd8df16c
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12368435
Cassandra does not need rebuilding.
Starting services.
Informing storage services of new volume

Reformatting done. Now do manual steps to
restore copies of data.
```

Una vez que se hayan reformateado y vuelto a montar los volúmenes de almacenamiento y se hayan completado las operaciones necesarias de Cassandra, puedes ["restaura datos de objetos usando Grid Manager"](#).

Restaurar los datos de objetos en el volumen de almacenamiento StorageGRID donde la unidad del sistema está intacta

Tras recuperar un volumen de almacenamiento en un nodo de almacenamiento en el que la unidad del sistema está intacta, puedes restaurar los datos de los objetos replicados o con código de borrado que se perdieron cuando falló el volumen de almacenamiento.

¿Qué procedimiento debo seguir?

Siempre que sea posible, restaura los datos de los objetos mediante la página **Restauración de volúmenes** en el Grid Manager.

- Si los volúmenes aparecen en **Mantenimiento > Restauración de volúmenes > Nodos para restaurar**, restaura los datos de objetos mediante ["Página de restauración de volumen en el Grid Manager"](#).
- Si los volúmenes no aparecen en **Mantenimiento > Restauración de volúmenes > Nodos para restaurar**, sigue los pasos que se indican a continuación para usar el script `repair-data` para restaurar datos de objetos.

Si el nodo de almacenamiento recuperado contiene menos volúmenes que el nodo al que sustituye, debes usar el script `repair-data`.



El script `repair-data` está obsoleto y se eliminará en una futura versión. Cuando sea posible, utiliza el ["Procedimiento de restauración del volumen en el Grid Manager"](#).

Utiliza el script `repair-data` para restaurar los datos de los objetos

Antes de empezar

- Has comprobado que el nodo de almacenamiento recuperado presenta un estado de conexión **Conectado**  en la pestaña **Nodos > Resumen** del Grid Manager.

Acerca de esta tarea

Los datos de los objetos se pueden restaurar desde otros Storage Nodes o desde un Cloud Storage Pool, siempre que las reglas de ILM de la grid se hayan configurado de tal forma que haya copias de los objetos disponibles.

Ten en cuenta lo siguiente:

- Si se ha configurado una regla de ILM para almacenar únicamente una copia replicada y dicha copia se encontraba en un volumen de almacenamiento que ha fallado, no podrás recuperar el objeto.
- Si la única copia restante de un objeto se encuentra en un Cloud Storage Pool, StorageGRID debe enviar varias solicitudes al endpoint del Cloud Storage Pool para restaurar los datos del objeto. Antes de realizar este procedimiento, ponte en contacto con soporte técnico para que te ayuden a estimar el plazo de recuperación y los costes asociados.

Acerca del `repair-data` script

Para restaurar los datos de objetos, ejecutas el script `repair-data`. Este script inicia el proceso de restauración de datos de objetos y funciona con el escaneo de ILM para garantizar que se cumplan las reglas de ILM.

Selecciona **Datos replicados** o **Datos con código de borrado (EC)** a continuación para conocer las diferentes opciones del `repair-data` script, en función de si vas a restaurar datos replicados o datos con código de borrado. Si necesitas restaurar ambos tipos de datos, debes ejecutar ambos conjuntos de comandos.



Para obtener más información sobre el script `repair-data`, introduce `repair-data --help` desde la línea de comandos del nodo de administración primario.



El script `repair-data` está obsoleto y se eliminará en una futura versión. Cuando sea posible, utiliza el ["Procedimiento de restauración del volumen en el Grid Manager"](#).

Datos replicados

Hay dos comandos disponibles para restaurar datos replicados, dependiendo de si necesitas reparar todo el nodo o solo ciertos volúmenes en el nodo:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

Puedes realizar un seguimiento de las reparaciones de los datos replicados con este comando:

```
repair-data show-replicated-repair-status
```

Datos con código de borrado (EC)

Hay dos comandos disponibles para la restauración de datos con código de borrado, dependiendo de si necesitas reparar todo el nodo o solo determinados volúmenes del mismo:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Puedes realizar un seguimiento de las reparaciones de los datos con código de borrado con este comando:

```
repair-data show-ec-repair-status
```



Las reparaciones de datos con codificación de borrado pueden comenzar mientras algunos nodos de almacenamiento están sin conexión. Sin embargo, si no se pueden localizar todos los datos con codificación de borrado, la reparación no se podrá completar. La reparación se completará una vez que todos los nodos estén disponibles.



La tarea de reparación de EC reserva temporalmente una gran cantidad de almacenamiento. Es posible que se activen alertas de almacenamiento, pero se resolverán cuando finalice la reparación. Si no hay suficiente almacenamiento para la reserva, la tarea de reparación de EC fallará. Las reservas de almacenamiento se liberan cuando finaliza la tarea de reparación de EC, ya sea que la tarea haya fallado o tenido éxito.

Buscar el nombre de host para el nodo de almacenamiento

1. Inicia sesión en cualquier Admin Node:

- Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.
- Introduce el siguiente comando para pasar a ser usuario root: `su -`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

2. Usa el archivo `/etc/hosts` para buscar el nombre de host del nodo de almacenamiento para los volúmenes de almacenamiento restaurados. Para ver una lista de todos los nodos del grid, introduce lo

siguiente: `cat /etc/hosts`.

Repara los datos si todos los volúmenes han fallado

Si todos los volúmenes de almacenamiento han fallado, repara todo el nodo. Sigue las instrucciones para **datos replicados**, **datos con codificación de borrado (EC)** o ambos, según si usas datos replicados, datos con codificación de borrado (EC) o ambos.

Si solo se han dañado algunos volúmenes, ve a [Repara los datos si solo han fallado algunos volúmenes](#).



No puedes ejecutar operaciones de `repair-data` en más de un nodo al mismo tiempo. Para recuperar varios nodos, ponte en contacto con soporte técnico.

Datos replicados

Si tu grid incluye datos replicados, usa el comando `repair-data start-replicated-node-repair` con la opción `--nodes`, donde `--nodes` es el nombre de host (nombre del sistema), para reparar todo el Storage Node.

Este comando repara los datos replicados en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



A medida que se restauran los datos 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. Debes determinar la causa de la pérdida y si la recuperación es posible. Consulta "[Investiga los objetos que puedan haberse perdido](#)".

Datos con código de borrado (EC)

Si tu grid contiene datos con código de borrado, usa el comando `repair-data start-ec-node-repair` con la opción `--nodes`, donde `--nodes` es el hostname (nombre del sistema), para reparar todo el Storage Node.

Este comando repara los datos con código de borrado en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

La operación devuelve un identificador único `repair ID` que identifica esta `repair_data` operación. Usa este `repair ID` para seguir el progreso y el resultado de la `repair_data` operación. No se devuelve ningún otro comentario cuando finaliza el proceso de recuperación.

Las reparaciones de los datos con código de borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. La reparación se completará cuando todos los nodos estén disponibles.

Repara los datos si solo han fallado algunos volúmenes

Si solo algunos de los volúmenes han fallado, repara los volúmenes afectados. Sigue las instrucciones para **datos replicados**, **datos con código de borrado (EC)** o ambos, en función de si utilizas datos replicados, datos con código de borrado (EC) o ambos.

Si todos los volúmenes han fallado, ve a [Repara los datos si todos los volúmenes han fallado](#).

Introduce los ID de los volúmenes en formato hexadecimal. Por ejemplo, 0000 es el primer volumen y 000F es el decimosexto volumen. Puedes especificar un volumen, un rango de volúmenes o varios volúmenes que no estén en secuencia.

Todos los volúmenes deben estar en el mismo Storage Node. Si necesitas restaurar volúmenes de más de un Storage Node, ponte en contacto con el soporte técnico.

Datos replicados

Si tu grid contiene datos replicados, usa el comando `start-replicated-volume-repair` con la opción `--nodes` para identificar el nodo (donde `--nodes` es el nombre de host del nodo). Luego añade la opción `--volumes` o `--volume-range`, como se muestra en los siguientes ejemplos.

Un solo volumen: Este comando restaura los datos replicados en el volumen 0002 en un nodo de almacenamiento denominado 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 al 0009 en un Storage Node llamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Varios volúmenes no secuenciales: Este comando restaura los datos replicados en los volúmenes 0001, 0005 y 0008 en un Storage Node 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 objetos, se activa la alerta **Objects Lost** si el sistema StorageGRID no puede localizar los datos de objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Toma nota de la descripción de la alerta y de las acciones recomendadas para determinar la causa de la pérdida y si la recuperación es posible.

Datos con código de borrado (EC)

Si tu grid contiene datos con código de borrado, utiliza el comando `start-ec-volume-repair` con la opción `--nodes` para identificar el nodo (donde `--nodes` es el hostname del nodo). Luego añade la opción `--volumes` o `--volume-range`, como se muestra en los siguientes ejemplos.

Volumen único: este comando restaura datos con codificación de borrado en el volumen 0007 de un Storage Node llamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Rango de volúmenes: Este comando restaura los datos con código de borrado en todos los volúmenes comprendidos entre 0004 y 0006 en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Varios volúmenes no consecutivos: Este comando restaura datos con código de borrado en los volúmenes 000A, 000C y 000E de un Storage Node denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

La `repair-data` operación devuelve un `repair ID` único que identifica esta `repair_data` operación. Usa este `repair ID` para seguir el progreso y el resultado de la `repair_data` operación. No se devuelve ningún otro comentario cuando finaliza el proceso de recuperación.



Las reparaciones de los datos con código de borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. La reparación se completará cuando todos los nodos estén disponibles.

Supervisar reparaciones

Supervisa el estado de los trabajos de reparación, dependiendo de si utilizas **datos replicados**, **datos con código de borrado (EC)** o ambos.

También puedes supervisar el estado de las tareas de restauración de volúmenes en curso y consultar el historial de las tareas de restauración completadas en ["Grid Manager"](#).

Datos replicados

- Para obtener un porcentaje estimado de finalización de la reparación replicada, añade la opción `show-replicated-repair-status` al comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Para comprobar si las reparaciones se han completado:
 - a. Selecciona **Nodos > Nodo de almacenamiento en reparación > ILM**.
 - b. Revisa los atributos en la sección de evaluación. Cuando se completen las reparaciones, el atributo **Awaiting - All** indica 0 objetos.
- Para monitorear la reparación con más detalle:
 - a. Selecciona **Nodos**.
 - b. Selecciona **nombre de la cuadrícula > ILM**.
 - c. Coloca el cursor sobre el gráfico de la cola de ILM para ver el valor del atributo **Frecuencia de escaneo (objetos/seg)**, que es la velocidad a la que se escanean los objetos en el grid y se colocan en la cola de ILM.
 - d. En la sección Cola de ILM, fíjate en los siguientes atributos:
 - **Duración del escaneo - estimada:** El tiempo estimado para completar un escaneo ILM completo de todos los objetos.

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

- **Reparaciones intentadas:** el número total de operaciones de reparación de objetos intentadas para datos replicados que se consideran de alto riesgo. Los objetos de alto riesgo son aquellos a los que les queda una sola copia, ya sea porque así lo especifica la política de ILM o como resultado de la pérdida de copias. Este recuento se incrementa cada vez que un Storage Node intenta reparar un objeto de alto riesgo. Las reparaciones de ILM de alto riesgo se priorizan si el grid se ocupa.

La misma reparación de objetos podría volver a incrementarse si la replicación falló después de la reparación. + Estos atributos pueden ser útiles cuando estés monitorizando el progreso de la recuperación de volúmenes del Storage Node. Si el número de intentos de reparación ha dejado de aumentar y se ha completado un escaneo completo, es probable que la reparación haya finalizado.

- e. Como alternativa, envía una consulta de Prometheus para `storagegrid_ilm_scan_period_estimated_minutes` y `storagegrid_ilm_repairs_attempted`.

Datos con código de borrado (EC)

Para supervisar la reparación de los datos con código de borrado y volver a intentar cualquier solicitud que haya podido fallar:

1. Determina el estado de las reparaciones de los datos con código de borrado:
 - Selecciona **Support > Tools > Metrics** para ver el tiempo estimado hasta la finalización y el porcentaje de finalización del trabajo actual. Luego, selecciona **EC Overview** en la sección de Grafana. Consulta los paneles **Grid EC Job Estimated Time to Completion** y **Grid EC Job Percentage Completed**.

- Usa este comando para ver el estado de una operación `repair-data` específica:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Utiliza este comando para listar todas las reparaciones:

```
repair-data show-ec-repair-status
```

El resultado muestra información, incluida `repair ID`, sobre todas las reparaciones que se han realizado anteriormente y las que se están llevando a cabo actualmente.

2. Si el resultado indica que la operación de reparación ha fallado, utiliza la opción `--repair-id` para volver a intentar la reparación.

Este comando vuelve a intentar la reparación de un nodo que ha fallado, usando el ID de reparación 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando vuelve a intentar una reparación de volumen que ha fallado, usando el ID de reparación 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Comprueba el estado del almacenamiento después de recuperar los volúmenes de almacenamiento de StorageGRID

Después de recuperar los volúmenes de almacenamiento, debes verificar que el estado deseado del nodo de almacenamiento esté en línea y asegurarte de que el estado sea en línea por defecto cada vez que se reinicie el servidor del nodo de almacenamiento.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- El nodo de almacenamiento se ha recuperado y la recuperación de datos ha finalizado.

Pasos

1. Selecciona **Nodos > Storage Node > Tareas**.
2. Si la lista desplegable **Estado de almacenamiento** está configurada en **Solo lectura** o **Sin conexión**, selecciona **En línea**.
3. Selecciona **Guardar**.

Recupera tu sistema tras un fallo de unidad

Advertencias para la recuperación de la unidad del sistema de StorageGRID Storage Node

Antes de recuperar una unidad con error en un nodo de almacenamiento, revisa la guía general ["Advertencias y consideraciones para la recuperación de nodos de grid"](#) y las siguientes advertencias específicas.

Los nodos de almacenamiento cuentan con una base de datos Cassandra que incluye metadatos de objetos. La base de datos Cassandra podría reconstruirse si:

- Un volumen de almacenamiento falla y se recupera.
- La unidad del sistema y uno o varios volúmenes de almacenamiento fallan y se recuperan.

Cuando se reconstruye Cassandra, el sistema utiliza información de otros nodos de almacenamiento. Si Cassandra se ha reconstruido recientemente, es posible que los datos de Cassandra aún no sean consistentes en todo el grid. Si hay demasiados nodos de almacenamiento fuera de línea:

- Es posible que algunos datos de Cassandra no estén disponibles.
- Podría producirse una pérdida de datos.



Si se ha producido un fallo en más de un nodo de almacenamiento (o está desconectado), ponte en contacto con soporte técnico. No realices el siguiente procedimiento de recuperación. Podría producirse una pérdida de datos. Para obtener más información, consulta ["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 defectuosos, recupera los volúmenes en el nodo de almacenamiento con volúmenes defectuosos antes de recuperar este nodo de almacenamiento defectuoso. Consulta las instrucciones para ["Recuperar de un fallo en el volumen de almacenamiento cuando la unidad del sistema está intacta"](#).



Si las reglas de ILM están configuradas para almacenar únicamente una copia replicada y dicha copia se encuentra en un volumen de almacenamiento que ha fallado, no podrás recuperar el objeto.

Reemplaza el nodo de almacenamiento StorageGRID

Si la unidad del sistema ha fallado, primero debes sustituir el nodo de almacenamiento.

Debes seleccionar el procedimiento de sustitución de nodos correspondiente a tu plataforma. Los pasos para sustituir un nodo son los mismos para todos los tipos de nodos de la grid.



Este procedimiento se aplica únicamente a los nodos de almacenamiento basados en software. Debes seguir un procedimiento diferente para ["Recupera un nodo de almacenamiento de un dispositivo"](#).

Linux: Si no estás seguro de si tu unidad del sistema ha fallado, sigue las instrucciones para sustituir el nodo y determinar qué pasos de recuperación son necesarios.

Plataforma	Procedimiento
VMware	"Sustituir un nodo de VMware"
Linux	"Sustituir un nodo de Linux"

Plataforma	Procedimiento
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 necesitas recuperar un nodo que se ejecuta en una implementación de OpenStack, descarga los archivos para tu sistema operativo Linux. Luego, sigue el procedimiento para "Reemplazar un nodo Linux" .

Selecciona Iniciar recuperación para configurar el nodo de almacenamiento StorageGRID

Después de reemplazar un nodo de almacenamiento, debes seleccionar Start Recovery en el Grid Manager para configurar el nuevo nodo como reemplazo del nodo fallido.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- Tienes la frase de contraseña de aprovisionamiento.
- Ya has implementado y configurado el nodo de sustitución.
- Dispones de la fecha de inicio de cualquier trabajo de reparación de datos con código de borrado.

Acerca de esta tarea

Si el nodo de almacenamiento está instalado como contenedor en un host Linux, solo debes realizar este paso si se cumple alguna de las siguientes condiciones:

- Tenías que usar la `--force` bandera para importar el nodo, o ejecutaste `storagegrid node force-recovery node-name`
- Tenías que reinstalar el nodo por completo o necesitabas restaurar `/var/local`.

Pasos

1. Desde el Grid Manager, selecciona **Maintenance > Tasks > Recovery**.
2. Selecciona el nodo de la grid que deseas recuperar en la lista Nodos pendientes.

Los nodos aparecen en la lista tras sufrir un fallo, pero no puedes seleccionar un nodo hasta que se haya reinstalado y esté listo para la recuperación.

3. Introduce la **frase de contraseña de aprovisionamiento**.
4. Haz 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. Supervisa el progreso de la recuperación en la tabla Recuperando nodo de grid.



Mientras se está ejecutando el procedimiento de recuperación, puedes hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparecerá un cuadro de diálogo en el que se indica que el nodo quedará en un estado indeterminado si restableces 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 quieres volver a intentar la recuperación después de reiniciar el procedimiento, debes restaurar el nodo a un estado preinstalado, así:

- **VMware:** Elimina el nodo de grid virtual desplegado. Luego, cuando estés listo para reiniciar la recuperación, vuelve a desplegar el nodo.
- **Linux:** Reinicia el nodo ejecutando este comando en el host Linux: `storagegrid node force-recovery node-name`

6. Cuando el nodo de almacenamiento llegue a la fase «Esperando pasos manuales», ve a ["Volver a montar y reformatear los 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 formatear los volúmenes de almacenamiento StorageGRID (pasos manuales)

Debes ejecutar manualmente dos scripts para volver a montar los volúmenes de almacenamiento conservados y para reformatear cualquier volumen de almacenamiento que haya fallado. El primer script vuelve a montar los volúmenes que están correctamente formateados como volúmenes de almacenamiento de StorageGRID. El segundo script reformatea cualquier volumen desmontado, reconstruye Cassandra, si es necesario, e inicia los servicios.

Antes de empezar

- Ya has sustituido el hardware de cualquier volumen de almacenamiento fallido que sabes que requiere reemplazo.

Ejecutar el `sn-remount-volumes` script podría ayudarte a identificar otros volúmenes de almacenamiento que hayan fallado.

- Has comprobado que no se está llevando a cabo el proceso de decomisionar un nodo de almacenamiento, o bien has pausado dicho proceso. (En Grid Manager, selecciona **Mantenimiento > Tareas > Decomisionar.**)
- Has comprobado que no hay ninguna expansión en curso. (En el Grid Manager, selecciona **Mantenimiento > Tareas > Expansión.**)
- Tienes "[Revisé las advertencias sobre la recuperación de la unidad del sistema del Storage Node](#)".



Ponte en contacto con el soporte técnico si hay más de un nodo de almacenamiento desconectado. No ejecutes el `sn-recovery-postinstall.sh` script.

Acerca de esta tarea

Para completar este procedimiento, debes realizar estas tareas a grandes rasgos:

- Inicia sesión en el nodo de almacenamiento recuperado.
- Ejecuta el `sn-remount-volumes` script para volver a montar los volúmenes de almacenamiento con el formato adecuado. Cuando se ejecuta este script, realiza lo siguiente:
 - Monta y desmonta cada volumen de almacenamiento para reproducir el journal de XFS.
 - Realiza una comprobación de la coherencia de archivos XFS.
 - Si el sistema de archivos es coherente, determina si el volumen de almacenamiento es un volumen de almacenamiento StorageGRID formateado correctamente.
 - Si el volumen de almacenamiento está formateado correctamente, vuelve a montar el volumen de almacenamiento. Los datos existentes en el volumen permanecen intactos.

- Revisa el resultado del script y resuelve cualquier problema.
- Ejecuta el `sn-recovery-postinstall.sh` script. Cuando se ejecuta este script, realiza lo siguiente.



No reinicies un nodo de almacenamiento durante la recuperación antes de ejecutar `sn-recovery-postinstall.sh` para reformatear los volúmenes de almacenamiento que han fallado y restaurar los metadatos de los objetos. Reiniciar el nodo de almacenamiento antes de que `sn-recovery-postinstall.sh` finalice provoca errores en los servicios que intentan iniciarse y hace que los nodos del dispositivo StorageGRID salgan del modo de mantenimiento. Consulta el paso para [script de postinstalación](#).

- Reformatea cualquier volumen de almacenamiento que el `sn-remount-volumes` script no haya podido montar o que se haya detectado que está formateado incorrectamente.



Si se vuelve a formatear un volumen de almacenamiento, se perderán todos los datos que contenga. Debes realizar un procedimiento adicional para restaurar los datos de objetos desde otras ubicaciones en el grid, suponiendo que las reglas de ILM se hayan configurado para almacenar más de una copia de cada objeto.

- Reconstruye la base de datos de Cassandra en el nodo, si es necesario.
- Inicia los servicios en el nodo de almacenamiento.

Pasos

1. Inicia sesión en el nodo de almacenamiento recuperado:

- a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
- b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
- d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de \$ a #.

2. Ejecuta el primer script para volver a montar los volúmenes de almacenamiento que estén correctamente formateados.



Si todos los volúmenes de almacenamiento son nuevos y hay que formatearlos, o si todos los volúmenes de almacenamiento han fallado, puedes saltarte este paso y ejecutar el segundo script para volver a formatear todos los volúmenes de almacenamiento desmontados.

- a. Ejecuta el script: `sn-remount-volumes`

Es posible que este script tarde horas en ejecutarse en volúmenes de almacenamiento que contengan datos.

- b. A medida que se ejecuta el script, revisa la salida y responde a cualquier mensaje.



Si lo necesitas, puedes usar el comando `tail -f` para supervisar el contenido del archivo de registro del script (`/var/local/log/sn-remount-volumes.log`). El archivo de registro contiene información más detallada que 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 resultado, un volumen de almacenamiento se volvió a montar correctamente y tres volúmenes de almacenamiento presentaron errores.

- `/dev/sdb` superó la comprobación de coherencia del sistema de archivos XFS y presentaba una estructura de volumen válida, por lo que se volvió a montar correctamente. Los datos de los dispositivos que el script vuelve a montar se conservan.
- `/dev/sdc` La comprobación de coherencia del sistema de archivos XFS falló porque el volumen de almacenamiento era nuevo o estaba dañado.
- `/dev/sdd` No se ha podido montar porque el disco no estaba inicializado o el superbloque del disco estaba dañado. Cuando el script no puede montar un volumen de almacenamiento, te pregunta si deseas ejecutar la comprobación de coherencia del sistema de archivos.
 - Si el volumen de almacenamiento está conectado a un disco nuevo, responde **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 ya existente, responde **Y** a la pregunta. Puedes 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` superó la comprobación de coherencia 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 Storage Node (el `configured LDR noid` que aparece en la parte superior). Este mensaje indica que este volumen pertenece a otro Storage Node.

3. Revisa el resultado del script y resuelve cualquier problema.



Si un volumen de almacenamiento no ha superado la comprobación de coherencia del sistema de archivos XFS o no se ha podido montar, revisa detenidamente los mensajes de error que aparecen en la salida. Debes comprender las implicaciones de ejecutar el `sn-recovery-postinstall.sh` script en estos volúmenes.

- Comprueba que los resultados incluyan una entrada para todos los volúmenes que esperabas. Si falta algún volumen en la lista, vuelve a ejecutar el script.
- Revisa los mensajes de todos los dispositivos montados. Asegúrate de que no haya errores que indiquen que un volumen de almacenamiento no pertenece a este Storage Node.

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 indica que un volumen de almacenamiento pertenece a otro Storage Node, ponte en contacto con soporte técnico. Si ejecutas el `sn-recovery-postinstall.sh` script, el volumen de almacenamiento se reformateará, lo que podría provocar la pérdida de datos.

- Si no se ha podido montar algún dispositivo de almacenamiento, anota el nombre del dispositivo y repáralo o reemplázalo.



Debes reparar o sustituir cualquier dispositivo de almacenamiento que no se haya podido montar.

Utilizarás el nombre del dispositivo para buscar el ID del volumen, que es un dato obligatorio cuando

ejecutes el script `repair-data` para restaurar los datos de objetos en el volumen (el siguiente procedimiento).

- d. Después de reparar o reemplazar todos los dispositivos que no se pueden montar, ejecuta de nuevo el script `sn-remount-volumes` para confirmar que todos los volúmenes de almacenamiento que se pueden volver a montar han sido montados nuevamente.



Si no se puede montar un volumen de almacenamiento o está formateado incorrectamente, y continúas con el siguiente paso, el volumen y cualquier dato en el volumen se eliminarán. Si tenías dos copias de los datos de objetos, solo tendrás una copia hasta que completes el siguiente procedimiento (restaurar los datos de objetos).



No ejecutes el script `sn-recovery-postinstall.sh` si crees que los datos que quedan en un volumen de almacenamiento con fallo no se pueden reconstruir desde otra parte de la grid (por ejemplo, si tu política de ILM usa una regla que solo hace una copia o si los volúmenes han fallado en varios nodos). En su lugar, contacta al soporte técnico para ver cómo recuperar tus datos.

4. Ejecuta el `sn-recovery-postinstall.sh` script: `sn-recovery-postinstall.sh`

Este script reformatea cualquier volumen de almacenamiento que no se haya podido montar o que se haya detectado que está formateado incorrectamente; reconstruye la base de datos de Cassandra en el nodo, si es necesario; e inicia los servicios en el nodo de almacenamiento.

Ten en cuenta lo siguiente:

- Es posible que el script tarde horas en ejecutarse.
- En general, deberías dejar la sesión SSH sin tocar mientras el script está en ejecución.
- No pulses **Ctrl+C** mientras la sesión SSH esté activa.
- El script se ejecutará en segundo plano si se produce una interrupción de la red y se interrumpe la sesión SSH, pero puedes ver el progreso desde la página de recuperación.
- Si el nodo de almacenamiento utiliza el servicio RSM, puede parecer que el script se queda bloqueado durante 5 minutos mientras se reinician los servicios del nodo. Este retraso de 5 minutos es normal 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 gestionar las reparaciones de Cassandra. Las reparaciones se llevan a cabo automáticamente en cuanto se han iniciado los servicios relacionados o necesarios. Es posible que veas en la salida del script menciones a "reaper" o "reparación de Cassandra". Si aparece un mensaje de error que indica que la reparación ha fallado, ejecuta el comando que se indica en dicho mensaje.

5. Mientras se ejecuta el `sn-recovery-postinstall.sh` script, supervisa la página de Recuperación en el Grid Manager.

La barra de progreso y la columna «Etapa» de la página «Recuperación» ofrecen a grandes rasgos el estado del `sn-recovery-postinstall.sh` script.

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 que el `sn-recovery-postinstall.sh` script haya iniciado los servicios en el nodo, puedes restaurar los datos de objetos en cualquier volumen de almacenamiento que haya formateado el script.

El script te pregunta si deseas utilizar el proceso de restauración de volúmenes de Grid Manager.

- En la mayoría de los casos, debes ["restaura datos de objetos usando Grid Manager"](#). Responde `y` para usar Grid Manager.
- En casos poco comunes, como cuando te lo indique el soporte técnico o cuando sepas que el nodo de reemplazo tiene menos volúmenes disponibles para el almacenamiento de objetos que el nodo original, debes ["restaurar los datos del objeto manualmente"](#) usando el script `repair-data`. Si se aplica alguno de estos casos, responde `n`.



Si respondes `n` al usar el proceso de restauración de volúmenes de Grid Manager (restaurar los datos de objetos manualmente):

- No puedes restaurar datos de objetos usando Grid Manager.
- Puedes supervisar el progreso de las tareas de restauración manual mediante Grid Manager.

Una vez realizada la selección, el script finaliza y se muestran los siguientes pasos para recuperar los datos del objeto. Tras revisar estos pasos, pulsa cualquier tecla para volver a la línea de comandos.

Restaura los datos de objetos en el volumen de almacenamiento de StorageGRID (fallo de unidad del sistema)

Tras recuperar los volúmenes de almacenamiento de un nodo de almacenamiento que no sea un dispositivo, puedes restaurar los datos de los objetos replicados o con código de borrado que se perdieron cuando el nodo de almacenamiento falló.

¿Qué procedimiento debo seguir?

Siempre que sea posible, restaura los datos de los objetos mediante la página **Restauración de volúmenes** en el Grid Manager.

- Si los volúmenes aparecen en **Mantenimiento > Restauración de volúmenes > Nodos para restaurar**, restaura los datos de objetos mediante ["Página de restauración de volumen en el Grid Manager"](#).
- Si los volúmenes no aparecen en **Mantenimiento > Restauración de volúmenes > Nodos para restaurar**, sigue los pasos que se indican a continuación para usar el script `repair-data` para restaurar datos de objetos.

Si el nodo de almacenamiento recuperado contiene menos volúmenes que el nodo al que sustituye, debes usar el script `repair-data`.



El script `repair-data` está obsoleto y se eliminará en una futura versión. Cuando sea posible, utiliza el ["Procedimiento de restauración del volumen en el Grid Manager"](#).

Utiliza el script `repair-data` para restaurar los datos de los objetos

Antes de empezar

- Has comprobado que el nodo de almacenamiento recuperado presenta un estado de conexión

Conectado  en la pestaña **Nodos > Resumen** del Grid Manager.

Acerca de esta tarea

Los datos de los objetos se pueden restaurar desde otros Storage Nodes o desde un Cloud Storage Pool, siempre que las reglas de ILM de la grid se hayan configurado de tal forma que haya copias de los objetos disponibles.

Ten en cuenta lo siguiente:

- Si se ha configurado una regla de ILM para almacenar únicamente una copia replicada y dicha copia se encontraba en un volumen de almacenamiento que ha fallado, no podrás recuperar el objeto.
- Si la única copia restante de un objeto se encuentra en un Cloud Storage Pool, StorageGRID debe enviar varias solicitudes al endpoint del Cloud Storage Pool para restaurar los datos del objeto. Antes de realizar este procedimiento, ponte en contacto con soporte técnico para que te ayuden a estimar el plazo de recuperación y los costes asociados.

Acerca del `repair-data` script

Para restaurar los datos de objetos, ejecutas el script `repair-data`. Este script inicia el proceso de restauración de datos de objetos y funciona con el escaneo de ILM para garantizar que se cumplan las reglas de ILM.

Selecciona **Datos replicados** o **Datos con código de borrado (EC)** a continuación para conocer las diferentes opciones del `repair-data` script, en función de si vas a restaurar datos replicados o datos con código de borrado. Si necesitas restaurar ambos tipos de datos, debes ejecutar ambos conjuntos de comandos.



Para obtener más información sobre el script `repair-data`, introduce `repair-data --help` desde la línea de comandos del nodo de administración primario.



El script `repair-data` está obsoleto y se eliminará en una futura versión. Cuando sea posible, utiliza el ["Procedimiento de restauración del volumen en el Grid Manager"](#).

Datos replicados

Hay dos comandos disponibles para restaurar datos replicados, dependiendo de si necesitas reparar todo el nodo o solo ciertos volúmenes en el nodo:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

Puedes realizar un seguimiento de las reparaciones de los datos replicados con este comando:

```
repair-data show-replicated-repair-status
```

Datos con código de borrado (EC)

Hay dos comandos disponibles para la restauración de datos con código de borrado, dependiendo de si necesitas reparar todo el nodo o solo determinados volúmenes del mismo:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Puedes realizar un seguimiento de las reparaciones de los datos con código de borrado con este comando:

```
repair-data show-ec-repair-status
```



Las reparaciones de datos con codificación de borrado pueden comenzar mientras algunos nodos de almacenamiento están sin conexión. Sin embargo, si no se pueden localizar todos los datos con codificación de borrado, la reparación no se podrá completar. La reparación se completará una vez que todos los nodos estén disponibles.



La tarea de reparación de EC reserva temporalmente una gran cantidad de almacenamiento. Es posible que se activen alertas de almacenamiento, pero se resolverán cuando finalice la reparación. Si no hay suficiente almacenamiento para la reserva, la tarea de reparación de EC fallará. Las reservas de almacenamiento se liberan cuando finaliza la tarea de reparación de EC, ya sea que la tarea haya fallado o tenido éxito.

Buscar el nombre de host para el nodo de almacenamiento

1. Inicia sesión en cualquier Admin Node:

- Introduce el siguiente comando: `ssh admin@primary_Admin_Node_IP`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.
- Introduce el siguiente comando para pasar a ser usuario root: `su -`
- Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Usa el archivo `/etc/hosts` para buscar el nombre de host del nodo de almacenamiento para los volúmenes de almacenamiento restaurados. Para ver una lista de todos los nodos del grid, introduce lo

siguiente: `cat /etc/hosts`.

Repara los datos si todos los volúmenes han fallado

Si todos los volúmenes de almacenamiento han fallado, repara todo el nodo. Sigue las instrucciones para **datos replicados**, **datos con codificación de borrado (EC)** o ambos, según si usas datos replicados, datos con codificación de borrado (EC) o ambos.

Si solo se han dañado algunos volúmenes, ve a [Repara los datos si solo han fallado algunos volúmenes](#).



No puedes ejecutar operaciones de `repair-data` en más de un nodo al mismo tiempo. Para recuperar varios nodos, ponte en contacto con soporte técnico.

Datos replicados

Si tu grid incluye datos replicados, usa el comando `repair-data start-replicated-node-repair` con la opción `--nodes`, donde `--nodes` es el nombre de host (nombre del sistema), para reparar todo el Storage Node.

Este comando repara los datos replicados en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```



A medida que se restauran los datos 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. Debes determinar la causa de la pérdida y si la recuperación es posible. Consulta "[Investiga los objetos que puedan haberse perdido](#)".

Datos con código de borrado (EC)

Si tu grid contiene datos con código de borrado, usa el comando `repair-data start-ec-node-repair` con la opción `--nodes`, donde `--nodes` es el hostname (nombre del sistema), para reparar todo el Storage Node.

Este comando repara los datos con código de borrado en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

La operación devuelve un identificador único `repair ID` que identifica esta `repair_data` operación. Usa este `repair ID` para seguir el progreso y el resultado de la `repair_data` operación. No se devuelve ningún otro comentario cuando finaliza el proceso de recuperación.

Las reparaciones de los datos con código de borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. La reparación se completará cuando todos los nodos estén disponibles.

Repara los datos si solo han fallado algunos volúmenes

Si solo algunos de los volúmenes han fallado, repara los volúmenes afectados. Sigue las instrucciones para **datos replicados**, **datos con código de borrado (EC)** o ambos, en función de si utilizas datos replicados, datos con código de borrado (EC) o ambos.

Si todos los volúmenes han fallado, ve a [Repara los datos si todos los volúmenes han fallado](#).

Introduce los ID de los volúmenes en formato hexadecimal. Por ejemplo, 0000 es el primer volumen y 000F es el decimosexto volumen. Puedes especificar un volumen, un rango de volúmenes o varios volúmenes que no estén en secuencia.

Todos los volúmenes deben estar en el mismo Storage Node. Si necesitas restaurar volúmenes de más de un Storage Node, ponte en contacto con el soporte técnico.

Datos replicados

Si tu grid contiene datos replicados, usa el comando `start-replicated-volume-repair` con la opción `--nodes` para identificar el nodo (donde `--nodes` es el nombre de host del nodo). Luego añade la opción `--volumes` o `--volume-range`, como se muestra en los siguientes ejemplos.

Un solo volumen: Este comando restaura los datos replicados en el volumen 0002 en un nodo de almacenamiento denominado 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 al 0009 en un Storage Node llamado SG-DC-SN3:

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range 0003,0009
```

Varios volúmenes no secuenciales: Este comando restaura los datos replicados en los volúmenes 0001, 0005 y 0008 en un Storage Node 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 objetos, se activa la alerta **Objects Lost** si el sistema StorageGRID no puede localizar los datos de objetos replicados. Es posible que se activen alertas en los nodos de almacenamiento de todo el sistema. Toma nota de la descripción de la alerta y de las acciones recomendadas para determinar la causa de la pérdida y si la recuperación es posible.

Datos con código de borrado (EC)

Si tu grid contiene datos con código de borrado, utiliza el comando `start-ec-volume-repair` con la opción `--nodes` para identificar el nodo (donde `--nodes` es el hostname del nodo). Luego añade la opción `--volumes` o `--volume-range`, como se muestra en los siguientes ejemplos.

Volumen único: este comando restaura datos con codificación de borrado en el volumen 0007 de un Storage Node llamado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Rango de volúmenes: Este comando restaura los datos con código de borrado en todos los volúmenes comprendidos entre 0004 y 0006 en un nodo de almacenamiento denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Varios volúmenes no consecutivos: Este comando restaura datos con código de borrado en los volúmenes 000A, 000C y 000E de un Storage Node denominado SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

La `repair-data` operación devuelve un `repair ID` único que identifica esta `repair_data` operación. Usa este `repair ID` para seguir el progreso y el resultado de la `repair_data` operación. No se devuelve ningún otro comentario cuando finaliza el proceso de recuperación.



Las reparaciones de los datos con código de borrado pueden comenzar mientras algunos nodos de almacenamiento están fuera de línea. La reparación se completará cuando todos los nodos estén disponibles.

Supervisar reparaciones

Supervisa el estado de los trabajos de reparación, dependiendo de si utilizas **datos replicados**, **datos con código de borrado (EC)** o ambos.

También puedes supervisar el estado de las tareas de restauración de volúmenes en curso y consultar el historial de las tareas de restauración completadas en ["Grid Manager"](#).

Datos replicados

- Para obtener un porcentaje estimado de finalización de la reparación replicada, añade la opción `show-replicated-repair-status` al comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Para comprobar si las reparaciones se han completado:
 - a. Selecciona **Nodos > Nodo de almacenamiento en reparación > ILM**.
 - b. Revisa los atributos en la sección de evaluación. Cuando se completen las reparaciones, el atributo **Awaiting - All** indica 0 objetos.
- Para monitorear la reparación con más detalle:
 - a. Selecciona **Nodos**.
 - b. Selecciona **nombre de la cuadrícula > ILM**.
 - c. Coloca el cursor sobre el gráfico de la cola de ILM para ver el valor del atributo **Frecuencia de escaneo (objetos/seg)**, que es la velocidad a la que se escanean los objetos en el grid y se colocan en la cola de ILM.
 - d. En la sección Cola de ILM, fíjate en los siguientes atributos:
 - **Duración del escaneo - estimada:** El tiempo estimado para completar un escaneo ILM completo de todos los objetos.

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

- **Reparaciones intentadas:** el número total de operaciones de reparación de objetos intentadas para datos replicados que se consideran de alto riesgo. Los objetos de alto riesgo son aquellos a los que les queda una sola copia, ya sea porque así lo especifica la política de ILM o como resultado de la pérdida de copias. Este recuento se incrementa cada vez que un Storage Node intenta reparar un objeto de alto riesgo. Las reparaciones de ILM de alto riesgo se priorizan si el grid se ocupa.

La misma reparación de objetos podría volver a incrementarse si la replicación falló después de la reparación. + Estos atributos pueden ser útiles cuando estés monitorizando el progreso de la recuperación de volúmenes del Storage Node. Si el número de intentos de reparación ha dejado de aumentar y se ha completado un escaneo completo, es probable que la reparación haya finalizado.

- e. Como alternativa, envía una consulta de Prometheus para `storagegrid_ilm_scan_period_estimated_minutes` y `storagegrid_ilm_repairs_attempted`.

Datos con código de borrado (EC)

Para supervisar la reparación de los datos con código de borrado y volver a intentar cualquier solicitud que haya podido fallar:

1. Determina el estado de las reparaciones de los datos con código de borrado:
 - Selecciona **Support > Tools > Metrics** para ver el tiempo estimado hasta la finalización y el porcentaje de finalización del trabajo actual. Luego, selecciona **EC Overview** en la sección de Grafana. Consulta los paneles **Grid EC Job Estimated Time to Completion** y **Grid EC Job Percentage Completed**.

- Usa este comando para ver el estado de una operación `repair-data` específica:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Utiliza este comando para listar todas las reparaciones:

```
repair-data show-ec-repair-status
```

El resultado muestra información, incluida `repair ID`, sobre todas las reparaciones que se han realizado anteriormente y las que se están llevando a cabo actualmente.

2. Si el resultado indica que la operación de reparación ha fallado, utiliza la opción `--repair-id` para volver a intentar la reparación.

Este comando vuelve a intentar la reparación de un nodo que ha fallado, usando el ID de reparación 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando vuelve a intentar una reparación de volumen que ha fallado, usando el ID de reparación 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Verifica el estado del almacenamiento después de recuperar una unidad del sistema StorageGRID Storage Node

Tras recuperar la unidad del sistema de un nodo de almacenamiento, debes comprobar que el estado deseado del nodo de almacenamiento esté configurado como «en línea» y asegurarte de que dicho estado sea «en línea» de forma predeterminada cada vez que se reinicie el servidor del nodo de almacenamiento.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- El nodo de almacenamiento se ha recuperado y la recuperación de datos ha finalizado.

Pasos

1. Selecciona **Nodos > Storage Node > Tareas**.
2. Si la lista desplegable **Estado de almacenamiento** está configurada en **Solo lectura** o **Sin conexión**, selecciona **En línea**.
3. Selecciona **Guardar**.

Restaura datos de objetos usando StorageGRID Grid Manager

Puedes restaurar los datos de objetos de un volumen de almacenamiento o un Storage Node que haya fallado usando Grid Manager. También puedes usar Grid Manager para monitorear los procesos de restauración en curso y mostrar un historial de restauración.

Antes de empezar

- Has completado uno de estos procedimientos para formatear los volúmenes defectuosos:
 - ["Volver a montar y formatear los volúmenes de almacenamiento del appliance \(pasos manuales\)"](#)
 - ["Volver a montar y reformatear los volúmenes de almacenamiento \(pasos manuales\)"](#)
- Has comprobado que el nodo de almacenamiento en el que estás restaurando los objetos presenta un estado de conexión **Conectado**  en la pestaña **Nodos > Resumen** del Grid Manager.
- Has confirmado lo siguiente:
 - No se está llevando a cabo una ampliación de grid para añadir un nodo de almacenamiento.
 - No se está llevando a cabo ni ha fallado el decomisionamiento de un nodo de almacenamiento.
 - No se está llevando a cabo ninguna recuperación de un volumen de almacenamiento que haya fallado.
 - No se está llevando a cabo la recuperación de un nodo de almacenamiento de StorageGRID con una unidad del sistema fallida.
 - No hay ninguna tarea de reequilibrio de EC en curso.
 - La clonación del nodo del dispositivo no está en proceso.

Acerca de esta tarea

Una vez que hayas sustituido las unidades y hayas seguido los pasos manuales para formatear los volúmenes, Grid Manager mostrará dichos volúmenes como candidatos para la restauración en la pestaña **Mantenimiento > Restauración de volúmenes > Nodos que restaurar**.

Siempre que sea posible, restaura los datos de objetos usando la página de restauración de volúmenes en Grid Manager. Puedes [activar el modo de restauración automática](#) para iniciar automáticamente la restauración de volúmenes cuando estén listos para restaurarse o [restaurar el volumen manualmente](#). Sigue estas directrices:

- Si los volúmenes aparecen en **Mantenimiento > Restauración de volúmenes > Nodos que restaurar**, restaura los datos de los objetos tal y como se describe en los pasos siguientes. Los volúmenes aparecerán en la lista si:
 - Algunos, pero no todos, los volúmenes de almacenamiento de un nodo han fallado
 - Todos los volúmenes de almacenamiento de un nodo han fallado y se están sustituyendo por el mismo número de volúmenes o por más volúmenes

La página «Restauración de volúmenes» del Grid Manager también te permite [supervisar el proceso de restauración del volumen](#) y [ver el historial de restauraciones](#).

- Si los volúmenes no aparecen en el Grid Manager como candidatos para restauración, sigue los pasos correspondientes para usar el script `repair-data` para restaurar los datos de objetos:
 - ["Restaurar los datos de los objetos en el volumen de almacenamiento \(fallo de unidad del sistema\)"](#)
 - ["Restaura los datos de los objetos en el volumen de almacenamiento donde la unidad del sistema está intacta"](#)
 - ["Restaura los datos de objetos en el volumen de almacenamiento del dispositivo"](#)



El script «repair-data» está obsoleto y se eliminará en una futura versión.

Si el nodo de almacenamiento recuperado contiene menos volúmenes que el nodo al que sustituye, debes usar el script `repair-data`.

Puedes restaurar dos tipos de datos de objetos:

- Los objetos de datos replicados se restauran desde otras ubicaciones, siempre que las reglas de ILM de la grid se hayan configurado para que las copias de los objetos estén disponibles.
 - Si se ha configurado una regla de ILM para almacenar únicamente una copia replicada y dicha copia se encontraba en un volumen de almacenamiento que ha fallado, no podrás recuperar el objeto.
 - Si la única copia restante de un objeto se encuentra en un Cloud Storage Pool, StorageGRID debe enviar varias solicitudes al endpoint del Cloud Storage Pool para restaurar los datos del objeto.
- Los objetos de datos con código de borrado (EC) se restauran reensamblando los fragmentos almacenados. Los fragmentos dañados o perdidos se recrean mediante el algoritmo de código de borrado a partir de los datos restantes y los fragmentos de paridad.

