



# **Gestione servicios de plataformas S3**

StorageGRID software

NetApp

February 12, 2026

# Tabla de contenidos

- Gestione servicios de plataformas S3 . . . . . 1
  - Servicios de plataforma S3 . . . . . 1
    - Descripción general y consideraciones de los servicios de la plataforma . . . . . 1
    - Conozca el servicio de replicación de CloudMirror . . . . . 4
    - Comprender las notificaciones para bloques . . . . . 6
    - Comprender el servicio de integración de búsquedas . . . . . 7
  - Gestione los extremos de los servicios de plataforma . . . . . 8
    - Configure los extremos de servicios de la plataforma . . . . . 8
    - Especifique URN para el extremo de servicios de la plataforma . . . . . 9
    - Cree un extremo de servicios de plataforma . . . . . 12
    - Probar la conexión para el extremo de servicios de la plataforma . . . . . 18
    - Editar extremo de servicios de plataforma . . . . . 19
    - Eliminar extremo de servicios de plataforma . . . . . 20
    - Solucionar errores de extremos de servicios de plataforma . . . . . 20
  - Configure la replicación de CloudMirror . . . . . 22
  - Configure las notificaciones de eventos . . . . . 24
  - Configure el servicio de integración de búsqueda . . . . . 28
    - Ejemplo: Configuración de notificación de metadatos que se aplica a todos los objetos . . . . . 31
    - Ejemplo: Configuración de notificación de metadatos con dos reglas . . . . . 31
    - Formato de notificación de metadatos . . . . . 32

# Gestione servicios de plataformas S3

## Servicios de plataforma S3

### Descripción general y consideraciones de los servicios de la plataforma

Antes de implementar servicios de plataforma, revise la descripción general y las consideraciones para usar estos servicios.

Para obtener información sobre S3, consulte ["USE LA API DE REST DE S3"](#).

### Descripción general de los servicios de la plataforma

Los servicios de plataforma de StorageGRID pueden ayudarte a implementar una estrategia de cloud híbrido permitiéndote enviar notificaciones de eventos y copias de objetos S3 y metadatos de objetos a destinos externos.

Puesto que la ubicación objetivo de los servicios de la plataforma suele ser externa a la puesta en marcha de StorageGRID, los servicios de plataforma le proporcionan la potencia y la flexibilidad que se obtiene al utilizar recursos de almacenamiento externo, servicios de notificación y servicios de búsqueda o análisis para sus datos.

Se puede configurar cualquier combinación de servicios de plataforma para un único bloque de S3. Por ejemplo, puede configurar tanto el ["Servicio CloudMirror"](#) como ["notificaciones"](#) en un bucket de StorageGRID S3 para que pueda reflejar objetos específicos en Amazon Simple Storage Service (S3), mientras envía una notificación sobre cada objeto a una aplicación de supervisión de terceros para ayudarle a realizar un seguimiento de sus gastos de AWS.



Un administrador de StorageGRID debe habilitar el uso de servicios de plataforma para cada cuenta de inquilino mediante el Administrador de grid o la API de gestión de grid.

### Cómo se configuran los servicios de plataforma

Los servicios de plataforma se comunican con puntos finales externos que usted configura mediante el ["Administrador de inquilinos"](#) o el ["API de gestión de inquilinos"](#). Cada punto final representa un destino externo, como un bucket S3 de StorageGRID, un bucket de Amazon Web Services, un tema de Amazon SNS, un punto final de webhook o un clúster de Elasticsearch alojado localmente, en AWS o en otro lugar.

Después de crear un punto final externo, puede activar un servicio de plataforma para un bloque agregando configuración XML al bloque. La configuración XML identifica los objetos en los que debe actuar el bloque, la acción que debe tomar el bloque y el extremo que el bloque debe utilizar para el servicio.

Debe agregar configuraciones XML independientes para cada servicio de plataforma que desee configurar. Por ejemplo:

- Si desea que todos los objetos cuyas claves comiencen con `/images` se repliquen en un bucket de Amazon S3, debe agregar una configuración de replicación al bucket de origen.
- Si también desea enviar notificaciones cuando estos objetos están almacenados en el bloque, debe añadir una configuración de notificaciones.
- Si desea indexar los metadatos de estos objetos, debe agregar la configuración de notificación de metadatos que se utiliza para implementar la integración de búsqueda.

El formato de la configuración XML está regido por las API DE REST de S3 que se usan para implementar los servicios de plataforma StorageGRID:

Servicio de plataforma	API REST DE S3	Consulte
Replicación de CloudMirror	<ul style="list-style-type: none"> <li>• GetBucketReplication</li> <li>• PutBucketReplication</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">"Replicación de CloudMirror"</a></li> <li>• <a href="#">"Operaciones en bloques"</a></li> </ul>
Notificaciones	<ul style="list-style-type: none"> <li>• GetBucketNotificationConfiguration</li> <li>• PutBucketNotificationConfiguration</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">"Notificaciones"</a></li> <li>• <a href="#">"Operaciones en bloques"</a></li> </ul>
Integración de búsqueda	<ul style="list-style-type: none"> <li>• OBTENGA la configuración de notificación de metadatos del bloque de datos</li> <li>• Configuración de notificaciones de metadatos de PUT Bucket</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">"Integración de búsqueda"</a></li> <li>• <a href="#">"Operaciones personalizadas de StorageGRID"</a></li> </ul>

### Consideraciones sobre el uso de servicios de plataforma

Consideración	Detalles
Supervisión del extremo de destino	<p>Debe supervisar la disponibilidad de cada extremo de destino. Si se pierde la conectividad con el extremo de destino durante un periodo de tiempo prolongado y existe una gran acumulación de solicitudes, se producirá un error en las solicitudes de cliente adicionales (como solicitudes PUT) a StorageGRID. Debe volver a intentar estas solicitudes con errores cuando se pueda acceder al extremo.</p>
Limitación de punto final de destino	<p>El software StorageGRID puede reducir las solicitudes entrantes de S3 para un bloque si la velocidad a la que se envían las solicitudes supera la velocidad a la que el extremo de destino puede recibir las solicitudes. La limitación sólo se produce cuando hay una acumulación de solicitudes que están a la espera de ser enviadas al extremo de destino.</p> <p>El único efecto visible es que las solicitudes entrantes de S3 tardarán más en ejecutarse. Si empieza a detectar un rendimiento significativamente más lento, debe reducir la tasa de procesamiento o utilizar un extremo con mayor capacidad. Si la acumulación de solicitudes sigue creciendo, las operaciones de S3 del cliente (como SOLICITUDES PUT) fallarán en el futuro.</p> <p>Las solicitudes de CloudMirror tienen más probabilidades de que se vean afectadas por el rendimiento del extremo de destino, ya que estas solicitudes suelen requerir más transferencia de datos que las solicitudes de integración de búsqueda o notificación de eventos.</p>

Consideración	Detalles
Solicitud de garantías	<p>StorageGRID garantiza la realización de pedidos de operaciones en un objeto dentro de un sitio. Siempre que todas las operaciones contra un objeto se encuentren en el mismo sitio, el estado del objeto final (para replicación) será siempre igual al estado en StorageGRID.</p> <p>StorageGRID hace todo un esfuerzo por intentar solicitar solicitudes cuando se realizan operaciones en todos los sitios de StorageGRID. Por ejemplo, si escribe un objeto inicialmente en el sitio A y después sobrescribe el mismo objeto en el sitio B, no se garantiza que el objeto final replicado por CloudMirror en el bloque de destino sea el más nuevo.</p>
Eliminaciones de objetos condicionados por ILM	<p>Para coincidir con el comportamiento de eliminación de AWS CRR y Amazon Simple Notification Service, CloudMirror y las solicitudes de notificación de eventos no se envían cuando se elimina un objeto del bloque de origen debido a las reglas de gestión de la vida útil de la información de StorageGRID. Por ejemplo, no se envían solicitudes de notificaciones de eventos o CloudMirror si una regla de ILM elimina un objeto después de 14 días.</p> <p>Por el contrario, las solicitudes de integración de búsqueda se envían cuando los objetos se eliminan debido a ILM.</p>
Utilizando puntos finales Kafka	<p>Para puntos finales Kafka, TLS mutuo no es compatible. Como resultado, si se ha <code>ssl.client.auth</code> establecido en <code>required</code> la configuración de su broker Kafka, puede causar problemas de configuración de punto final Kafka.</p> <p>La autenticación de los puntos finales de Kafka utiliza los siguientes tipos de autenticación. Estos tipos son diferentes de los utilizados para la autenticación de otros puntos finales, como Amazon SNS, y requieren credenciales de nombre de usuario y contraseña.</p> <ul style="list-style-type: none"> <li>• SASL/PLAIN</li> <li>• SASL/SCRAM-SHA-256</li> <li>• SASL/SCRAM-SHA-512</li> </ul> <p><b>Nota:</b> Los ajustes de proxy de almacenamiento configurados no se aplican a los endpoints de servicios de la plataforma Kafka.</p>

### Consideraciones sobre el uso del servicio de replicación de CloudMirror

Consideración	Detalles
Estado de replicación	StorageGRID no admite <code>x-amz-replication-status</code> el encabezado.

Consideración	Detalles
Tamaño del objeto	<p>El tamaño máximo de los objetos que se pueden replicar en un bloque de destino mediante el servicio de replicación de CloudMirror es de 5 TiB, que es el mismo que el tamaño máximo de objeto <i>admitido</i>.</p> <p><b>Nota:</b> El tamaño máximo <i>Recommended</i> para una sola operación PutObject es de 5 GiB (5.368.709.120 bytes). Si tiene objetos que sean mayores de 5 GiB, utilice la carga de varias partes en su lugar.</p>
Versiones de bloques e ID de versión	<p>Si el bloque de S3 de origen de StorageGRID tiene habilitado el control de versiones, también debe habilitar el control de versiones para el bloque de destino.</p> <p>Al usar el control de versiones, tenga en cuenta que el orden de las versiones de objetos en el bloque de destino es el mejor esfuerzo y no está garantizado por el servicio CloudMirror, debido a las limitaciones del protocolo S3.</p> <p><b>Nota:</b> Los ID de versión para el depósito de origen en StorageGRID no están relacionados con los ID de versión para el depósito de destino.</p>
Etiquetado para versiones de objetos	<p>El servicio CloudMirror no replica ninguna solicitud PutObjectTagging o DeleteObjectTagging que proporcione un ID de versión, debido a las limitaciones del protocolo S3. Debido a que los ID de versión para el origen y el destino no están relacionados, no hay forma de garantizar que se replique una actualización de etiqueta para un ID de versión específico.</p> <p>Por el contrario, el servicio CloudMirror replica las solicitudes PutObjectTagging o las solicitudes DeleteObjectTagging que no especifican un ID de versión. Estas solicitudes actualizan las etiquetas de la clave más reciente (o la versión más reciente si el bloque está versionado). También se replican búsquedas normales con etiquetas (no actualizaciones de etiquetado).</p>
Cargas y valores de varias partes ETag	<p>Cuando se crea un mirroring de objetos cargados con una carga de varias partes, el servicio CloudMirror no conserva las piezas. Como resultado, el ETag valor del objeto reflejado será diferente al ETag valor del objeto original.</p>
Objetos cifrados con SSE-C (cifrado en el lado del servidor con claves proporcionadas por el cliente)	<p>El servicio CloudMirror no admite objetos cifrados con SSE-C. Si intenta ingerir un objeto en el depósito de origen para la replicación de CloudMirror y la solicitud incluye los encabezados de solicitud SSE-C, la operación falla.</p>
Bloque con S3 Object Lock habilitado	<p>La replicación no es compatible con buckets de origen o destino con el bloqueo de objetos S3 habilitado.</p>

## Conozca el servicio de replicación de CloudMirror

Puede habilitar la replicación de CloudMirror para un bloque de S3 si desea que StorageGRID replique los objetos especificados agregados al bloque en uno o más bloques de destino externos.

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



La replicación de CloudMirror no es compatible si el bloque de origen tiene la función S3 Object Lock habilitada.

## CloudMirror y ILM

La replicación de CloudMirror funciona independientemente de las políticas de gestión de la vida útil de la información activas del grid. El servicio CloudMirror replica los objetos cuando se almacenan en el bloque de origen y los envía al Lo antes posible. de bloque de destino. La entrega de objetos replicados se activa cuando la ingesta de objetos se realiza correctamente.

## CloudMirror y replicación entre grid

La replicación de CloudMirror tiene similitudes y diferencias importantes con la función de replicación entre grid. Consulte "[Compare la replicación entre grid y la replicación de CloudMirror](#)".

## CloudMirror y bloques de S3

La replicación de CloudMirror suele configurarse para utilizar un bloque de S3 externo como destino. Sin embargo, también puede configurar la replicación para que utilice otra implementación de StorageGRID o cualquier servicio compatible con S3.

## Cucharones existentes

Cuando habilita la replicación de CloudMirror para un bloque existente, solo se replican los objetos nuevos agregados a ese bloque. Todos los objetos existentes del bloque no se replican. Para forzar la replicación de objetos existentes, puede actualizar los metadatos del objeto existente ejecutando una copia de objeto.



Si utiliza la replicación de CloudMirror para copiar objetos a un destino de Amazon S3, tenga en cuenta que Amazon S3 limita el tamaño de los metadatos definidos por el usuario dentro de cada encabezado de solicitud PUT a 2 KB. Si un objeto tiene metadatos definidos por el usuario mayores de 2 KB, ese objeto no se replicará.

## Varios cubos de destino

Para replicar objetos de un solo depósito en varios depósitos de destino, especifique el destino de cada regla en el XML de configuración de replicación. No puede replicar un objeto en más de un bloque a la vez.

## Bloques con versiones o sin versiones

Puede configurar la replicación de CloudMirror en bloques con versiones o sin versiones. Los cubos de destino se pueden versionar o no versionar. Puede utilizar cualquier combinación de cubos con versiones y sin versiones. Por ejemplo, puede especificar un bloque con versiones como destino para un bloque de origen sin versiones o viceversa. También puede replicar entre cubos sin versiones.

## Eliminación, bucles de replicación y eventos

### Comportamiento de eliminación

Es el mismo comportamiento que el comportamiento de eliminación del servicio Amazon S3, Replicación entre regiones (CRR). Al eliminar un objeto en un bloque de origen nunca se elimina un objeto replicado en el destino. Si se van a crear versiones de los cubos de origen y de destino, se replica el marcador de borrado. Si el depósito de destino no tiene versiones, al suprimir un objeto del depósito de origen no se replica el marcador de eliminación en el depósito de destino ni se elimina el objeto de destino.

## Protección de bucles de replicación

A medida que los objetos se replican en el bloque de destino, StorageGRID los marca como «réplicas». Un bucket de StorageGRID de destino no replicará objetos marcados como réplicas de nuevo, lo que le protegerá de bucles de replicación accidentales. Esta marca de réplica es interna en StorageGRID y no le impide aprovechar AWS CRR cuando use un bucket de Amazon S3 como destino.



El encabezado personalizado utilizado para marcar una réplica es `x-ntap-sg-replica`. Esta Marca evita una duplicación en cascada. StorageGRID sí admite un CloudMirror bidireccional entre dos grids.

## Eventos en el bloque de destino

La singularidad y el orden de los eventos en el cubo de destino no están garantizados. Puede que más de una copia idéntica de un objeto de origen se proporcione en el destino como resultado de las operaciones realizadas para garantizar un éxito en la entrega. En raras ocasiones, cuando se actualiza el mismo objeto de forma simultánea desde dos o más sitios StorageGRID distintos, es posible que la ordenación de las operaciones en el bloque de destino no coincida con la ordenación de eventos en el bloque de origen.