La reparación de los datos con código de borrado puede comenzar aunque algunos nodos de almacenamiento estén fuera de línea. Sin embargo, si no se pueden localizar todos los datos con código de borrado, la reparación no puede completarse. La reparación se completará cuando todos los nodos estén disponibles.



La restauración del volumen depende de la disponibilidad de los recursos en los que se almacenan las copias de los objetos. El progreso de la restauración del volumen no es lineal y puede tardar días o semanas en completarse.

Activar el modo de restauración automática

Al activar el modo de restauración automática, la restauración de los volúmenes se inicia automáticamente cuando estos están listos para ser restaurados.

Pasos

1. En Grid Manager, ve a **Mantenimiento > Restauración de volumen**.
2. Selecciona la pestaña **Nodos que se van a restaurar** y luego desliza el interruptor de **Modo de restauración automática** hasta la posición activada.
3. Cuando aparezca el cuadro de diálogo de confirmación, revisa los detalles.



- No podrás iniciar manualmente tareas de restauración de volúmenes en ningún nodo.
- Las restauraciones de volumen se iniciarán automáticamente solo cuando no haya ningún otro procedimiento de mantenimiento en curso.
- Puedes consultar el estado del trabajo en la página de seguimiento del progreso.
- StorageGRID vuelve a intentar automáticamente las restauraciones de volúmenes que no se inician.

4. Cuando comprendas los resultados de activar el modo de restauración automática, selecciona **Sí** en el cuadro de diálogo de confirmación.

Puedes desactivar el modo de restauración automática en cualquier momento.

Restaurar manualmente un volumen o nodo que falló

Sigue estos pasos para restaurar un volumen o nodo que haya fallado.

Pasos

1. En Grid Manager, ve a **Mantenimiento > Restauración de volumen**.
2. Selecciona la pestaña **Nodos que se van a restaurar** y luego desliza el interruptor de **Modo de restauración automática** hasta la posición desactivada.

El número que aparece en la pestaña indica el número de nodos con volúmenes que requieren restauración.

3. Despliega cada nodo para ver los volúmenes que necesitan restauración y su estado.
4. Corrige cualquier problema que impida la restauración de cada volumen. Los problemas se indicarán cuando selecciones **A la espera de pasos manuales**, si ese es el estado que aparece para el volumen.
5. Selecciona un nodo para restaurar donde todos los volúmenes indiquen el 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. Selecciona **Iniciar restauración**.
7. Resuelve cualquier advertencia que pueda aparecer o selecciona **Iniciar de todos modos** para ignorar las advertencias e iniciar la restauración.

Los nodos pasan de la pestaña **Nodos que se van a restaurar** a la pestaña **Progreso de la restauración** cuando comienza la restauración.

Si no es posible iniciar la restauración de un volumen, el nodo vuelve a la pestaña **Nodos que restaurar**.

Ver el progreso de la restauración

La pestaña **Progreso de la restauración** muestra el estado del proceso de restauración de volúmenes e información sobre los volúmenes de un nodo que se está restaurando.

Las tasas de reparación de datos para los objetos replicados y con código de borrado en todos los volúmenes son medias que resumen todas las restauraciones en curso, incluidas aquellas restauraciones iniciadas mediante el `repair-data` script. 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 los recursos en los que 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 «Tareas de restauración» muestra información sobre las restauraciones de volúmenes iniciadas desde Grid Manager.

- El número que aparece en el encabezado de la sección de tareas de restauración indica la cantidad de volúmenes que se están restaurando o que están en cola para 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 correspondiente a cada trabajo.
 - Despliega la columna «Detalles» para ver la hora de inicio de la restauración y el ID del trabajo.
- Si falla una restauración de volumen:
 - La columna Estado indica `failed (attempting retry)`, y se volverá a intentar automáticamente.

- Si han fallado varias tareas de restauración, primero se volverá a intentar automáticamente la tarea más reciente.
- La alerta **«Error de reparación de EC»** se activa si los reintentos siguen fallando. Sigue los pasos que se indican en la alerta para resolver el problema.

Ver historial de restauraciones

La pestaña **Historial de restauraciones** muestra información sobre todas las restauraciones de volúmenes que se han completado con éxito.



Los tamaños no son aplicables a los objetos replicados y solo aparecen en las restauraciones que contienen objetos de datos con código de borrado (EC).

Supervisa los trabajos de reparación de StorageGRID

Puedes supervisar el estado de los trabajos de reparación utilizando el script `repair-data` desde la línea de comandos.

Entre ellos se incluyen los trabajos que iniciaste manualmente o los que StorageGRID inició automáticamente como parte de un procedimiento de decomisionar.



Si estás ejecutando tareas de restauración de volúmenes, utiliza ["supervisar el progreso y consultar el historial de esos trabajos en el Grid Manager"](#) en su lugar.

Supervisa el estado de los trabajos de `repair-data` según si usas **datos replicados**, **datos con código de borrado (EC)** o ambos.

Datos replicados

- Para obtener un porcentaje estimado de finalización de la reparación replicada, añade la opción `show-replicated-repair-status` al comando `repair-data`.

```
repair-data show-replicated-repair-status
```

- Para comprobar si las reparaciones se han completado:
 - a. Selecciona **Nodos > Nodo de almacenamiento en reparación > ILM**.
 - b. Revisa los atributos en la sección de evaluación. Cuando se completen las reparaciones, el atributo **Awaiting - All** indica 0 objetos.
- Para monitorear la reparación con más detalle:
 - a. Selecciona **Nodos**.
 - b. Selecciona **nombre de la cuadrícula > ILM**.
 - c. Coloca el cursor sobre el gráfico de la cola de ILM para ver el valor del atributo **Frecuencia de escaneo (objetos/seg)**, que es la velocidad a la que se escanean los objetos en el grid y se colocan en la cola de ILM.
 - d. En la sección Cola de ILM, fíjate en los siguientes atributos:
 - **Duración del escaneo - estimada:** El tiempo estimado para completar un escaneo ILM completo de todos los objetos.

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

- **Reparaciones intentadas:** el número total de operaciones de reparación de objetos intentadas para datos replicados que se consideran de alto riesgo. Los objetos de alto riesgo son aquellos a los que les queda una sola copia, ya sea porque así lo especifica la política de ILM o como resultado de la pérdida de copias. Este recuento se incrementa cada vez que un Storage Node intenta reparar un objeto de alto riesgo. Las reparaciones de ILM de alto riesgo se priorizan si el grid se ocupa.

La misma reparación de objetos podría volver a incrementarse si la replicación falló después de la reparación. + Estos atributos pueden ser útiles cuando estés monitorizando el progreso de la recuperación de volúmenes del Storage Node. Si el número de intentos de reparación ha dejado de aumentar y se ha completado un escaneo completo, es probable que la reparación haya finalizado.

- e. Como alternativa, envía una consulta de Prometheus para `storagegrid_ilm_scan_period_estimated_minutes` y `storagegrid_ilm_repairs_attempted`.

Datos con código de borrado (EC)

Para supervisar la reparación de los datos con código de borrado y volver a intentar cualquier solicitud que haya podido fallar:

1. Determina el estado de las reparaciones de los datos con código de borrado:
 - Selecciona **Support > Tools > Metrics** para ver el tiempo estimado hasta la finalización y el porcentaje de finalización del trabajo actual. Luego, selecciona **EC Overview** en la sección de Grafana. Consulta los paneles **Grid EC Job Estimated Time to Completion** y **Grid EC Job Percentage Completed**.

- Usa este comando para ver el estado de una operación `repair-data` específica:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Utiliza este comando para listar todas las reparaciones:

```
repair-data show-ec-repair-status
```

El resultado muestra información, incluida `repair ID`, sobre todas las reparaciones que se han realizado anteriormente y las que se están llevando a cabo actualmente.

2. Si el resultado indica que la operación de reparación ha fallado, utiliza la opción `--repair-id` para volver a intentar la reparación.

Este comando vuelve a intentar la reparación de un nodo que ha fallado, usando el ID de reparación 6949309319275667690:

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Este comando vuelve a intentar una reparación de volumen que ha fallado, usando el ID de reparación 6949309319275667690:

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Recupérate de fallos del nodo de administración

Recuperación del nodo de administración primario o no primario en StorageGRID

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.

A grandes rasgos, los pasos para recuperar un nodo de administración principal o no principal son los mismos, aunque los detalles de los pasos difieren.

Sigue siempre el procedimiento de recuperación adecuado para el nodo de administración que estés recuperando. Los procedimientos son similares a grandes rasgos, pero difieren en los detalles.

Opciones

- ["Recupérate de fallos del nodo de administración principal"](#)
- ["Recupérate de fallos del nodo de administración no principal"](#)

Recupérate de fallos del nodo de administración principal

Recupera de fallos del nodo primario de administración de StorageGRID

Debes realizar una serie de tareas específicas para recuperarte de un fallo del nodo de administración principal. El nodo de administración principal aloja el servicio Configuration Management Node (CMN) para el grid.



Debes reparar o sustituir sin demora un nodo de administración principal que haya fallado o podrías no poder realizar ciertos procedimientos de mantenimiento.

Sigue estos pasos a grandes rasgos para recuperar un nodo de administración principal:

1. "Copiar los registros de auditoría del nodo de administración principal que ha fallado"
2. "Sustituir el nodo de administración principal"
3. "Configura el nodo de administración principal de sustitución"
4. "Determina si hay un requisito de corrección urgente para el nodo de administración principal recuperado"
5. "Restaura el registro de auditoría en el nodo de administración principal recuperado"
6. "Restaura la base de datos del nodo de administración cuando recuperas un nodo de administración principal"
7. "Restaurar las métricas de Prometheus al recuperar un nodo de administración principal"

Copia los registros de auditoría de un nodo de administración StorageGRID primario fallido

Si puedes copiar los registros de auditoría del nodo de administración principal que ha fallado, debes conservarlos para mantener el historial de la grid sobre la actividad y el uso del sistema. Puedes restaurar los registros de auditoría conservados en el nodo de administración principal recuperado una vez que esté en funcionamiento.

Acerca de esta tarea

Este procedimiento copia los archivos de auditoría del nodo de administración que ha fallado a una ubicación temporal en un nodo de grid independiente. Luego, estos registros de auditoría conservados pueden copiarse al nodo de administración de reemplazo. Los registros de auditoría no se copian automáticamente al nuevo nodo de administración.

Dependiendo del tipo de fallo, es posible que no puedas copiar los registros de auditoría de un nodo de administración que haya fallado. Si la implementación solo cuenta con 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 anteriormente. Si la implementación incluye más de un nodo de administración, puedes recuperar los registros de auditoría desde otro nodo de administración.



Si ahora no se puede acceder a los registros de auditoría en el nodo de administración que ha fallado, es posible que puedas acceder a ellos más adelante, por ejemplo, tras la recuperación del host.

Pasos

1. Inicia sesión en el nodo de administración principal que ha fallado, si es posible. De lo contrario, inicia sesión en cualquier nodo de administración disponible.
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Detén el servicio AMS para evitar que cree un nuevo archivo de registro: `service ams stop`

3. Accede al directorio de exportación de auditorías:

```
cd /var/local/audit/export
```

(o `cd /var/local/log` en sistemas anteriores)

4. Cambia el nombre del archivo de registro de origen por un nombre de archivo con un número único.



- Si el archivo de registro está en el directorio `/var/local/audit/export`, su nombre es `audit.log`.
- Si el archivo de registro está en el directorio `/var/local/log`, su nombre es `localaudit.log`.

Por ejemplo, cambia el nombre del archivo `localaudit.log` a `2025-10-22.txt.1`.

```
ls -l
mv localaudit.log 2025-10-22.txt.1
```

5. Reinicia el servicio AMS: `service ams start`

6. Crea el directorio para copiar todos los archivos de auditoría a una ubicación temporal en un nodo independiente de la grid: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Cuando se te solicite, introduce la contraseña de admin.

7. Copia todos los archivos de auditoría en la ubicación temporal: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Cuando se te solicite, introduce la contraseña de admin.

8. Cerrar sesión como root: `exit`

Sustituir el nodo primario de administración de StorageGRID

Para recuperar un nodo de administración principal, primero debes sustituir el hardware físico o virtual.

Puedes sustituir un nodo de administración principal que haya fallado por otro nodo de administración principal que se ejecute en la misma plataforma, o bien sustituir un nodo de administración principal que se ejecute en un host VMware o Linux por un nodo de administración principal alojado en un dispositivo de servicios.

Sigue el procedimiento correspondiente a la plataforma de sustitución que elijas para el nodo. Una vez completado el procedimiento de sustitución del nodo (apto para todos los tipos de nodos), dicho procedimiento te indicará el siguiente paso para la recuperación del nodo de administración principal.

Plataforma de sustitución	Procedimiento
VMware	"Sustituir un nodo de VMware"
Linux	"Sustituir un nodo de Linux"
Dispositivos de servicios	"Sustituir 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 necesitas recuperar un nodo que se ejecuta en una implementación de OpenStack, descarga los archivos para tu sistema operativo Linux. Luego, sigue el procedimiento para "Reemplazar un nodo Linux" .

Configura un nodo de administración primario de reemplazo en StorageGRID

El nodo de sustitución debe configurarse como nodo de administración principal para tu sistema StorageGRID.

Antes de empezar

- Para los nodos de administración primarios alojados en máquinas virtuales, la máquina virtual ya fue implementada, encendida e inicializada.
- En el caso de los nodos de administración principales alojados en un dispositivo de servicios, has sustituido el dispositivo y has instalado el software. Consulta el ["Instrucciones de instalación de tu appliance"](#).
- Tienes la última copia de seguridad del archivo del paquete de recuperación (`sgws-recovery-package-id-revision.zip`).
- Tienes la frase de contraseña de aprovisionamiento.

Pasos

1. Abre tu navegador web y ve a `https://primary_admin_node_ip`.
2. Gestiona una contraseña temporal de instalador según sea necesario:
 - Si ya se ha establecido una contraseña mediante uno de estos métodos, introduce la contraseña para continuar.
 - Un usuario estableció la contraseña al acceder al instalador anteriormente
 - Para los sistemas bare metal, 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 del OVF
 - Si no se ha establecido una contraseña, opcionalmente establece una para proteger el instalador de StorageGRID.
3. Haz clic en **Recuperar un nodo de administración principal que ha fallado**.

Install

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. Sube la copia de seguridad más reciente del paquete de recuperación:
 - a. Haz clic en **Examinar**.
 - b. Busca el archivo del paquete de recuperación más reciente para tu sistema StorageGRID y haz clic en **Abrir**.
5. Introduce la contraseña de aprovisionamiento.
6. Haz clic en **Iniciar recuperación**.

Comienza el proceso de recuperación. Es posible que el Grid Manager no esté disponible durante unos minutos mientras se inician los servicios necesarios. Cuando se completa la recuperación, se muestra la página de inicio de sesión.

7. Si el inicio de sesión único (SSO) está habilitado para tu sistema StorageGRID y la confianza de parte dependiente del nodo de administración que recuperaste se configuró para usar el certificado predeterminado de la interfaz de gestión, actualiza (o elimina y vuelve a crear) la confianza de parte dependiente del nodo en Active Directory Federation Services (AD FS). Usa el nuevo certificado de servidor predeterminado que se generó durante el proceso de recuperación del nodo de administración.