## Comprender las notificaciones para bloques

Puede habilitar la notificación de eventos para un bucket S3 si desea que StorageGRID envíe notificaciones sobre eventos específicos a un clúster de Kafka de destino, un punto final de webhook o Amazon Simple Notification Service.

Por ejemplo, podría configurar que se envíen alertas a administradores acerca de cada objeto agregado a un bloque, donde los objetos representan los archivos de registro asociados a un evento crítico del sistema.

Las notificaciones de eventos se crean en el bloque de origen tal y como se especifica en la configuración de notificación y se envían al destino. Si un evento asociado con un objeto se realiza correctamente, se crea una notificación sobre ese evento y se pone en cola para su entrega.

La singularidad y el orden de las notificaciones no están garantizados. Como resultado de las operaciones realizadas para garantizar el éxito en la entrega, se podría enviar más de una notificación de un evento al destino. Además, como la entrega es asíncrona, no se garantiza que la ordenación del tiempo de las notificaciones en el destino coincida con la ordenación de eventos del bloque de origen, especialmente en las operaciones que se originan en diferentes sitios de StorageGRID. Puede utilizar la `sequencer` clave en el mensaje de 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 evento:
  - S3:ObjetoCreado:
  - S3:ObjectCreated:Put
  - S3:ObjectCreated:Post
  - S3:ObjectCreated:Copiar
  - S3:ObjectCreated:CompleteMultipartUpload
  - S3:ObjectRemoved:
  - S3:ObjectRemoved:Eliminar
  - S3:ObjectRemoved>DeleteMarkerCreated



- S3:ObjectRestore:Post

- Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar, pero no incluyen algunas claves ni utilizan valores específicos para otros, como se muestra en la tabla:

Nombre de clave	Valor de StorageGRID
EventSource	sgws:s3
AwsRegion	<i>no incluido</i>
x-amz-id-2	<i>no incluido</i>
arn	urn:sgws:s3:::bucket_name

## Comprender el servicio de integración de búsquedas

Puede habilitar la integración de búsqueda para un bloque de S3 si desea usar un servicio de búsqueda y análisis de datos externo para sus metadatos de objetos.

El servicio de integración de búsqueda es un servicio StorageGRID personalizado que envía de forma automática y asíncrona metadatos de objetos S3 a un extremo de destino cada vez que se crea o se elimina un objeto, o se actualizan sus metadatos o etiquetas. A continuación, puede usar herramientas sofisticadas de búsqueda, análisis de datos, visualización o aprendizaje automático que proporciona el servicio de destino para buscar, analizar y obtener información de sus datos de objetos.

Por ejemplo, podría configurar sus bloques para que envíen metadatos de objetos S3 a un servicio Elasticsearch remoto. Luego, podría usar Elasticsearch para realizar búsquedas en los bloques y ejecutar análisis sofisticados de los patrones presentes en los metadatos de objetos.

Aunque la integración de Elasticsearch se puede configurar en un bucket con S3 Object Lock habilitado, los metadatos de S3 Object Lock (incluidos el estado Retain Until Date y Legal hold) de los objetos no se incluirán en los metadatos enviados a Elasticsearch.



Debido a que el servicio de integración de búsqueda hace que los metadatos del objeto se envíen a un destino, su configuración XML se conoce como “*metadata* notification configuration XML”. Este XML de configuración es diferente del XML de configuración de notificación utilizado para activar las notificaciones *event*.

## Integración de búsqueda y bloques de S3

Puede activar el servicio de integración de búsqueda para cualquier bloque con versiones o sin versiones. La integración de búsqueda se configura asociando el XML de configuración de notificación de metadatos al bloque que especifica los objetos en los que actuar y el destino de los metadatos del objeto.

Las notificaciones de metadatos se generan en forma de un documento JSON denominado con el nombre del bloque, el nombre del objeto y el ID de versión, si corresponde. Cada notificación de metadatos contiene un conjunto estándar de metadatos del sistema para el objeto, además de todas las etiquetas del objeto y los metadatos del usuario.



Para las etiquetas y los metadatos de usuario, StorageGRID pasa las fechas y los números a Elasticsearch como cadenas o como notificaciones de eventos S3. Para configurar Elasticsearch para interpretar estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para la asignación dinámica de campos y para asignar formatos de fecha. Debe habilitar las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Después de indexar un documento, no puede editar los tipos de campo del documento en el índice.

## Buscar notificaciones

Las notificaciones de metadatos se generan y se ponen en cola para su entrega siempre que:

- Se crea un objeto.
- Se elimina un objeto, incluso cuando se eliminan objetos como resultado del funcionamiento de la política de ILM de la cuadrícula.
- Los metadatos o las etiquetas de los objetos son añadidos, actualizados o eliminados. El conjunto completo de metadatos y etiquetas se envía siempre al momento de la actualización, no sólo los valores modificados.

Después de agregar XML de configuración de notificación de metadatos a un bloque, se envían notificaciones para los objetos nuevos que cree y para los objetos que modifique mediante la actualización de sus datos, metadatos de usuario o etiquetas. Sin embargo, no se envían notificaciones de ningún objeto que ya estuviera en el bloque. Para garantizar que los metadatos de objeto de todos los objetos del bloque se envíen al destino, debe realizar una de las siguientes acciones:

- Configure el servicio de integración de búsqueda inmediatamente después de crear el bloque y antes de agregar ningún objeto.
- Realice una acción en todos los objetos que ya están en el bloque que activará un mensaje de notificación de metadatos que se enviará al destino.

## Servicio de integración de búsqueda y Elasticsearch

El servicio de integración de búsqueda StorageGRID admite un clúster de Elasticsearch como destino. Al igual que con los demás servicios de plataforma, el destino se especifica en el extremo cuyo URN se utiliza en el XML de configuración del servicio. Utilice el ["Herramienta de matriz de interoperabilidad de NetApp"](#) para determinar las versiones compatibles de Elasticsearch.

# Gestione los extremos de los servicios de plataforma

## Configure los extremos de servicios de la plataforma

Para poder configurar un servicio de plataforma para un bloque, debe configurar al menos un extremo para que sea el destino del servicio de plataforma.

El acceso a servicios de la plataforma está habilitado por inquilino por un administrador de StorageGRID. Para crear o utilizar un punto final de servicios de plataforma, debe ser un usuario inquilino con permiso de gestión de puntos finales o acceso raíz, en una cuadrícula cuya red se ha configurado para permitir que los nodos de almacenamiento accedan a recursos de punto final externo. Para un solo inquilino, puede configurar un máximo de 500 puntos finales de servicios de plataforma. Si desea obtener más información, póngase en contacto con el administrador de StorageGRID.

## ¿Qué es un extremo de servicios de plataforma?

Un punto final de servicios de plataforma especifica la información que StorageGRID necesita para acceder al destino externo.

Por ejemplo, si desea replicar objetos de un bucket de StorageGRID en un bucket de Amazon S3, cree un punto final de servicios de plataforma que incluya la información y las credenciales que necesita StorageGRID para acceder al bucket de destino en Amazon.

Cada tipo de servicio de plataforma requiere su propio extremo, por lo que debe configurar al menos un extremo para cada servicio de plataforma que tenga previsto utilizar. Después de definir un extremo de servicios de plataforma, se utiliza URN del extremo como destino en el XML de configuración utilizado para habilitar el servicio.

Puede utilizar el mismo extremo que el destino para más de un bloque de origen. Por ejemplo, se pueden configurar varios bloques de origen para que envíen metadatos de objetos al mismo extremo de integración de búsqueda, de modo que se puedan realizar búsquedas en varios bloques. También puede configurar un depósito de origen para que utilice más de un extremo como destino, lo que permite hacer cosas como enviar notificaciones sobre la creación de objetos a un tema de Amazon Simple Notification Service (Amazon SNS) y notificaciones sobre la eliminación de objetos a un segundo tema de Amazon SNS.

### Extremos para la replicación de CloudMirror

StorageGRID admite extremos de replicación que representan bloques de S3. Estos bloques se pueden alojar en Amazon Web Services, la misma puesta en marcha de StorageGRID remota o en otro servicio.

### Extremos para notificaciones

StorageGRID admite puntos finales de Amazon SNS, Kafka y webhook. Los puntos finales de Simple Queue Service (SQS) y AWS Lambda no son compatibles.

Para los puntos finales de Kafka, no se admite TLS mutuo. Como resultado, si tienes `ssl.client.auth` empezar a `required` en la configuración de su agente de Kafka, podría causar problemas de configuración del punto final de Kafka.

### Extremos del servicio de integración de búsqueda

StorageGRID admite extremos de integración de búsqueda que representan clústeres de Elasticsearch. Estos clústeres de Elasticsearch pueden estar en un centro de datos local o alojados en un cloud de AWS o en otro lugar.

El extremo de integración de búsqueda hace referencia a un índice y un tipo específicos de Elasticsearch. Debe crear el índice en Elasticsearch antes de crear el extremo en StorageGRID o se producirá un error en la creación del extremo. No es necesario crear el tipo antes de crear el punto final. StorageGRID creará el tipo si es necesario al enviar metadatos de objetos al extremo.

### Información relacionada

["Administre StorageGRID"](#)

## Especifique URN para el extremo de servicios de la plataforma

Al crear un extremo de servicios de plataforma, debe especificar un nombre de recurso único (URN). Utilizará el URN para hacer referencia al punto final cuando cree un XML de configuración para el servicio de plataforma. El URN de cada extremo debe ser único.

StorageGRID valida los extremos de los servicios de la plataforma a medida que se crean. Antes de crear un extremo de servicios de plataforma, confirme que el recurso especificado en el extremo existe y que se puede alcanzar.

## URN elementos

El URN para un punto final de servicios de plataforma debe empezar por `arn:aws` o `urn:mystore`, de la siguiente manera:

- Si el servicio está alojado en Amazon Web Services (AWS), utilice `arn:aws`
- Si el servicio está alojado en Google Cloud Platform (GCP), utilice `arn:aws`
- Si el servicio está alojado localmente, utilice `urn:mystore`

Por ejemplo, si especifica el URN para un punto final de CloudMirror alojado en StorageGRID, el URN puede empezar por `urn:sgws`.

El siguiente elemento de URN especifica el tipo de servicio de plataforma, como se indica a continuación:

Servicio	Tipo
Replicación de CloudMirror	s3
Notificaciones	sns, kafka , o webhook
Integración de búsqueda	es

Por ejemplo, para seguir especificando el URN para un punto final de CloudMirror alojado en StorageGRID, debe agregar `s3` a `Get urn:sgws:s3`.

Para la mayoría de los puntos finales, el elemento final del URN identifica el recurso de destino específico en el URI de destino, por ejemplo, `sns-topic-name`.

Para los puntos finales de webhook, el recurso de destino es el propio URI de destino.

Servicio	Recurso específico
Replicación de CloudMirror	bucket-name
Notificaciones	sns-topic-name o. kafka-topic-name  <b>Nota:</b> Para los puntos finales de webhook, el elemento final del URN puede ser cualquier cadena, siempre que el URN del punto final sea único.
Integración de búsqueda	domain-name/index-name/type-name  <b>Nota:</b> Si el clúster Elasticsearch está <b>no</b> configurado para crear índices automáticamente, debe crear el índice manualmente antes de crear el punto final.

## Urnas para servicios alojados en AWS y GCP

Para las entidades AWS y GCP, el URN completo es un AWS ARN válido. Por ejemplo:

- Replicación de CloudMirror:

```
arn:aws:s3:::bucket-name
```

- Notificaciones:

```
arn:aws:sns:region:account-id:topic-name
```

- Integración de búsqueda:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```



Para un punto final de integración de búsqueda de AWS, `domain-name` debe incluir la cadena literal `domain/`, como se muestra aquí.

## Servicios alojados localmente

Al usar servicios alojados localmente en lugar de servicios de cloud, puede especificar el URN de cualquier forma que cree una URN válida y única, siempre y cuando URN incluya los elementos necesarios en la tercera y última posición. Puede dejar los elementos indicados por opcional en blanco o puede especificarlos de cualquier forma que le ayude a identificar el recurso y hacer que el URN sea único. Por ejemplo:

- Replicación de CloudMirror:

```
urn:mysite:s3:optional:optional:bucket-name
```

Para un extremo de CloudMirror alojado en StorageGRID, se puede especificar un URN válido que comience por `urn:sgws:`

```
urn:sgws:s3:optional:optional:bucket-name
```

- Notificaciones:

Especifique un punto final de Amazon Simple Notification Service:

```
urn:mysite:sns:optional:optional:sns-topic-name
```

Especifique un punto final Kafka:

```
urn:mysite:kafka:optional:optional:kafka-topic-name
```

Especifique un punto final 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 puntos finales de integración de búsqueda alojados localmente, el `domain-name` elemento puede ser cualquier cadena siempre que el URN del punto final sea único.

## Cree un extremo de servicios de plataforma

Debe crear al menos un extremo del tipo correcto para poder habilitar un servicio de plataforma.

### Antes de empezar

- Ha iniciado sesión en el gestor de inquilinos mediante un ["navegador web compatible"](#).
- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Pertenece a un grupo de usuarios que tiene el ["Gestionar puntos finales o permisos de acceso raíz"](#).
- Se ha creado el recurso al que hace referencia el punto final de servicios de la plataforma:
  - Replicación de CloudMirror: Bloque de S3
  - Notificación de eventos: tema de Amazon Simple Notification Service (Amazon SNS), tema de Kafka o punto final de webhook
  - Notificación de búsqueda: índice de Elasticsearch, si el clúster de destino no está configurado para crear índices automáticamente.
- Tiene la información sobre el recurso de destino:
  - Host y puerto para el Identificador uniforme de recursos (URI)



Si piensa utilizar un bloque alojado en un sistema StorageGRID como extremo para la replicación de CloudMirror, póngase en contacto con el administrador de grid para determinar los valores que debe introducir.

- Nombre del recurso único (URN)

["Especifique URN para el extremo de servicios de la plataforma"](#)

- Credenciales de autenticación (si es necesario):

### Buscar puntos finales de integración

Para los puntos finales de integración de búsqueda, puede utilizar las siguientes credenciales:

- Clave de acceso: ID de clave de acceso y clave de acceso secreta
- Basic HTTP: Nombre de usuario y contraseña

### Extremos de replicación de CloudMirror

En el caso de los extremos de replicación de CloudMirror, se pueden usar las siguientes credenciales:

- Clave de acceso: ID de clave de acceso y clave de acceso secreta
- CAP (C2S Access Portal): URL de credenciales temporales, certificados de servidor y de cliente, claves de cliente y una contraseña de clave privada de cliente opcional.

### Extremos de Amazon SNS

Para los extremos de Amazon SNS, puede usar las siguientes credenciales:

- Clave de acceso: ID de clave de acceso y clave de acceso secreta

### Puntos finales de Kafka

Para los puntos finales de Kafka, puede utilizar las siguientes credenciales:

- SASL/PLAIN: Nombre de usuario y contraseña
- SASL/SCRAM-SHA-256: Nombre de usuario y contraseña
- SASL/SCRAM-SHA-512: Nombre de usuario y contraseña

- Certificado de seguridad (si se requiere verificación del certificado)

- Si las funciones de seguridad de Elasticsearch están activadas, tiene el privilegio de clúster de supervisión para las pruebas de conectividad y el privilegio WRITE INDEX o los privilegios INDEX y DELETE INDEX para las actualizaciones de documentos.

## Pasos

1. Seleccione **STORAGE (S3) > Platform Services Endpoints**. Aparece la página de extremos de servicios de plataforma.
2. Seleccione **Crear punto final**.
3. Introduzca un nombre para mostrar para describir brevemente el extremo y su propósito.

El tipo de servicio de plataforma que admite el punto final se muestra junto al nombre del punto final cuando aparece en la página Puntos finales, por lo que no es necesario incluir esa información en el nombre.