Para configurar una relación de confianza con una parte confiable, consulta "[Configura el inicio de sesión único](#)". Para acceder al certificado predeterminado del servidor, inicia sesión en el intérprete de comandos del Admin Node. Ve al directorio `/var/local/mgmt-api` y selecciona el archivo `server.crt`.



Tras recuperar un nodo de administración principal, "[Averigua si necesitas aplicar una corrección urgente](#)".

Determina el requisito de corrección urgente para el nodo de administración primario en StorageGRID

Después de recuperar un nodo de administración principal, determina si necesitas aplicar una corrección urgente.

Antes de empezar

La recuperación del nodo de administración principal está completa.

Pasos

1. Inicia sesión en Grid Manager usando una ["navegador web compatible"](#) cuenta.
2. Selecciona **Nodos**.
3. En la lista de la izquierda, selecciona el nodo de administración principal.
4. En la pestaña «Descripción general», fíjate en la versión que aparece en el campo **Versión del software**.
5. Selecciona cualquier otro nodo de la cuadrícula.
6. En la pestaña «Descripción general», fíjate en la versión que aparece en el campo **Versión del software**.
 - Si las versiones que aparecen en los campos **Versión de software** son las mismas, no necesitas aplicar una corrección urgente.
 - Si las versiones que aparecen en los campos **Versión de software** son diferentes, debes ["aplicar una corrección urgente"](#) para actualizar el nodo de administración principal recuperado a la misma versión.

Restaurar el registro de auditoría en el nodo primario StorageGRID Admin recuperado

Si has podido conservar el registro de auditoría del nodo de administración principal que ha fallado, puedes copiarlo al nodo de administración principal que estás recuperando.

Antes de empezar

- El nodo de administración recuperado está instalado y en funcionamiento.
- Has copiado los registros de auditoría a otra ubicación después de que fallara el nodo de administración original.

Acerca de esta tarea

Si un nodo de administración falla, los registros de auditoría guardados en ese nodo de administración podrían perderse. Podría ser posible evitar la pérdida de datos copiando los registros de auditoría del nodo de administración que falló y luego restaurando esos registros en el nodo de administración recuperado. Dependiendo del fallo, podría no ser posible copiar los registros de auditoría del nodo de administración que falló. En ese caso, si la implementación tiene más de un nodo de administración, puedes recuperar los registros de auditoría desde 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 es posible copiar el registro de auditoría del nodo que ha fallado, el nodo de administración recuperado comienza a registrar eventos en el registro de auditoría como si se tratara de una instalación nueva.

Debes recuperar un nodo de administración lo antes posible para restablecer la funcionalidad de registro.

De forma predeterminada, la información de auditoría se envía al registro de auditoría en los nodos de administración. Puedes omitir estos pasos si se da cualquiera de las siguientes circunstancias:



- Has configurado un servidor syslog externo y ahora los registros de auditoría se envían al servidor syslog en lugar de a los nodos de administración.
- Has especificado expresamente que los mensajes de auditoría solo deben guardarse en los nodos locales que los generaron.

Consulta "[Configura la gestión de registros y el servidor syslog externo](#)" para más detalles.

Pasos

1. Inicia sesión en el nodo de administración recuperado:

- a. Introduce el siguiente comando: `ssh admin@recovery_Admin_Node_IP`
- b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
- d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Una vez que hayas iniciado sesión como root, el indicador de comando cambia de `$` a `#`.

2. Comprueba qué archivos de auditoría se han conservado: `cd /var/local/audit/export`

3. Copia los archivos de auditoría conservados en el nodo de administración recuperado: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

Cuando se te solicite, introduce la contraseña de admin.

4. Por motivos de seguridad, elimina los registros de auditoría del nodo de grid que ha fallado después de verificar que se han copiado correctamente al Admin Node recuperado.
5. Actualiza la configuración de usuarios y grupos de los archivos de auditoría en el nodo de administración recuperado: `chown ams-user:broadcast *`
6. Cerrar sesión como root: `exit`

Restaurar la base de datos del nodo de administración StorageGRID al recuperar el nodo de administración primario

Si deseas conservar la información histórica sobre los atributos y las alertas de un nodo de administración principal que ha fallado, puedes restaurar la base de datos del nodo de administración. Solo puedes restaurar esta base de datos si tu sistema StorageGRID incluye otro nodo de administración.

Antes de empezar

- El nodo de administración recuperado está instalado y en funcionamiento.
- El sistema StorageGRID incluye al menos dos nodos de administración.
- Tienes el archivo `Passwords.txt`.
- Tienes la frase de contraseña de aprovisionamiento.

Acerca de esta tarea

Si un nodo de administración falla, se pierde la información histórica almacenada en su base de datos de nodo de administración. Esta base de datos incluye la siguiente información:

- Historial de alertas
- Datos históricos de atributos, que se usan en los gráficos de estilo clásico en la página Nodes

Al recuperar un nodo de administración, el proceso de instalación del software crea una base de datos vacía del nodo de administración en el nodo recuperado. Sin embargo, la nueva base de datos solo incluye información sobre los servidores y servicios que forman parte del sistema en ese momento o que se añadan posteriormente.

Si has restaurado un nodo de administración principal y tu sistema StorageGRID cuenta con otro nodo de administración, puedes recuperar la información histórica copiando la base de datos del nodo de administración desde un nodo de administración que no sea el principal (el *nodo de administración de origen*) al nodo de administración principal recuperado. Si tu sistema solo cuenta con un nodo de administración principal, no puedes restaurar la base de datos del nodo de administración.



La copia de 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. Inicia sesión en el nodo Admin de origen:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.
2. Desde el nodo de administración de origen, detén el servicio MI: `service mi stop`
3. Desde el nodo de administración de origen, detén el servicio de la Management Application Program Interface (mgmt-api): `service mgmt-api stop`
4. Sigue estos pasos en el nodo de administración recuperado:
 - a. Inicia sesión en el nodo de administración recuperado:
 - i. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - iii. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - iv. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - b. Detén el servicio MI: `service mi stop`
 - c. Detén el servicio API mgmt-api: `service mgmt-api stop`
 - d. Añade la clave privada SSH al agente SSH. Introduce: `ssh-add`
 - e. Introduce la contraseña de acceso SSH que figura en el archivo `Passwords.txt`.
 - f. Copia 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 te solicite, confirma que quieres sobrescribir la base de datos MI en el nodo de administración recuperado.

La base de datos y sus datos históricos se copian en el nodo de administración recuperado. Una vez finalizada la operación de copia, el script inicia el nodo de administración recuperado.

- h. Cuando ya no necesites acceso sin contraseña a otros servidores, elimina la clave privada del agente SSH. Introduce: `ssh-add -D`

5. Reinicia los servicios en el nodo de administración de origen: `service servermanager start`

Restaura las métricas de Prometheus al recuperar el nodo primario de administración de StorageGRID

Si lo deseas, puedes conservar las métricas históricas gestionadas por Prometheus en un nodo de administración principal que haya fallado. Las métricas de Prometheus solo se pueden restaurar si tu sistema StorageGRID incluye otro nodo de administración.

Antes de empezar

- El nodo de administración recuperado está instalado y en funcionamiento.
- El sistema StorageGRID incluye al menos dos nodos de administración.
- Tienes el archivo `Passwords.txt`.
- Tienes la frase de contraseña de aprovisionamiento.

Acerca de esta tarea

Si un nodo de administración falla, se pierden las métricas almacenadas en la base de datos de Prometheus de dicho nodo. Al recuperar 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, este registra las métricas como si se hubiera realizado una nueva instalación del sistema StorageGRID.

Si has restaurado un nodo de administración principal y tu sistema StorageGRID cuenta con otro nodo de administración, puedes restaurar las métricas históricas copiando la base de datos de Prometheus desde un nodo de administración que no sea el principal (el nodo de administración de origen) al nodo de administración principal recuperado. Si tu sistema solo cuenta con un nodo de administración principal, no puedes restaurar la base de datos de Prometheus.



Copiar la base de datos de Prometheus puede tardar una hora o más. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios estén detenidos en el Admin Node de origen.

Pasos

1. Inicia sesión en el nodo Admin de origen:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.
2. Desde el nodo de administración de origen, detén el servicio Prometheus: `service prometheus stop`
3. Sigue estos pasos en el nodo de administración recuperado:

- a. Inicia sesión en el nodo de administración recuperado:
 - i. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - iii. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - iv. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- b. Detén el servicio Prometheus: `service prometheus stop`
- c. Añade la clave privada SSH al agente SSH. Introduce: `ssh-add`
- d. Introduce la contraseña de acceso SSH que figura en el archivo `Passwords.txt`.
- e. Copia la base de datos de Prometheus desde el 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 te solicite, pulsa **Intro** para confirmar que quieres 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 en el 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 necesites acceso sin contraseña a otros servidores, elimina la clave privada del agente SSH. Introduce: `ssh-add -D`
4. Reinicia el servicio Prometheus en el nodo de administración de origen. `service prometheus start`

Recupérate de fallos del nodo de administración no principal

Recupera de fallos no primarios del nodo de administración StorageGRID

Debes realizar las siguientes tareas para recuperarte de un fallo en un nodo de administración no principal. Un nodo de administración aloja el servicio Configuration Management Node (CMN) y se conoce como el nodo de administración principal. Aunque puedes 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.

Sigue estos pasos a grandes rasgos para recuperar un nodo de administración no principal:

1. "Copia los registros de auditoría del nodo de administración no principal que ha fallado"
2. "Sustituye el nodo de administración no principal"
3. "Selecciona Iniciar recuperación para configurar el nodo de administración no principal"
4. "Restaura el registro de auditoría en un nodo de administración no principal recuperado"
5. "Restaura la base de datos del nodo de administración cuando recuperas un nodo de administración que no es principal"
6. "Restaura las métricas de Prometheus al recuperar un nodo de administración no principal"

Copia los registros de auditoría de un nodo de administración StorageGRID no primario que falló

Si puedes copiar los registros de auditoría del nodo de administración que ha fallado, debes conservarlos para mantener el historial de la grid sobre la actividad y el uso del sistema. Puedes restaurar los registros de auditoría conservados en el nodo de administración no principal recuperado una vez que esté en funcionamiento.

Este procedimiento copia los archivos de auditoría del nodo de administración que ha fallado a una ubicación temporal en un nodo de grid independiente. Luego, estos registros de auditoría conservados pueden copiarse al nodo de administración de reemplazo. Los registros de auditoría no se copian automáticamente al nuevo nodo de administración.

Dependiendo del tipo de fallo, es posible que no puedas copiar los registros de auditoría de un nodo de administración que haya fallado. Si la implementación solo cuenta con 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 anteriormente. Si la implementación incluye más de un nodo de administración, puedes recuperar los registros de auditoría desde otro nodo de administración.



Si ahora no se puede acceder a los registros de auditoría en el nodo de administración que ha fallado, es posible que puedas acceder a ellos más adelante, por ejemplo, tras la recuperación del host.

1. Si es posible, inicia sesión en el nodo de administración que ha fallado. De lo contrario, inicia sesión en el nodo de administración principal o en otro nodo de administración, si hay alguno disponible.

- a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
- b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
- c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
- d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Detén el servicio AMS para evitar que cree un nuevo archivo de registro: `service ams stop`
3. Accede al directorio de exportación de auditorías:

```
cd /var/local/audit/export/
```

4. Cambia el nombre del archivo `audit.log` original por un nombre de archivo con un número único. Por ejemplo, cambia el nombre del archivo `audit.log` por `2023-10-25.txt.1`.

```
ls -l
mv audit.log 2023-10-25.txt.1
```

5. Reinicia el servicio AMS: `service ams start`
6. Crea el directorio para copiar todos los archivos de auditoría a una ubicación temporal en un nodo independiente de la grid: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Cuando se te solicite, introduce la contraseña de admin.

7. Copia todos los archivos de auditoría en la ubicación temporal: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Cuando se te solicite, introduce la contraseña de admin.

8. Cerrar sesión como root: `exit`

Sustituir nodo de administración StorageGRID no primario

Para recuperar un nodo de administración que no sea el principal, primero debes sustituir el hardware físico o virtual.

Puedes sustituir un nodo de administración no primario que haya fallado por otro nodo de administración no primario que se ejecute en la misma plataforma, o puedes sustituir un nodo de administración no primario que se ejecute en VMware o en un host Linux por un nodo de administración no primario alojado en un dispositivo de servicios.

Sigue el procedimiento correspondiente a la plataforma de sustitución que elijas para el nodo. Una vez completado el procedimiento de sustitución del nodo (apto para todos los tipos de nodos), dicho procedimiento te guiará hacia el siguiente paso para la recuperación de un nodo de administración no principal.

Plataforma de sustitución	Procedimiento
VMware	"Sustituir un nodo de VMware"
Linux	"Sustituir un nodo de Linux"
Dispositivos de servicios	"Sustituir 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 necesitas recuperar un nodo que se ejecuta en una implementación de OpenStack, descarga los archivos para tu sistema operativo Linux. Luego, sigue el procedimiento para "Reemplazar un nodo Linux" .

Selecciona Iniciar recuperación para configurar el nodo de administración StorageGRID no primario

Tras sustituir un nodo de administración no principal, debes seleccionar Iniciar recuperación en el Grid Manager para configurar el nuevo nodo como sustituto del nodo que ha fallado.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- Tienes la frase de contraseña de aprovisionamiento.
- Ya has implementado y configurado el nodo de sustitución.

Pasos

1. Desde el Grid Manager, selecciona **Maintenance > Tasks > Recovery**.
2. Selecciona el nodo de la grid que deseas recuperar en la lista Nodos pendientes.

Los nodos aparecen en la lista tras sufrir un fallo, pero no puedes seleccionar un nodo hasta que se haya reinstalado y esté listo para la recuperación.

3. Introduce la **frase de contraseña de aprovisionamiento**.
4. Haz 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. Supervisa el progreso de la recuperación en la tabla Recuperando nodo de grid.



Mientras se está ejecutando el procedimiento de recuperación, puedes hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparecerá un cuadro de diálogo en el que se indica que el nodo quedará en un estado indeterminado si restableces 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 quieres volver a intentar la recuperación después de reiniciar el procedimiento, debes restaurar el nodo a un estado preinstalado, así:

- **VMware:** Elimina el nodo de grid virtual desplegado. Luego, cuando estés listo para reiniciar la recuperación, vuelve a desplegar el nodo.
- **Linux:** Reinicia el nodo ejecutando este comando en el host Linux: `storagegrid node force-recovery node-name`
- **Dispositivo:** Si quieres volver a intentar la recuperación después de reiniciar el procedimiento, debes restaurar el nodo del dispositivo a un estado preinstalado ejecutando `sgareinstall` en el nodo. Consulta ["Prepara el appliance para la reinstalación \(solo reemplazo de la plataforma\)"](#).

6. Si el inicio de sesión único (SSO) está habilitado para tu sistema StorageGRID y la confianza de parte dependiente del nodo de administración que recuperaste se configuró para usar el certificado predeterminado de la interfaz de gestión, actualiza (o elimina y vuelve a crear) la confianza de parte dependiente del nodo en Active Directory Federation Services (AD FS). Usa el nuevo certificado de servidor predeterminado que se generó durante el proceso de recuperación del nodo de administración.