4. En el campo **URI**, especifique el Identificador de recursos único (URI) del extremo.

Utilice uno de los siguientes formatos:

```
https://host:port  
http://host:port
```

Si no especifica un puerto, se utilizan los siguientes puertos predeterminados:

- Puerto 443 para URI HTTPS y puerto 80 para URI HTTP (mayoría de extremos)
- Puerto 9092 para URI HTTPS y HTTP (solo puntos finales Kafka)

Por ejemplo, el URI para un bloque alojado en StorageGRID podría ser:

```
https://s3.example.com:10443
```

En este ejemplo, `s3.example.com` representa la entrada DNS para la IP virtual (VIP) del grupo de alta disponibilidad (HA) de StorageGRID y `10443` representa el puerto definido en el extremo del equilibrador de carga.



Siempre que sea posible, debe conectarse a un grupo de alta disponibilidad de nodos de equilibrio de carga para evitar un único punto de error.

Del mismo modo, el URI para un bloque alojado en AWS podría ser:

```
https://s3-aws-region.amazonaws.com
```



Si el punto final se utiliza para el servicio de replicación de CloudMirror, no incluya el nombre del bloque en el URI. Incluye el nombre de bloque en el campo **URN**.

5. Introduzca el nombre de recurso único (URN) para el extremo.



No puede cambiar el URN de un punto final después de crear el punto final.

6. Seleccione **continuar**.

7. Seleccione un valor para **Tipo de autenticación**.



Si desea autenticación para los puntos finales del webhook, configure la Seguridad de la capa de transporte mutua (mTLS) en [Paso 9](#).



### Buscar puntos finales de integración

Introduzca o cargue las credenciales para un punto final de integración de búsqueda.

Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Proporciona acceso anónimo al destino. Solo funciona para extremos con seguridad deshabilitada.	Sin autenticación.
Clave de acceso	Usa credenciales de estilo AWS para autenticar conexiones con el destino.	<ul style="list-style-type: none"><li>• ID de clave de acceso</li><li>• Clave de acceso secreta</li></ul>
HTTP básico	Utiliza un nombre de usuario y una contraseña para autenticar las conexiones al destino.	<ul style="list-style-type: none"><li>• Nombre de usuario</li><li>• Contraseña</li></ul>

### Extremos de replicación de CloudMirror

Introduzca o cargue las credenciales para un extremo de replicación de CloudMirror.

Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Proporciona acceso anónimo al destino. Solo funciona para extremos con seguridad deshabilitada.	Sin autenticación.
Clave de acceso	Usa credenciales de estilo AWS para autenticar conexiones con el destino.	<ul style="list-style-type: none"><li>• ID de clave de acceso</li><li>• Clave de acceso secreta</li></ul>
CAP (Portal de acceso C2S)	Usa certificados y claves para autenticar las conexiones al destino.	<ul style="list-style-type: none"><li>• URL de credenciales temporales</li><li>• Certificado de CA de servidor (carga de archivo PEM)</li><li>• Certificado de cliente (carga de archivo PEM)</li><li>• Clave privada de cliente (carga de archivo PEM, formato cifrado OpenSSL o formato de clave privada no cifrado)</li><li>• Contraseña de clave privada de cliente (opcional)</li></ul>

### Extremos de Amazon SNS

Introduzca o cargue las credenciales para un extremo de Amazon SNS.

Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Proporciona acceso anónimo al destino. Solo funciona para extremos con seguridad deshabilitada.	Sin autenticación.
Clave de acceso	Usa credenciales de estilo AWS para autenticar conexiones con el destino.	<ul style="list-style-type: none"><li>• ID de clave de acceso</li><li>• Clave de acceso secreta</li></ul>

#### Puntos finales de Kafka

Introduzca o cargue las credenciales para un punto final de Kafka.

Las credenciales que proporcione deben tener permisos de escritura para el recurso de destino.

Tipo de autenticación	Descripción	Credenciales
Anónimo	Proporciona acceso anónimo al destino. Solo funciona para extremos con seguridad deshabilitada.	Sin autenticación.
SASL/PLAIN	Utiliza un nombre de usuario y una contraseña con texto sin formato para autenticar las conexiones al destino.	<ul style="list-style-type: none"><li>• Nombre de usuario</li><li>• Contraseña</li></ul>
SASL/SCRAM-SHA-256	Utiliza un nombre de usuario y una contraseña mediante un protocolo de respuesta de desafío y hash SHA-256 para autenticar las conexiones al destino.	<ul style="list-style-type: none"><li>• Nombre de usuario</li><li>• Contraseña</li></ul>
SASL/SCRAM-SHA-512	Utiliza un nombre de usuario y una contraseña mediante un protocolo de respuesta de desafío y hash SHA-512 para autenticar las conexiones al destino.	<ul style="list-style-type: none"><li>• Nombre de usuario</li><li>• Contraseña</li></ul>

Seleccione **Usar la autenticación de delegación tomada** si el nombre de usuario y la contraseña se derivan de un token de delegación que se obtuvo de un clúster de Kafka.

8. Seleccione **continuar**.

9. Seleccione un botón de opción para **Verificar certificados** para elegir cómo se verifica la conexión TLS al punto final.

### La mayoría de los puntos finales

Verifique la conexión TLS para la integración de búsqueda, la replicación de CloudMirror, Amazon SNS o los puntos finales de Kafka.

Tipo de verificación del certificado	Descripción
TLS	Valida el certificado del servidor para conexiones TLS al recurso del punto final.
Desactivado	La verificación del certificado está deshabilitada. Esta opción no es segura.
Utilizar certificado de CA personalizado	El certificado CA personalizado se utiliza para verificar la identidad del servidor cuando se conecta al punto final.
Utilizar certificado de CA del sistema operativo	Utilice el certificado de CA de cuadrícula predeterminado instalado en el sistema operativo para asegurar las conexiones.

### Solo puntos finales de webhook

Verificar la conexión TLS para los puntos finales del webhook.

Tipo de verificación del certificado	Descripción
TLS	Valida el certificado del servidor para conexiones TLS al recurso del punto final.
mTLS	Valida los certificados de cliente y servidor para conexiones TLS mutuas al recurso del punto final.
Desactivado	La verificación del certificado está deshabilitada. Esta opción no es segura.
Utilizar certificado de CA personalizado	El certificado CA personalizado se utiliza para verificar la identidad del servidor cuando se conecta al punto final.

Cuando selecciona **mTLS**, estas opciones estarán disponibles.

Tipo de verificación del certificado	Descripción
No verificar el certificado del servidor	Deshabilita 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 cuando se conecta al punto final.

Tipo de verificación del certificado	Descripción
Clave privada del cliente	La clave privada para el certificado del cliente. Si está encriptado, debe utilizar el formato tradicional PKCS #1 (el formato PKCS #8 no es compatible).
Frase de 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, déjelo en blanco.

#### 10. Seleccione **probar y crear punto final**.

- Aparece un mensaje de éxito si se puede acceder al extremo con las credenciales especificadas. La conexión con el extremo se valida desde un nodo en cada sitio.
- Aparece un mensaje de error si se produce un error en la validación del extremo. Si necesita modificar el punto final para corregir el error, seleccione **Volver a los detalles del punto final** y actualice la información. A continuación, seleccione **probar y crear punto final**.



La creación de punto final falla si los servicios de plataforma no están activados para su cuenta de inquilino. Póngase en contacto con el administrador de StorageGRID.

Una vez que haya configurado un extremo, puede utilizar su URN para configurar un servicio de plataforma.

#### Información relacionada

- ["Especifique URN para el extremo de servicios de la plataforma"](#)
- ["Configure la replicación de CloudMirror"](#)
- ["Configure las notificaciones de eventos"](#)
- ["Configure el servicio de integración de búsqueda"](#)

## Probar la conexión para el extremo de servicios de la plataforma

Si la conexión a un servicio de plataforma ha cambiado, puede probar la conexión del extremo para validar que el recurso de destino existe y que se puede acceder a él utilizando las credenciales especificadas.

#### Antes de empezar

- Ha iniciado sesión en el gestor de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el ["Gestionar puntos finales o permisos de acceso raíz"](#).

#### Acerca de esta tarea

StorageGRID no valida que las credenciales tengan los permisos correctos.

#### Pasos

1. Seleccione **STORAGE (S3) > Platform Services Endpoints**.

Aparece la página de extremos de servicios de plataforma y muestra la lista de extremos de servicios de plataforma que ya se han configurado.

2. Seleccione el extremo cuya conexión desea probar.

Aparece la página de detalles del extremo.

3. Seleccione **probar conexión**.

- Aparece un mensaje de éxito si se puede acceder al extremo con las credenciales especificadas. La conexión con el extremo se valida desde un nodo en cada sitio.
- Aparece un mensaje de error si se produce un error en la validación del extremo. Si necesita modificar el extremo para corregir el error, seleccione **Configuración** y actualice la información. A continuación, seleccione **probar y guardar los cambios**.

## Editar extremo de servicios de plataforma

Puede editar la configuración de un extremo de servicios de plataforma para cambiar su nombre, URI u otros detalles. Por ejemplo, es posible que deba actualizar las credenciales caducadas o cambiar el URI para apuntar a un índice de Elasticsearch de backup para la conmutación por error. No puede cambiar el URN para un punto final de servicios de plataforma.

### Antes de empezar

- Ha iniciado sesión en el gestor de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el ["Gestionar puntos finales o permisos de acceso raíz"](#).

### Pasos

1. Seleccione **STORAGE (S3) > Platform Services Endpoints**.

Aparece la página de extremos de servicios de plataforma y muestra la lista de extremos de servicios de plataforma que ya se han configurado.

2. Seleccione el extremo que desea editar.

Aparece la página de detalles del extremo.

3. Seleccione **Configuración**.
4. Según sea necesario, cambie la configuración del extremo.



No puede cambiar el URN de un punto final después de crear el punto final.

- a. Para cambiar el nombre mostrado del punto final, seleccione el icono de edición
- b. Según sea necesario, cambie el URI.
- c. Según sea necesario, cambie el tipo de autenticación.
  - Para la autenticación de la clave de acceso, cambie la clave según sea necesario seleccionando **Editar clave S3** y pegando un nuevo ID de clave de acceso y una clave de acceso secreta. Si necesita cancelar los cambios, seleccione **Revert S3 key EDIT**.
  - Para la autenticación CAP (C2S Access Portal), cambie la URL de las credenciales temporales o la frase de contraseña de la clave privada del cliente opcional y cargue nuevos archivos de certificado y claves según sea necesario.



La clave privada del cliente debe estar en formato cifrado OpenSSL o en formato de clave privada no cifrada.

d. Según sea necesario, cambie el método para verificar los certificados.

5. Seleccione **probar y guardar los cambios**.

- Aparece un mensaje de éxito si se puede acceder al extremo con las credenciales especificadas. La conexión al extremo se verifica desde un nodo en cada sitio.
- Aparece un mensaje de error si se produce un error en la validación del extremo. Modifique el extremo para corregir el error y, a continuación, seleccione **probar y guardar los cambios**.

## Eliminar extremo de servicios de plataforma

Puede eliminar un extremo si ya no desea utilizar el servicio de plataforma asociado.

### Antes de empezar

- Ha iniciado sesión en el gestor de inquilinos mediante un ["navegador web compatible"](#).
- Pertenece a un grupo de usuarios que tiene el ["Gestionar puntos finales o permisos de acceso raíz"](#).

### Pasos

1. Seleccione **STORAGE (S3) > Platform Services Endpoints**.

Aparece la página de extremos de servicios de plataforma y muestra la lista de extremos de servicios de plataforma que ya se han configurado.

2. Seleccione la casilla de verificación de cada punto final que desee suprimir.



Si elimina un extremo de servicios de plataforma que está en uso, el servicio de plataforma asociado se deshabilitará para todos los bloques que utilicen el extremo. Se descartarán las solicitudes que aún no se hayan completado. Se continuarán generando todas las solicitudes nuevas hasta que cambie la configuración de bloque para que ya no haga referencia a URN eliminado. StorageGRID informará de estas solicitudes como errores irrecuperables.

3. Seleccione **acciones > Eliminar punto final**.

Aparecerá un mensaje de confirmación.


4. Seleccione **Eliminar punto final**.

## Solucionar errores de extremos de servicios de plataforma

Si se produce un error cuando StorageGRID intenta comunicarse con un punto final de servicios de plataforma, se muestra un mensaje en el panel de control. En la página Platform Services Endpoints, la columna Last error indica durante cuánto tiempo se produjo el error. No se muestra ningún error si los permisos asociados con las credenciales de un extremo son incorrectos.


## Determine si se ha producido un error

Si se ha producido algún error de punto final de servicios de plataforma en los últimos 7 días, el panel de control del gestor de inquilinos muestra un mensaje de alerta. Puede ir a la página de extremos de servicios de plataforma para ver más detalles sobre el error.

 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 Puntos Finales de Servicios de Plataforma. Para ver un mensaje de error más detallado:

### Pasos

1. En la lista de puntos finales, seleccione el extremo que tiene el error.
2. En la página de detalles del punto final, seleccione **Conexión**. Esta pestaña muestra sólo el error más reciente de un punto final e indica cuánto tiempo se produjo el error. Los errores que incluyen el icono rojo X  se han producido en los últimos 7 días.

## Compruebe si el error sigue estando actualizado

Es posible que algunos errores sigan apareciendo en la columna **último error** incluso después de que se hayan resuelto. Para ver si un error es actual o para forzar la eliminación de un error resuelto de la tabla:

### Pasos

1. Seleccione el extremo.

Aparece la página de detalles del extremo.

2. Seleccione **Conexión** > **probar conexión**.

Al seleccionar **probar conexión**, StorageGRID valida que el extremo de servicios de la plataforma existe y que se puede alcanzar con las credenciales actuales. La conexión con el extremo se valida desde un nodo en cada sitio.

## Resolver errores de punto final

Puede utilizar el mensaje **último error** de la página de detalles del punto final para ayudar a determinar qué está causando el error. Es posible que algunos errores requieran que edite el extremo para resolver el problema. Por ejemplo, se puede producir un error CloudMirroring si StorageGRID no puede acceder al bloque de S3 de destino porque no tiene los permisos de acceso correctos o si la clave de acceso ha caducado. El mensaje es «Las credenciales del punto final o el acceso al destino deben actualizarse» y los detalles son «ACCESSDENIED» o «InvalidAccessKeyId».

Si necesita editar el extremo para resolver un error, al seleccionar **probar y guardar cambios** StorageGRID validará el extremo actualizado y confirmará que se puede alcanzar con las credenciales actuales. La conexión con el extremo se valida desde un nodo en cada sitio.

### Pasos

1. Seleccione el extremo.
2. En la página de detalles del punto final, seleccione **Configuración**.
3. Edite la configuración del extremo según sea necesario.

4. Seleccione **Conexión > probar conexión**.

### Credenciales de extremo con permisos insuficientes

Cuando StorageGRID valida un extremo de servicios de plataforma, confirma que las credenciales del extremo se pueden utilizar para ponerse en contacto con el recurso de destino y realiza una comprobación básica de permisos. Sin embargo, StorageGRID no valida todos los permisos necesarios para ciertas operaciones de servicios de plataforma. Por este motivo, si recibe un error al intentar utilizar un servicio de plataforma (como "403 Forbidden"), compruebe los permisos asociados con las credenciales del punto final.

#### Información relacionada

- [Administrar los servicios de plataforma de StorageGRID > Solucionar problemas](#)
- ["Cree un extremo de servicios de plataforma"](#)
- ["Probar la conexión para el extremo de servicios de la plataforma"](#)
- ["Editar extremo de servicios de plataforma"](#)

## Configure la replicación de CloudMirror

Para habilitar la replicación de CloudMirror para un bucket, cree y aplique un XML de configuración de replicación de bucket válido.