Para configurar una relación de confianza con una parte confiable, consulta ["Configura el inicio de sesión único"](#). Para acceder al certificado predeterminado del servidor, inicia sesión en el intérprete de comandos del Admin Node. Ve al directorio `/var/local/mgmt-api` y selecciona el archivo `server.crt`.

Restaurar registro de auditoría en un nodo de administración StorageGRID no primario recuperado

Si has podido conservar el registro de auditoría del nodo de administración no principal que ha fallado, de modo que se mantenga la información histórica del registro de auditoría, puedes copiarlo al nodo de administración no principal que estás recuperando.

Antes de empezar

- El nodo de administración recuperado está instalado y en funcionamiento.
- Has copiado los registros de auditoría a otra ubicación después de que fallara el nodo de administración original.

Acerca de esta tarea

Si un nodo de administración falla, los registros de auditoría guardados en ese nodo de administración podrían perderse. Podría ser posible evitar la pérdida de datos copiando los registros de auditoría del nodo de administración que falló y luego restaurando esos registros en el nodo de administración recuperado. Dependiendo del fallo, podría no ser posible copiar los registros de auditoría del nodo de administración que falló. En ese caso, si la implementación tiene más de un nodo de administración, puedes recuperar los registros de auditoría desde 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 es posible copiar el registro de auditoría del nodo que ha fallado, el nodo de administración recuperado comienza a registrar eventos en el registro de auditoría como si se tratara de una instalación nueva.

Debes recuperar un nodo de administración lo antes posible para restablecer la funcionalidad de registro.

De forma predeterminada, la información de auditoría se envía al registro de auditoría en los nodos de administración. Puedes omitir estos pasos si se da cualquiera de las siguientes circunstancias:



- Has configurado un servidor syslog externo y ahora los registros de auditoría se envían al servidor syslog en lugar de a los nodos de administración.
- Has especificado expresamente que los mensajes de auditoría solo deben guardarse en los nodos locales que los generaron.

Consulta ["Configura la gestión de registros y el servidor syslog externo"](#) para más detalles.

Pasos

1. Inicia sesión en el nodo de administración recuperado:

a. Introduce el siguiente comando:

```
ssh admin@recovery_Admin_Node_IP
```

b. Introduce la contraseña que figura en el archivo `Passwords.txt`.

c. Introduce el siguiente comando para pasar a ser usuario root: `su -`

d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Una vez que hayas iniciado sesión como root, el indicador de comando cambia de `$` a `#`.

2. Comprueba qué archivos de auditoría se han conservado:

```
cd /var/local/log
```

3. Copia los archivos de auditoría conservados en el nodo de administración recuperado:

```
scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
```

Cuando se te solicite, introduce la contraseña de admin.

4. Por motivos de seguridad, elimina los registros de auditoría del nodo de grid que ha fallado después de verificar que se han copiado correctamente al Admin Node recuperado.

5. Actualiza la configuración de usuarios y grupos 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 StorageGRID al recuperar un nodo de administración no primario

Si deseas conservar la información histórica sobre los atributos y las alertas de un nodo de administración no principal que haya fallado, puedes restaurar la base de datos del nodo de administración a partir del nodo de administración principal.

Antes de empezar

- El nodo de administración recuperado está instalado y en funcionamiento.

- El sistema StorageGRID incluye al menos dos nodos de administración.
- Tienes el archivo `Passwords.txt`.
- Tienes la frase de contraseña de aprovisionamiento.

Acerca de esta tarea

Si un nodo de administración falla, se pierde la información histórica almacenada en su base de datos de nodo de administración. Esta base de datos incluye la siguiente información:

- Historial de alertas
- Datos históricos de atributos, que se usan en los gráficos de estilo clásico en la página de Nodos

Al recuperar un nodo de administración, el proceso de instalación del software crea una base de datos vacía del nodo de administración en el nodo recuperado. Sin embargo, la nueva base de datos solo incluye información sobre los servidores y servicios que forman parte del sistema en ese momento o que se añadan posteriormente.

Si has restaurado un nodo de administración que no es el principal, puedes recuperar la información histórica copiando la base de datos del nodo de administración principal (el *nodo de administración de origen*) al nodo recuperado.



La copia de 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. Inicia sesión en el nodo Admin de origen:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.
2. Ejecuta el siguiente comando desde el nodo de administración de origen. Luego, introduce la frase de contraseña de aprovisionamiento si se te solicita. `recover-access-points`
3. Desde el nodo de administración de origen, detén el servicio MI: `service mi stop`
4. Desde el nodo de administración de origen, detén el servicio de la Management Application Program Interface (mgmt-api): `service mgmt-api stop`
5. Sigue estos pasos en el nodo de administración recuperado:
 - a. Inicia sesión en el nodo de administración recuperado:
 - i. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - iii. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - iv. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - b. Detén el servicio MI: `service mi stop`
 - c. Detén el servicio API mgmt-api: `service mgmt-api stop`

- d. Añade la clave privada SSH al agente SSH. Introduce: `ssh-add`
- e. Introduce la contraseña de acceso SSH que figura en el archivo `Passwords.txt`.
- f. Copia 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 te solicite, confirma que quieres sobrescribir la base de datos MI en el nodo de administración recuperado.

La base de datos y sus datos históricos se copian en el nodo de administración recuperado. Una vez finalizada la operación de copia, el script inicia el nodo de administración recuperado.

- h. Cuando ya no necesites acceso sin contraseña a otros servidores, elimina la clave privada del agente SSH. Introduce: `ssh-add -D`

6. Reinicia los servicios en el nodo de administración de origen: `service servermanager start`

Restaura las métricas de Prometheus cuando recuperas un nodo de administración de StorageGRID que no es primario

Si lo deseas, puedes conservar las métricas históricas que gestiona Prometheus en un nodo de administración no principal que ha fallado.

Antes de empezar

- El nodo de administración recuperado está instalado y en funcionamiento.
- El sistema StorageGRID incluye al menos dos nodos de administración.
- Tienes el archivo `Passwords.txt`.
- Tienes la frase de contraseña de aprovisionamiento.

Acerca de esta tarea

Si un nodo de administración falla, se pierden las métricas almacenadas en la base de datos de Prometheus de dicho nodo. Al recuperar 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, este registra las métricas como si se hubiera realizado una nueva instalación del sistema StorageGRID.

Si has restaurado un nodo de administración que no es el principal, puedes recuperar 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 puede tardar una hora o más. Algunas funciones de Grid Manager no estarán disponibles mientras los servicios estén detenidos en el Admin Node de origen.

Pasos

1. Inicia sesión en el nodo Admin de origen:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

2. Desde el nodo de administración de origen, detén el servicio Prometheus: `service prometheus stop`
3. Sigue estos pasos en el nodo de administración recuperado:
 - a. Inicia sesión en el nodo de administración recuperado:
 - i. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - ii. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - iii. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - iv. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - b. Detén el servicio Prometheus: `service prometheus stop`
 - c. Añade la clave privada SSH al agente SSH. Introduce: `ssh-add`
 - d. Introduce la contraseña de acceso SSH que figura en el archivo `Passwords.txt`.
 - e. Copia la base de datos de Prometheus desde el 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 te solicite, pulsa **Intro** para confirmar que quieres 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 en el 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 necesites acceso sin contraseña a otros servidores, elimina la clave privada del agente SSH. Introduce: `ssh-add -D`
4. Reinicia el servicio Prometheus en el nodo de administración de origen. `service prometheus start`

Recupera ante fallos del nodo de puerta de enlace

Reemplazar nodo StorageGRID Gateway

Puedes sustituir un Gateway Node que haya fallado por un Gateway Node que se ejecute en el mismo hardware físico o virtual, o bien puedes sustituir un Gateway Node que se ejecute en un host VMware o Linux por un Gateway Node alojado en un services appliance.

El procedimiento de sustitución del nodo que debes seguir depende de la plataforma que vaya a utilizar el nodo de sustitución. Una vez que completes el procedimiento de sustitución del nodo (que es apto para todos los tipos de nodos), ese procedimiento te llevará al siguiente paso para la recuperación del Gateway Node.

Plataforma de sustitución	Procedimiento
VMware	"Sustituir un nodo de VMware"
Linux	"Sustituir un nodo de Linux"

Plataforma de sustitución	Procedimiento
Dispositivos de servicios	"Sustituir 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 necesitas recuperar un nodo que se ejecuta en una implementación de OpenStack, descarga los archivos para tu sistema operativo Linux. Luego, sigue el procedimiento para "Reemplazar un nodo Linux" .

Selecciona Iniciar recuperación para configurar el nodo StorageGRID Gateway

Después de reemplazar un nodo de puerta de enlace, debes seleccionar Iniciar recuperación en el Grid Manager para configurar el nuevo nodo como reemplazo del nodo con fallo.

Antes de empezar

- Has iniciado sesión en Grid Manager mediante un ["navegador web compatible"](#).
- Tienes el ["Permiso de mantenimiento o acceso de usuario raíz"](#).
- Tienes la frase de contraseña de aprovisionamiento.
- Ya has implementado y configurado el nodo de sustitución.

Pasos

1. Desde el Grid Manager, selecciona **Maintenance > Tasks > Recovery**.
2. Selecciona el nodo de la grid que deseas recuperar en la lista Nodos pendientes.

Los nodos aparecen en la lista tras sufrir un fallo, pero no puedes seleccionar un nodo hasta que se haya reinstalado y esté listo para la recuperación.

3. Introduce la **frase de contraseña de aprovisionamiento**.
4. Haz 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. Supervisa el progreso de la recuperación en la tabla Recuperando nodo de grid.



Mientras se está ejecutando el procedimiento de recuperación, puedes hacer clic en **Restablecer** para iniciar una nueva recuperación. Aparecerá un cuadro de diálogo en el que se indica que el nodo quedará en un estado indeterminado si restableces 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 quieres volver a intentar la recuperación después de reiniciar el procedimiento, debes restaurar el nodo a un estado preinstalado, así:

- **VMware:** Elimina el nodo de grid virtual desplegado. Luego, cuando estés listo para reiniciar la recuperación, vuelve a desplegar el nodo.
- **Linux:** Reinicia el nodo ejecutando este comando en el host Linux: `storagegrid node force-recovery node-name`
- **Dispositivo:** Si quieres volver a intentar la recuperación después de reiniciar el procedimiento, debes restaurar el nodo del dispositivo a un estado preinstalado ejecutando `sgareinstall` en el nodo.

Recupera tras fallos en los nodos de archivo

Recupera de fallos del nodo de archivo StorageGRID

Se ha eliminado la compatibilidad con los Archive Nodes.

Para obtener información sobre cómo recuperar nodos de archivo, consulta ["Recupera tras fallos en los nodos de archivo \(sitio de documentación de StorageGRID 11.8\)"](#).

Reemplazar nodo Linux

Reemplazar un nodo Linux en StorageGRID

Si un fallo requiere que implementes uno o varios hosts físicos o virtuales nuevos, o que reinstales Linux en un host existente, primero debes implementar y configurar el host de reemplazo antes de poder recuperar el nodo de grid. Este procedimiento es un paso del proceso de recuperación de nodos de grid para todos los tipos de nodos de grid.

«Linux» hace referencia a una instalación de Red Hat® Enterprise Linux® (RHEL), Ubuntu® o Debian®. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Este procedimiento solo se lleva a cabo 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 pasarela. Los pasos son idénticos independientemente del tipo de nodo de grid que estés recuperando.

Si hay más de un nodo de red alojado en un servidor Linux físico o virtual, puedes recuperar los nodos de red en cualquier orden. Sin embargo, si recuperas primero el nodo de administración principal, en caso de que exista, evitas que la recuperación de los demás nodos de red se bloquee al intentar ponerse en contacto con el nodo de administración principal para registrarse en la recuperación.

Implementa nuevos hosts Linux para StorageGRID

Salvo algunas excepciones, debes preparar los nuevos hosts tal y como lo hiciste durante el proceso de instalación inicial.

Para implementar hosts Linux físicos o virtuales nuevos o reinstalados, sigue el procedimiento de preparación de los hosts que se describe en las instrucciones de instalación de StorageGRID correspondientes a tu sistema operativo Linux. Consulta ["Instalar Linux"](#).



«Linux» hace referencia a una instalación de RHEL, Ubuntu o Debian. Para consultar la lista de versiones compatibles, visita ["Herramienta de matriz de interoperabilidad \(IMT\) de NetApp"](#).

Este procedimiento incluye los pasos necesarios para realizar las siguientes tareas:

1. Instala Linux.
2. Configura la red del host.

3. Configura el almacenamiento del host.
4. Instala el motor de contenedores.
5. Instala el servicio de host de StorageGRID.



Detente una vez que hayas completado la tarea «Instalar el servicio de host de StorageGRID» de las instrucciones de instalación. No inicies la tarea «Implementar nodos de la grid».

Mientras sigues estos pasos, ten en cuenta las siguientes indicaciones importantes:

- Asegúrate de utilizar los mismos nombres de interfaz del host que utilizaste en el host original.
- Si utilizas almacenamiento compartido para tus nodos de StorageGRID, o si has trasladado algunas o todas las unidades o SSD de los nodos con error a los nodos de sustitución, debes restablecer las mismas asignaciones de almacenamiento que había en el host original. Por ejemplo, si usaste WWID y alias en `/etc/multipath.conf` como se recomienda en las instrucciones de instalación, asegúrate de usar los mismos pares de alias/WWID en `/etc/multipath.conf` en el host de sustitución.
- Si el nodo de StorageGRID utiliza almacenamiento asignado desde un sistema NetApp ONTAP, comprueba que el volumen no tenga una política de nivelación de FabricPool habilitada. Desactivar la nivelación de FabricPool para los volúmenes usados con nodos de StorageGRID simplifica la solución de problemas y las operaciones de almacenamiento.



Nunca uses FabricPool para transferir ningún dato relacionado con StorageGRID de vuelta al propio StorageGRID. Transferir datos de StorageGRID de vuelta a StorageGRID aumenta la complejidad de la resolución de problemas y de las operaciones.

Restaura los nodos StorageGRID en el host

Para restaurar un nodo de grid que ha fallado en un nuevo host Linux, sigue 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, creas un archivo de configuración de nodo para cada nodo de grid que se va a instalar en un host. Cuando restauras un nodo de grid en un host de reemplazo, restauras o reemplazas el archivo de configuración de nodo para cualquier nodo de grid que haya fallado.
2. [Inicia el servicio de host de StorageGRID](#).
3. Si es necesario, [recupera cualquier nodo que no logre iniciarse](#).

Si se han conservado volúmenes de almacenamiento en bloque del host anterior, es posible que tengas que llevar a cabo procedimientos de recuperación adicionales. Los comandos de esta sección te ayudan a determinar qué procedimientos adicionales son necesarios.

Restaurar y validar los nodos de la red

Debes restaurar los archivos de configuración de la grid para cualquier nodo de la grid que haya fallado y luego validar los archivos de configuración de la grid y resolver cualquier error.

Acerca de esta tarea

Puedes importar cualquier nodo de la grid que deba estar presente en el host, siempre y cuando su volumen `/var/local` no se haya perdido como resultado del fallo del host anterior. Por ejemplo, el volumen

`/var/local` podría seguir existiendo si usaste almacenamiento compartido para los volúmenes de datos del sistema StorageGRID, como se describe en las instrucciones de instalación de StorageGRID para tu sistema operativo Linux. Importar el nodo restaura su archivo de configuración en el host.

Si no es posible importar los nodos que faltan, deberás volver a crear sus archivos de configuración de grid.