#### Antes de empezar

- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Ya ha creado un bucket que actúa como origen de replicación.
- El punto final que pretende utilizar como destino para la replicación de CloudMirror ya existe y tiene su URN.
- Pertenece a un grupo de usuarios que tiene el ["Gestione todos los bloques o permisos de acceso raíz"](#). Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

#### Acerca de esta tarea

La replicación de CloudMirror copia los objetos de un bloque de origen en un bloque de destino que se especifique en un extremo.

Para obtener información general sobre la replicación de buckets y cómo configurarla, consulte ["Documentación de Amazon Simple Storage Service \(S3\): Replicación de objetos"](#). Para obtener información sobre cómo StorageGRID implementa GetBucketReplication, DeleteBucketReplication y PutBucketReplication, consulte la ["Operaciones en bloques"](#).



La replicación de CloudMirror tiene similitudes y diferencias importantes con la función de replicación entre grid. Para obtener más información, consulte ["Compare la replicación entre grid y la replicación de CloudMirror"](#).

Tenga en cuenta los siguientes requisitos y características al configurar la replicación de CloudMirror:

- Al crear y aplicar un XML de configuración de replicación de bucket válido, debe utilizar el URN de un punto final de bucket S3 para cada destino.
- La replicación no es compatible con buckets de origen o destino con el bloqueo de objetos S3 habilitado.



- Si habilita la replicación de CloudMirror en un bloque que contiene objetos, se replican los nuevos objetos agregados al bloque, pero los objetos existentes del bloque no se replican. Debe actualizar los objetos existentes para activar la replicación.
- Si se especifica una clase de almacenamiento en el XML de configuración de replicación, StorageGRID utiliza esa clase al realizar operaciones en el extremo de S3 de destino. El extremo de destino también debe admitir la clase de almacenamiento especificada. Asegúrese de seguir las recomendaciones que proporciona el proveedor del sistema de destino.

## Pasos

### 1. Habilite la replicación para su bloque de origen:

- Utilice un editor de texto para crear el XML de configuración de replicación necesario para habilitar la replicación, tal y como se especifica en la API de replicación de S3.
- Al configurar XML:
  - Tenga en cuenta que StorageGRID solo admite V1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso `Filter` del elemento para reglas y sigue las convenciones de V1 para eliminar versiones de objetos. Consulte la documentación de Amazon sobre la configuración de replicación para obtener más información.
  - Use el URN de un extremo de bloque de S3 como destino.
  - Si lo desea, agregue el `<StorageClass>` elemento y especifique una de las siguientes opciones:
    - `STANDARD`: La clase de almacenamiento predeterminada. Si no especifica una clase de almacenamiento al cargar un objeto, se `STANDARD` utilizará la clase de almacenamiento.
    - `STANDARD_IA`: (Estándar - Acceso poco frecuente.) Utilice esta clase de almacenamiento para los datos a los que se accede con menos frecuencia, pero que siguen requiriendo un acceso rápido cuando es necesario.
    - `REDUCED_REDUNDANCY`: Utilice esta clase de almacenamiento para datos no críticos y reproducibles que se pueden almacenar con menos redundancia que la `STANDARD` clase de almacenamiento.
  - Si especifica un `Role` en el XML de configuración, se ignorará. StorageGRID no utiliza este valor.

```
<ReplicationConfiguration>
  <Role></Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>2020</Prefix>
    <Destination>
      <Bucket>urn:sgws:s3:::2017-records</Bucket>
      <StorageClass>STANDARD</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

2. Seleccione **Ver cubos** en el panel de control o seleccione **ALMACENAMIENTO (S3) > Buckets**.
3. Seleccione el nombre del bloque de origen.

Aparece la página de detalles bucket.

4. Seleccione **Servicios de plataforma > replicación**.
5. Seleccione la casilla de verificación **Habilitar replicación**.
6. Pegue el XML de configuración de replicación en el cuadro de texto y seleccione **Guardar cambios**.



Un administrador de StorageGRID debe habilitar los servicios de plataforma para cada cuenta de inquilino mediante Grid Manager o la API de gestión de grid. Póngase en contacto con el administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Compruebe que la replicación está configurada correctamente:
  - a. Añada un objeto al bloque de origen que cumpla con los requisitos de replicación según se especifica en la configuración de replicación.

En el ejemplo mostrado anteriormente, se replican los objetos que coincidan con el prefijo «2020».

- b. Confirme que el objeto se ha replicado en el bloque de destino.

En el caso de objetos pequeños, la replicación se realiza con rapidez.

#### Información relacionada

["Cree un extremo de servicios de plataforma"](#)

## Configure las notificaciones de eventos

Para habilitar las notificaciones de un depósito, cree XML de configuración de notificaciones y utilice el Gestor de inquilinos para aplicar el XML a un bloque.

#### Antes de empezar

- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Ya creó un bloque para que actúe como origen de notificaciones.
- El punto final que pretende utilizar como destino para las notificaciones de eventos ya existe y tiene su URN.
- Pertenece a un grupo de usuarios que tiene el ["Gestione todos los bloques o permisos de acceso raíz"](#). Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

#### Acerca de esta tarea

Puede configurar las notificaciones de eventos asociando el XML de configuración de notificaciones con un depósito de origen. El XML de configuración de notificaciones sigue las convenciones S3 para configurar notificaciones de bucket, con el tema de Amazon SNS de destino, el tema de Kafka o el punto final del webhook especificado como el URN de un punto final.

Para obtener información general sobre las notificaciones de eventos y cómo configurarlas, consulte la ["Documentación de Amazon"](#). Para obtener información sobre cómo StorageGRID implementa la API de configuración de notificación de buckets S3, consulte la ["Instrucciones para implementar aplicaciones cliente de S3"](#).

Tenga en cuenta los siguientes requisitos y características al configurar las notificaciones de eventos para un bloque:

- Al crear y aplicar un XML de configuración de notificación válido, debe utilizar el URN de un punto final de notificaciones de eventos para cada destino.
- Aunque la notificación de eventos se puede configurar en un depósito con bloqueo de objetos S3 activado, los metadatos de bloqueo de objetos S3 (incluidos el estado de retención legal y la fecha de retención hasta) de los objetos no se incluirán en los mensajes de notificación.
- Después de configurar las notificaciones de eventos, cada vez que ocurre un evento específico para un objeto en el bucket de origen, se genera una notificación y se envía al tema de Amazon SNS, al tema de Kafka o al punto final del webhook utilizado como destino.
- Si habilita las notificaciones de eventos para un bloque que contiene objetos, las notificaciones se envían solo para las acciones que se realizan una vez guardada la configuración de notificación.

## Pasos

### 1. Habilite las notificaciones para su bloque de origen:

- Use un editor de texto para crear el XML de configuración de notificaciones necesario para habilitar las notificaciones de eventos, como se especifica en la API de notificación de S3.
- Al configurar XML, utilice URN de un extremo de notificaciones de eventos como tema de destino.

```
<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images/</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
  </TopicConfiguration>
</NotificationConfiguration>
```

### 2. En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3) > Cuchos**.

### 3. Seleccione el nombre del bloque de origen.

Aparece la página de detalles bucket.

### 4. Seleccione **Servicios de plataforma > Notificaciones de eventos**.

### 5. Seleccione la casilla de verificación **Habilitar notificaciones de eventos**.

### 6. Pegue el XML de configuración de notificación en el cuadro de texto y seleccione **Guardar cambios**.



Un administrador de StorageGRID debe habilitar los servicios de plataforma para cada cuenta de inquilino mediante Grid Manager o la API de gestión de grid. Póngase en contacto con el administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Compruebe que las notificaciones de eventos están configuradas correctamente:

- a. Realice una acción en un objeto del bloque de origen que cumpla los requisitos para activar una notificación tal y como se ha configurado en el XML de configuración.

En el ejemplo, una notificación de evento se envía cada vez que se crea un objeto con `images/` el prefijo.

- b. Confirme que se haya enviado una notificación al tema de Amazon SNS de destino, al tema de Kafka o al punto final del webhook.

Por ejemplo, si el tema de destino está alojado en Amazon SNS, puede configurar el servicio para que le envíe un correo electrónico cuando se entregue la notificación.

```

{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "arn": "arn:sgws:s3:::test1"
        },
        "object": {
          "key": "images/cat.jpg",
          "size": 0,
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",
          "sequencer": "14D90402421461C7"
        }
      }
    }
  ]
}

```

+ Si se recibe la notificación en el tema de destino, ha configurado correctamente el bloque de origen para las notificaciones StorageGRID.

#### Información relacionada

- ["Comprender las notificaciones para bloques"](#)
- ["USE LA API DE REST DE S3"](#)
- ["Cree un extremo de servicios de plataforma"](#)

# Configure el servicio de integración de búsqueda

Para activar la integración de búsqueda de un depósito, cree XML de integración de búsqueda y utilice el gestor de inquilinos para aplicar el XML al bloque.

## Antes de empezar

- Un administrador de StorageGRID activó los servicios de plataforma para su cuenta de inquilino.
- Ya ha creado un bucket S3 cuyo contenido desea indexar.
- El punto final que pretende utilizar como destino para el servicio de integración de búsqueda ya existe y tiene su URN.
- Pertenece a un grupo de usuarios que tiene el ["Gestione todos los bloques o permisos de acceso raíz"](#). Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

## Acerca de esta tarea

Después de configurar el servicio de integración de búsqueda para un bloque de origen, al crear un objeto o actualizar los metadatos o las etiquetas de un objeto se activan los metadatos de objeto que se enviarán al extremo de destino.

Si habilita el servicio de integración de búsqueda para un depósito que ya contiene objetos, las notificaciones de metadatos no se envían automáticamente para los objetos existentes. Actualice estos objetos existentes para asegurarse de que sus metadatos se agregan al índice de búsqueda de destino.

## Pasos

1. Habilitar la integración de búsqueda para un bloque:

- Utilice un editor de texto para crear el XML de notificación de metadatos necesario para habilitar la integración de búsqueda.
- Al configurar XML, utilice URN de un extremo de integración de búsqueda como destino.

Los objetos se pueden filtrar según el prefijo del nombre del objeto. Por ejemplo, puede enviar metadatos para objetos con el prefijo `images` a un destino y metadatos para los objetos con el prefijo `videos` a otro. Las configuraciones que tienen prefijos superpuestos no son válidas y se rechazan cuando se envían. Por ejemplo, no se permite una configuración que incluya una regla para los objetos con el prefijo `test` y una segunda regla para los objetos con el prefijo `test2`.

Si es necesario, consulte la [Ejemplos del XML de configuración de metadatos](#).

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>/Urn</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Elementos del XML de configuración de notificación de metadatos:

Nombre	Descripción	Obligatorio
MetadataNotificationConfiguration	<p>Etiqueta de contenedor para las reglas que se usan para especificar los objetos y el destino de las notificaciones de metadatos.</p> <p>Contiene uno o más elementos Regla.</p>	Sí
Regla	<p>Código de contenedor de una regla que identifica los objetos cuyos metadatos deben agregarse a un índice especificado.</p> <p>Se rechazan las reglas con prefijos superpuestos.</p> <p>Incluido en el elemento MetadataNotificationConfiguration.</p>	Sí
ID	<p>Identificador único de la regla.</p> <p>Incluido en el elemento Regla.</p>	No
Estado	<p>El estado puede ser "activado" o "desactivado". No se toman medidas para las reglas que están desactivadas.</p> <p>Incluido en el elemento Regla.</p>	Sí
Prefijo	<p>Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado.</p> <p>Para hacer coincidir todos los objetos, especifique un prefijo vacío.</p> <p>Incluido en el elemento Regla.</p>	Sí
Destino	<p>Etiqueta de contenedor para el destino de una regla.</p> <p>Incluido en el elemento Regla.</p>	Sí

Nombre	Descripción	Obligatorio
No	<p>URN del destino donde se envían los metadatos del objeto. Debe ser URN de un extremo de StorageGRID con las siguientes propiedades:</p> <ul style="list-style-type: none"> <li>• es debe ser el tercer elemento.</li> <li>• El URN debe terminar con el índice y el tipo donde se almacenan los metadatos, en la forma <code>domain-name/myindex/mytype</code>.</li> </ul> <p>Los extremos se configuran con el administrador de inquilinos o la API de gestión de inquilinos. Tienen el siguiente formato:</p> <ul style="list-style-type: none"> <li>• <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code></li> <li>• <code>urn:mysite:es:::mydomain/myindex/mytype</code></li> </ul> <p>El punto final debe estar configurado antes de enviar el XML de configuración o la configuración fallará con un error 404.</p> <p>EL VALOR DE URN se incluye en el elemento Destination.</p>	Sí

- En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3) > Cuchos**.
  - Seleccione el nombre del bloque de origen.
- Aparece la página de detalles bucket.
- Seleccione **Servicios de plataforma > integración de búsqueda**
  - Seleccione la casilla de verificación **Habilitar integración de búsqueda**.
  - Pegue la configuración de notificación de metadatos en el cuadro de texto y seleccione **Guardar cambios**.



Un administrador de StorageGRID debe habilitar los servicios de plataforma para cada cuenta de inquilino mediante Grid Manager o la API de gestión. Póngase en contacto con el administrador de StorageGRID si se produce un error al guardar el XML de configuración.

- Compruebe que el servicio de integración de búsqueda está configurado correctamente:
  - Añada un objeto al bloque de origen que cumpla los requisitos para activar una notificación de metadatos tal y como se especifica en el XML de configuración.

En el ejemplo mostrado anteriormente, todos los objetos añadidos al bloque activan una notificación de metadatos.

  - Confirme que se ha agregado un documento JSON que contiene los metadatos y las etiquetas del objeto al índice de búsqueda especificado en el extremo.

### Después de terminar

Según sea necesario, se puede deshabilitar la integración de búsqueda para un bloque con cualquiera de los siguientes métodos:



- Seleccione **STORAGE (S3) > Buckets** y desactive la casilla de verificación **Enable search integration**.
- Si utiliza la API de S3 directamente, utilice una solicitud de notificación DELETE Bucket. Consulte las instrucciones para implementar aplicaciones cliente de S3.

## Ejemplo: Configuración de notificación de metadatos que se aplica a todos los objetos

En este ejemplo, los metadatos de objeto de todos los objetos se envían al mismo destino.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:myes:es::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

## Ejemplo: Configuración de notificación de metadatos con dos reglas

En este ejemplo, los metadatos del objeto para los objetos que coinciden con el prefijo `/images` se envían a un destino, mientras que los metadatos del objeto para 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-1:33333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

## Formato de notificación de metadatos

Al habilitar el servicio de integración de búsqueda para un bloque, se genera un documento JSON y se envía al extremo de destino cada vez que se agregan, actualizan o eliminan metadatos o etiquetas del objeto.

Este ejemplo muestra un ejemplo del JSON que podría generarse cuando se crea un objeto con la clave `SGWS/Tagging.txt` en un cubo llamado `test`. El `test` depósito no está versionado, por lo que la `versionId` etiqueta está vacía.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

## Campos incluidos en el documento JSON

El nombre del documento incluye el nombre del bloque, el nombre del objeto y el ID de versión, si existe.

## Información sobre bloques y objetos

bucket: Nombre del cubo

key: Nombre de clave de objeto

versionID: Versión de objeto, para objetos en cubos versionados

region: Región de cubo, por ejemplo us-east-1

## Metadatos del sistema

size: Tamaño del objeto (en bytes) como visible para 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, como pares clave-valor

key:value

## Cómo ver 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 S3. Para configurar Elasticsearch para interpretar estas

cadenas como fechas o números, siga las instrucciones de Elasticsearch para la asignación dinámica de campos y para asignar formatos de fecha. Active las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Después de indexar un documento, no puede editar los tipos de campo del documento en el índice.

## Información 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.