A continuación, debes validar el archivo de configuración de grid y resolver cualquier problema de red o almacenamiento que pueda surgir antes de reiniciar StorageGRID. Cuando vuelvas a crear el archivo de configuración de un nodo, debes usar el mismo nombre para el nodo de reemplazo que se usó para el nodo que estás recuperando.

Consulta la ["Instrucciones de instalación de Linux"](#) para obtener más información sobre la ubicación del volumen `/var/local` de un nodo.

Pasos

1. En la línea de comandos del host recuperado, muestra todos los nodos de StorageGRID configurados actualmente:`sudo storagegrid node list`

Si no se ha configurado ningún nodo de la grid, no habrá salida. Si se han configurado algunos nodos de la grid, la salida tendrá el siguiente formato:

Name	Metadata-Volume
dc1-adm1	/dev/mapper/sgws-adm1-var-local
dc1-gw1	/dev/mapper/sgws-gw1-var-local
dc1-sn1	/dev/mapper/sgws-sn1-var-local
dc1-arc1	/dev/mapper/sgws-arc1-var-local

Si no aparecen en la lista algunos o todos los nodos de grid que deberían estar configurados en el host, necesitas restaurar los nodos de grid que faltan.

2. Para importar nodos de la grid que tienen un volumen `/var/local`:

- a. Ejecuta el siguiente comando para cada nodo que quieras importar:`sudo storagegrid node import node-var-local-volume-path`

El `storagegrid node import` comando solo se ejecuta correctamente si el nodo de destino se apagó correctamente en el host en el que se ejecutó por última vez. Si no es así, aparecerá 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 ves el error de que el nodo pertenece a otro host, ejecuta el comando de nuevo con la opción `--force` para completar la importación:`sudo storagegrid --force node import node-var-local-volume-path`



Cualquier nodo importado con el indicador `--force` requerirá pasos de recuperación adicionales antes de poder volver a unirse a la grid, como se describe en ["Próximos pasos: realiza los pasos de recuperación adicionales, si es necesario"](#).

3. Para los nodos de la grid que no tienen un volumen `/var/local`, vuelve a crear el archivo de configuración del nodo para restaurarlo en el host. Para obtener instrucciones, consulta ["Crear archivos de configuración de nodos"](#).



Al volver a crear el archivo de configuración de un nodo, debes usar para el nodo de reemplazo el mismo nombre que se usó para el nodo que estás recuperando. Para implementaciones en Linux, asegúrate de que el nombre del archivo de configuración contenga el nombre de nodo. Deberías usar las mismas interfaces de red, asignaciones de dispositivos de bloque y direcciones IP siempre que sea posible. Esta práctica minimiza la cantidad de datos que se deben copiar 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 utilizas dispositivos de bloque nuevos (dispositivos que el nodo de StorageGRID no haya utilizado anteriormente) como valores para cualquiera de las variables de configuración que comienzan con `BLOCK_DEVICE_` cuando vuelvas a crear el archivo de configuración de un nodo, sigue las pautas de [Soluciona los errores de dispositivos de bloque que faltan](#).

4. Ejecuta el siguiente comando en el host recuperado para listar todos los nodos de StorageGRID.

```
sudo storagegrid node list
```

5. Valida el archivo de configuración de cada nodo de grid cuyo nombre apareció en la salida de `storagegrid node list`:

```
sudo storagegrid node validate node-name
```

Debes solucionar cualquier error o advertencia antes de iniciar el servicio de host de StorageGRID. En las secciones siguientes se ofrece más información sobre los errores que pueden tener una importancia especial durante la recuperación.

Soluciona los errores de interfaz de red faltante

Si la red de host no está configurada correctamente o hay un error ortográfico en un nombre, se produce un error cuando StorageGRID comprueba la asignación especificada en el archivo `/etc/storagegrid/nodes/node-name.conf`.

Es posible que veas un error o una advertencia que se ajuste a 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 haberse notificado en la red Grid, la red Admin o la red Client. Este error significa que el `/etc/storagegrid/nodes/node-name.conf` archivo asigna la red StorageGRID indicada a la interfaz del host llamada `host-interface-name`, pero no existe ninguna interfaz con ese nombre en el host actual.

Si aparece este error, comprueba que hayas seguido los pasos que se indican en ["Implementar nuevos hosts Linux"](#). Utiliza para todas las interfaces del host los mismos nombres que se utilizaban en el host original.

Si no puedes asignar nombres a las interfaces del host que coincidan con el archivo de configuración del nodo, puedes 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 del host ya existente.

Asegúrate de que la interfaz del host proporcione acceso al puerto de red físico o a la VLAN adecuados, y de que la interfaz no haga referencia directa a un dispositivo bond o bridge. Debes configurar una VLAN (u otra interfaz virtual) sobre el dispositivo bond del host, o bien utilizar un bridge y un par de Ethernet virtual (veth).

Soluciona los errores de dispositivos de bloque que faltan

El sistema comprueba que cada nodo recuperado se asigne a un archivo especial de dispositivo de bloques válido o a un enlace simbólico válido que apunte a un archivo especial de dispositivo de bloques. Si StorageGRID detecta una asignación no válida en el archivo `/etc/storagegrid/nodes/node-name.conf`, se muestra un error de dispositivo de bloques ausente.

Si detectas un error que se ajuste a 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
```

Esto significa que `/etc/storagegrid/nodes/node-name.conf` asigna el dispositivo de bloques 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 bloques válido ni un enlace simbólico a un archivo especial de dispositivo de bloques en esa ubicación.

Comprueba que has seguido los pasos descritos en ["Implementar nuevos hosts Linux"](#). Utiliza los mismos nombres de dispositivo persistentes para todos los dispositivos de bloque que se usaban en el host original.

Si no puedes restaurar o volver a crear el archivo especial de dispositivo de bloques que falta, puedes asignar un nuevo dispositivo de bloques del tamaño y la categoría de almacenamiento adecuados y editar el archivo de configuración del nodo para cambiar el valor de `BLOCK_DEVICE_PURPOSE` para que apunte al nuevo archivo especial de dispositivo de bloques.

Determina el tamaño y la categoría de almacenamiento adecuados utilizando las tablas correspondientes a tu sistema operativo Linux. Consulta ["Requisitos de almacenamiento y rendimiento"](#).

Consulta las recomendaciones de ["configuración del almacenamiento del host"](#) antes de proceder con la sustitución del dispositivo de bloque.



Si tienes que proporcionar un nuevo dispositivo de almacenamiento en bloque para cualquiera de las variables del archivo de configuración que comienzan por `BLOCK_DEVICE_` porque el dispositivo en bloque original se perdió junto con el host que falló, asegúrate de que el nuevo dispositivo en bloque no esté formateado antes de intentar seguir con los procedimientos de recuperación. El nuevo dispositivo en bloque no estará formateado si usas almacenamiento compartido y has creado un nuevo volumen. Si no estás seguro, ejecuta el siguiente comando en cualquier archivo especial de un nuevo dispositivo de almacenamiento en bloque.



Ejecuta el siguiente comando únicamente para dispositivos de almacenamiento en bloque nuevos. No ejecutes este comando si crees 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
```

Inicia el servicio de host de StorageGRID

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

Pasos

1. Ejecuta los siguientes comandos en cada host:

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

2. Ejecuta el siguiente comando para asegurarte de que la implementación se está llevando a cabo:

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

3. Si algún nodo muestra el estado "Not Running" o "Stopped", ejecuta el siguiente comando:

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

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

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

Recupera los nodos que no se inician normalmente

Si un nodo de StorageGRID no vuelve a incorporarse a la red de forma normal y no aparece como recuperable, es posible que esté dañado. Puedes forzar que el nodo entre en modo de recuperación.

Pasos

1. Comprueba que la configuración de red del nodo sea correcta.

Es posible que el nodo no haya podido volver a unirse al grid debido a asignaciones incorrectas de la interfaz de red o a una dirección IP o puerta de enlace incorrectas de la Grid Network.

2. Si la configuración de red es correcta, ejecuta el comando `force-recovery`:

```
sudo storagegrid node force-recovery node-name
```

3. Sigue los pasos de recuperación adicionales para el nodo. Consulta ["Próximos pasos: realiza los pasos de recuperación adicionales, si es necesario"](#).

Realiza los pasos adicionales de recuperación del nodo StorageGRID

Dependiendo de las acciones concretas que hayas llevado a cabo para poner en marcha los nodos de StorageGRID en el host de sustitución, es posible que tengas que realizar pasos de recuperación adicionales para cada nodo.

La recuperación del nodo se completa si no necesitaste tomar ninguna medida correctiva mientras reemplazabas el host Linux o restaurabas el nodo de grid que falló en el nuevo host.

Medidas correctivas y próximos pasos

Durante la sustitución del nodo, es posible que hayas tenido que tomar una de estas acciones correctivas:

- Tenías que usar la bandera `--force` para importar el nodo.
- Para cualquier `<PURPOSE>`, el valor de la variable del archivo de configuración `BLOCK_DEVICE_<PURPOSE>` hace referencia a un dispositivo de bloque que no contiene los mismos datos que tenía antes del fallo del host.
- Has emitido `storagegrid node force-recovery node-name` para el nodo.
- Has añadido un nuevo dispositivo de bloque.

Si has llevado a cabo **cualquiera** de estas medidas correctivas, debes realizar pasos de recuperación adicionales.

Tipo de recuperación	Siguiente paso
Nodo de administración principal	"Configura el nodo de administración principal de sustitución"
Nodo de administración no principal	"Selecciona Iniciar recuperación para configurar un nodo de administración no principal"
Nodo de puerta de enlace	"Selecciona Iniciar recuperación para configurar el nodo de puerta de enlace"
Nodo de almacenamiento (basado en software): • Si tuviste que usar el indicador <code>--force</code> para importar el nodo, o ejecutaste <code>storagegrid node force-recovery node-name</code> • Si tuvieras que reinstalar completamente el nodo o necesitaras restaurar <code>/var/local</code>	"Selecciona Iniciar recuperación para configurar el nodo de almacenamiento"

Tipo de recuperación	Siguiente paso
Nodo de almacenamiento (basado en software): • Si has añadido un nuevo dispositivo de bloque. • Si, por cualquier <PURPOSE>, el valor de la variable del archivo de configuración <code>BLOCK_DEVICE_<PURPOSE></code> hace referencia a un dispositivo de bloque que no contiene los mismos datos que tenía antes del fallo del host.	"Recupérate de un fallo del volumen de almacenamiento cuando la unidad del sistema está intacta"

Reemplazar un nodo VMware en StorageGRID

Cuando recuperas un nodo de StorageGRID que ha fallado y que estaba alojado en VMware, eliminas el nodo que falló e implementas un nodo de recuperación.

Antes de empezar

Has determinado que la máquina virtual no se puede restaurar y que hay que reemplazarla.

Acerca de esta tarea

Usa el cliente web de VMware vSphere para primero eliminar la máquina virtual asociada con el nodo de grid que falló. Luego, puedes implementar una nueva máquina virtual.

Este procedimiento es solo uno de los pasos del proceso de recuperación de nodos de la red. El procedimiento de eliminación y despliegue 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. Inicia sesión en VMware vSphere Web Client.
2. Accede a la máquina virtual del nodo de grid que ha fallado.
3. Anota toda la información necesaria para implementar el nodo de recuperación.
 - a. Haz clic con el botón derecho del ratón sobre la máquina virtual, selecciona la pestaña **Editar configuración** y toma nota de los ajustes en uso.
 - b. Selecciona la pestaña **vApp Options** para ver y registrar la configuración de red del nodo de grid.
4. Si el nodo de la cuadrícula que ha fallado es un nodo de almacenamiento, determina si alguno de los discos duros virtuales usados para el almacenamiento de datos está sin daños y consérvales para volver a adjuntarlos al nodo de la cuadrícula recuperado.
5. Apaga la máquina virtual.
6. Selecciona **Acciones > Todas las acciones de vCenter > Eliminar del disco** para eliminar la máquina virtual.
7. Implementa una nueva máquina virtual que sirva como nodo de sustitución y conéctala a una o varias redes StorageGRID. Para obtener instrucciones, consulta ["Implementación de un nodo de StorageGRID como máquina virtual"](#).

Cuando implementas el nodo, puedes opcionalmente reasignar los puertos del nodo o aumentar la configuración de CPU o memoria.



Después de implementar el nuevo nodo, puedes añadir nuevos discos virtuales según tus requisitos de almacenamiento, volver a conectar cualquier disco duro virtual que hayas conservado del nodo de grid averiado y eliminado anteriormente, o ambas cosas.

8. Completa el procedimiento de recuperación del nodo, según el tipo de nodo que estés recuperando.

Tipo de nodo	Ir a
Nodo de administración principal	"Configura el nodo de administración principal de sustitución"
Nodo de administración no principal	"Selecciona Iniciar recuperación para configurar un nodo de administración no principal"
Nodo de puerta de enlace	"Selecciona Iniciar recuperación para configurar el nodo de puerta de enlace"
Nodo de almacenamiento	"Selecciona Iniciar recuperación para configurar el nodo de almacenamiento"

Sustituye el nodo averiado por un dispositivo de servicios

Reemplaza el nodo StorageGRID fallido con un dispositivo de servicios

Puedes utilizar un dispositivo de servicios para recuperar un Gateway Node que haya fallado, un non-primary Admin Node que haya fallado o un primary Admin Node que haya fallado y que estuviera alojado en VMware, en un host Linux o en un dispositivo de servicios. Este procedimiento es un paso del procedimiento de recuperación de grid node.

Antes de empezar

- Has determinado que se da una de las siguientes situaciones:
 - No es posible restaurar la máquina virtual que aloja el nodo.
 - El host Linux físico o virtual del nodo de grid ha fallado y debe ser reemplazado.
 - Hay que sustituir el dispositivo de servicios que aloja el nodo de la grid.
- Has confirmado que la versión del instalador de StorageGRID Appliance en el dispositivo de servicios coincide con la versión de software de tu sistema StorageGRID. Consulta ["Verifica y actualiza la versión de StorageGRID Appliance Installer"](#).



No instales tanto un dispositivo de servicios SG110 como un SG1100, ni un SG100 y un SG1000, en el mismo sitio. Podrías obtener un rendimiento impredecible.

Acerca de esta tarea

Puedes utilizar un dispositivo de servicios para recuperar un nodo de grid que haya fallado en los siguientes casos:

- El nodo que ha fallado estaba alojado en VMware o Linux (["cambio de plataforma"](#))

- El nodo que ha fallado estaba alojado en un dispositivo de servicios ("[sustitución de la plataforma](#)")

Instala el dispositivo de servicios StorageGRID (solo cambio de plataforma)

Cuando estés recuperando un nodo de la red que haya fallado y que estuviera alojado en VMware o en un host Linux, y estés usando un dispositivo de servicios como nodo de reemplazo, primero debes instalar el nuevo hardware del dispositivo usando el mismo nombre de nodo (nombre del sistema) que el nodo que falló.

Antes de empezar

Dispones de la siguiente información sobre el nodo que ha fallado:

- **Nombre de nodo:** Debes instalar el dispositivo de servicios utilizando el mismo nombre de nodo que el nodo que ha fallado. El nombre de nodo es el nombre de host (nombre del sistema).
- **Direcciones IP:** Puedes asignar al dispositivo de servicios las mismas direcciones IP que el nodo que falló, que es la opción preferida, o puedes seleccionar una nueva dirección IP no utilizada en cada red.

Acerca de esta tarea

Realiza este procedimiento únicamente si vas a recuperar un nodo que ha fallado y que estaba alojado en VMware o Linux y lo vas a sustituir por un nodo alojado en un dispositivo de servicios.

Pasos

1. Sigue las instrucciones para instalar un nuevo dispositivo de servicios. Consulta "[Guía de inicio rápido para la instalación del hardware](#)".
2. Cuando se te solicite un nombre de nodo, usa el nombre de nodo del nodo que falló.

Prepara el dispositivo StorageGRID para la reinstalación (solo reemplazo de plataforma)

Al recuperar un nodo de la red que estaba alojado en un dispositivo de servicios, primero debes preparar el dispositivo para la reinstalación del software StorageGRID.

Realiza este procedimiento únicamente si vas a sustituir un nodo averiado que estaba alojado en un dispositivo de servicios. No sigas estos pasos si el nodo averiado estaba alojado originalmente en VMware o en un host Linux.

Pasos

1. Inicia sesión en el nodo de grid que ha fallado:
 - a. Introduce el siguiente comando: `ssh admin@grid_node_IP`
 - b. Introduce la contraseña que figura en el archivo `Passwords.txt`.
 - c. Introduce el siguiente comando para pasar a ser usuario root: `su -`
 - d. Introduce la contraseña que figura en el archivo `Passwords.txt`.

Cuando inicias sesión como root, el indicador cambia de `$` a `#`.

2. Prepara el dispositivo para la instalación del software StorageGRID. Introduce: `sgareinstall`
3. Cuando se te pida que continúes, introduce: `y`

El dispositivo se reinicia y tu sesión SSH finaliza. Normalmente, el instalador de StorageGRID Appliance tarda unos 5 minutos en estar disponible, aunque en algunos casos puede que tengas que esperar hasta 30 minutos.

El dispositivo de servicios se ha reiniciado y ya no se puede acceder a los datos del nodo de la red. Las direcciones IP configuradas durante el proceso de instalación original deberían permanecer intactas; sin embargo, se recomienda que lo confirmes cuando termine el procedimiento.

Después de ejecutar el comando `sgareinstall`, se eliminan todas las cuentas, contraseñas y claves SSH aprovisionadas por StorageGRID, y se generan nuevas claves de host.

Inicia la instalación del software StorageGRID en un dispositivo de servicios

Para instalar un nodo de puerta de enlace o un nodo de administración en un dispositivo de servicios, usas el StorageGRID Appliance Installer, que viene incluido en el dispositivo.

Antes de empezar

- El dispositivo se instala en un rack, se conecta a tus redes y se enciende.
- Las conexiones de red y las direcciones IP se configuran para el dispositivo usando el StorageGRID Appliance Installer.
- Si vas a instalar un nodo de puerta de enlace o un nodo de administración no principal, debes conocer la dirección IP del nodo de administración principal de StorageGRID.
- Todas las subredes de la Grid Network que aparecen en la página de configuración de IP del StorageGRID Appliance Installer están definidas en la Grid Network Subnet List en el nodo Admin principal.

Consulta ["Guía de inicio rápido para la instalación del hardware"](#).

- Estás usando un ["navegador web compatible"](#).
- Tienes una de las direcciones IP asignadas al dispositivo. Puedes utilizar la dirección IP para la red de administración, la red de grid o la red de clientes.
- Si vas a instalar un nodo de administración principal, tienes a tu disposición los archivos de instalación de Ubuntu o Debian para esta versión de StorageGRID.



Durante la fabricación, se instala de fábrica una versión reciente del software StorageGRID en el dispositivo de servicios. Si la versión del software instalada de fábrica coincide con la versión que usas en tu implementación de StorageGRID, no necesitas los archivos de instalación.

Acerca de esta tarea

Para instalar el software StorageGRID en un dispositivo de servicios:

- Para un nodo de administración principal, especificas el nombre de nodo y luego cargas los paquetes de software correspondientes (si es necesario).
- Para un nodo de administración no principal o un nodo de puerta de enlace, especificas o confirmas la dirección IP del nodo de administración principal y el nombre del nodo.
- Inicia la instalación y espera a que se configuren los volúmenes y se instale el software.

- A mitad del proceso, la instalación se detiene. Para reanudar la instalación, debes iniciar sesión en Grid Manager y configurar el nodo pendiente como reemplazo del nodo que ha fallado.
- Después de que hayas configurado el nodo, el proceso de instalación del dispositivo se completa y el dispositivo se reinicia.

Pasos

1. Abre un navegador e introduce una de las direcciones IP del dispositivo de servicios.

`https://Controller_IP:8443`

Aparece la página de inicio del instalador de StorageGRID Appliance.

2. Para instalar un nodo de administración principal:

- a. En la sección Este nodo, para **Tipo de nodo**, selecciona **Administrador principal**.
- b. En el campo **Nombre de nodo**, introduce el mismo nombre que se utilizó para el nodo que estás recuperando y haz clic en **Guardar**.
- c. En la sección Instalación, comprueba la versión del software que aparece en Estado actual

Si la versión del software que está lista para instalar es la correcta, salta directamente a la [Paso de instalación](#).

- d. Si necesitas cargar una versión diferente del software, en el menú **Avanzado**, selecciona **Cargar software de StorageGRID**.

Aparece la página «Cargar el software de StorageGRID».

- e. Haz clic en **Examinar** para cargar el **paquete de software** y el **archivo de suma de comprobación** para el software StorageGRID.

Los archivos se suben automáticamente una vez que los seleccionas.

- f. Haz clic en **Inicio** para volver a la página de inicio del instalador de StorageGRID Appliance.

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**, selecciona **Gateway** o **Non-Primary Admin**, según el tipo de nodo que vayas a restaurar.
- b. En el campo **Nombre de nodo**, introduce el mismo nombre que se utilizó para el nodo que estás recuperando y haz clic en **Guardar**.
- c. En la sección «Conexión al nodo de administración principal», determina si necesitas especificar la dirección IP del nodo de administración principal.

El instalador de StorageGRID Appliance puede detectar esta dirección IP automáticamente, siempre que el nodo de administración principal, o al menos otro nodo de grid con ADMIN_IP configurado, esté presente en la misma subred.

- d. Si esta dirección IP no aparece o necesitas cambiarla, indica la dirección:

Opción	Descripción
Introducción manual de la dirección IP	a. Desmarca la casilla Habilitar detección de nodos de administración. b. Introduce la dirección IP manualmente. c. Haz clic en Guardar. d. Espera mientras el estado de conexión de la nueva dirección IP se vuelve "listo".
Detección automática de todos los nodos de administración principales conectados	a. Marca la casilla Habilitar detección de nodos de administración. b. De la lista de direcciones IP detectadas, selecciona el nodo de administración principal para el grid donde se va a implementar este dispositivo de servicios. c. Haz clic en Guardar. d. Espera mientras el estado de conexión de la nueva dirección IP se vuelve "listo".

4. En la sección Instalación, comprueba que el estado actual sea Listo para iniciar la instalación de nombre de nodo y que el botón **Iniciar instalación** esté activado.

Si el botón **Iniciar instalación** no está activo, es posible que tengas que modificar la configuración de red o los ajustes de puerto. Consulta las instrucciones de mantenimiento de tu appliance.

5. En la página de inicio del instalador de StorageGRID Appliance, haz clic en **Iniciar instalación**.

El estado actual cambia a «Instalación en curso» y se muestra la página «Supervisar la instalación».



Si necesitas acceder manualmente a la página **Monitor Installation**, haz clic en **Monitor Installation** en la barra de menú.

Supervisa la instalación del dispositivo de servicios StorageGRID

El instalador de StorageGRID Appliance muestra el estado hasta que la instalación se completa. Cuando la instalación del software se completa, el appliance se reinicia.

Pasos

1. Para supervisar el progreso de la instalación, haz clic en **Monitor Installation** en la barra de menús.

La página de instalación del monitor muestra el progreso de la instalación.

La barra de estado azul indica qué tarea está actualmente en progreso. Las barras de estado verdes indican las tareas que se han completado correctamente.



El instalador se asegura de que las tareas completadas en una instalación anterior no se vuelvan a ejecutar. Si vuelves a ejecutar una instalación, las tareas que no necesiten volver a ejecutarse se muestran con una barra de estado verde y el estado "Skipped".

2. Revisa el avance de las dos primeras fases de la instalación.

◦ **1. Configura el almacenamiento**

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

◦ **2. Instala el sistema operativo**

Durante esta fase, el instalador copia la imagen del sistema operativo base de StorageGRID desde el nodo de administración principal al dispositivo, o bien instala el sistema operativo base a partir del paquete de instalación del nodo de administración principal.

3. Sigue supervisando el progreso de la instalación hasta que ocurra una de las siguientes situaciones:

- Para los nodos Gateway de appliance o los nodos Admin de appliance que no son primarios, la etapa **Install StorageGRID** se pausa y aparece un mensaje en la consola integrada, indicándote que apruebes este nodo en el Admin Node usando Grid Manager.
- Para los nodos de administración principales del appliance, aparece una quinta fase (Cargar StorageGRID Installer). Si la quinta fase está en curso durante más de 10 minutos, actualiza la página manualmente.

4. Pasa al siguiente paso del proceso de recuperación para el tipo de nodo de grid del appliance que estás recuperando.

Tipo de recuperación	Referencia
Nodo de puerta de enlace	"Selecciona Iniciar recuperación para configurar el nodo de puerta de enlace"
Nodo de administración no principal	"Selecciona Iniciar recuperación para configurar un nodo de administración no principal"
Nodo de administración principal	"Configura el nodo de administración principal de sustitución"

Cómo el soporte técnico recupera un sitio StorageGRID

Si falla todo un sitio de StorageGRID o si fallan varios nodos de almacenamiento, tienes que ponerte en contacto con soporte técnico. Soporte técnico evaluará tu situación, desarrollará un plan de recuperación y luego recuperará los nodos o el sitio que fallaron de una manera que cumpla con tus objetivos empresariales, optimice el tiempo de recuperación y evite la pérdida innecesaria de datos.



La recuperación del sitio solo puede realizarla el soporte técnico.

Los sistemas StorageGRID son resistentes a una amplia variedad de fallos, y tú mismo puedes realizar con éxito muchos procedimientos de recuperación y mantenimiento. Sin embargo, es difícil crear un procedimiento de recuperación del sitio sencillo y generalizado porque los pasos detallados dependen de factores que son específicos de tu situación. Por ejemplo:

- **Tus objetivos empresariales:** tras la pérdida total de un sitio de StorageGRID, debes evaluar cuál es la

mejor forma de cumplir tus objetivos empresariales. Por ejemplo, ¿quieres reconstruir el sitio perdido en el mismo lugar? ¿Quieres reemplazar el sitio de StorageGRID perdido en una nueva ubicación? La situación de cada cliente es diferente, y tu plan de recuperación debe estar diseñado para abordar tus prioridades.

- **Naturaleza exacta del fallo:** Antes de iniciar la recuperación de un sitio, comprueba si hay algún nodo intacto en el sitio afectado o si algún nodo de almacenamiento contiene objetos recuperables. Si reconstruyes nodos o volúmenes de almacenamiento que contienen datos válidos, podría producirse una pérdida innecesaria de datos.
- **Políticas de ILM activas:** El número, el tipo y la ubicación de las copias de los objetos en tu grid están controlados por tus políticas de ILM activas. Los detalles de tus políticas de ILM pueden afectar la cantidad de datos recuperables, así como las técnicas específicas necesarias para la recuperación.



Si un sitio contiene la única copia de un objeto y el sitio se pierde, el objeto se pierde.

- **Consistencia del bucket (o contenedor):** la consistencia aplicada a un bucket (o contenedor) determina si StorageGRID replica íntegramente los metadatos del objeto en todos los nodos y sitios antes de indicar al cliente que la incorporación del objeto se ha realizado correctamente. Si el valor de consistencia permite la consistencia eventual, es posible que se hayan perdido algunos metadatos del objeto durante el fallo 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 tu procedimiento de recuperación pueden verse afectados por el hecho de que se estuvieran llevando a cabo procedimientos de mantenimiento en el momento del fallo o de que se hubieran realizado cambios recientes en tus políticas de ILM. El soporte técnico debe evaluar el historial reciente de tu grid, así como su situación actual, antes de iniciar la recuperación de un sitio.



La recuperación del sitio solo puede realizarla el soporte técnico.

Esta es una descripción general del proceso que soporte técnico utiliza para recuperar un sitio que ha fallado:

1. Soporte técnico:
 - a. Realiza una evaluación detallada del fallo.
 - b. Colabora contigo para analizar los objetivos de tu empresa.
 - c. Elabora un plan de recuperación adaptado a tu situación.
2. Si el nodo de administración principal ha fallado, el soporte técnico lo recupera.
3. El soporte técnico recupera todos los Storage Nodes siguiendo este esquema:
 - a. Sustituye el hardware o las máquinas virtuales del nodo de almacenamiento según sea necesario.
 - b. Restaura los metadatos del objeto en el sitio afectado por el fallo.
 - c. Restaura los datos de los objetos en los nodos de almacenamiento recuperados.



Se producirá una pérdida de datos si se utilizan los procedimientos de recuperación para un único nodo de almacenamiento fallido.



Cuando se produce un fallo en todo un sitio, el soporte técnico utiliza comandos especializados para restaurar correctamente los objetos y los metadatos de objetos.

4. El soporte técnico recupera otros nodos que han fallado.

Una vez recuperados los metadatos y los datos de los objetos, el soporte técnico sigue los procedimientos estándar para recuperar los nodos Gateway que hayan fallado o los nodos Admin no principales.

Información relacionada

["Decomisionar el sitio"](#)

Soluciones y recursos de StorageGRID

Ve a "[Soluciones y recursos de StorageGRID](#)" para aprender cómo probar y habilitar aplicaciones en tu entorno StorageGRID.

Cómo gestionar StorageGRID con NetApp Console

Ve a "[Gestión de StorageGRID usando la NetApp Console](#)" para aprender a gestionar tus sistemas StorageGRID desde NetApp Console mediante Grid Manager y utilizar los servicios de datos de NetApp Console para realizar copias de seguridad, tiering de datos y mucho más.

BlueXP ahora es NetApp Console

La NetApp Console, creada sobre la base mejorada y reestructurada de BlueXP, te ofrece una gestión centralizada del almacenamiento de NetApp y de los NetApp Data Services en entornos locales y de nube a nivel empresarial, proporcionando información en tiempo real, flujos de trabajo más rápidos y una administración simplificada, de forma muy segura y conforme a las normativas.

Para más detalles sobre lo que ha cambiado, consulta la "[Notas de la versión de NetApp Console](#)".

Avisos legales

Los avisos legales proporcionan acceso a declaraciones de derechos de autor, marcas registradas, patentes y más.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marcas registradas

NETAPP, el logotipo de NETAPP y las marcas que aparecen en la página de NetApp Trademarks 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

Una lista actual de patentes propiedad de NetApp se puede encontrar 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/)

Licencia de la API

Esta documentación no concede ninguna licencia ni otros derechos sobre la API de REST de StorageGRID S3. Cualquier uso o acceso a la API de REST de StorageGRID S3 requiere y está sujeto a un contrato de licencia independiente con NetApp.

Código abierto

Los archivos de aviso proporcionan información sobre los derechos de autor y las licencias de terceros utilizadas en el software NetApp.

https://library.netapp.com/ecm/ecm_download_file/ECMLP3351268

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.