



Gestione servicios de plataformas S3

StorageGRID

NetApp
April 10, 2024

Tabla de contenidos

- Gestione servicios de plataformas S3 1
 - ¿Qué son los servicios de plataforma? 1
 - Consideraciones sobre el uso de servicios de plataforma 6
 - Configure los extremos de servicios de la plataforma 8
 - Configure la replicación de CloudMirror 27
 - Configure las notificaciones de eventos 31
 - Utilice el servicio de integración de búsqueda 35

Gestione servicios de plataformas S3

¿Qué son los servicios de plataforma?

Los servicios de plataforma de StorageGRID pueden ayudarle a implementar una estrategia de cloud híbrido.

Si se permite el uso de servicios de plataforma para su cuenta de inquilino, puede configurar los siguientes servicios para cualquier bloque de S3:

- **Duplicación CloudMirror:** La [Servicio de replicación CloudMirror de StorageGRID](#) Se utiliza para reflejar objetos específicos de un bloque de StorageGRID en un destino externo especificado.

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



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

- **Notificaciones:** [Notificaciones de eventos por bloque](#) Se utilizan para enviar notificaciones sobre acciones específicas realizadas en objetos a un Amazon simple Notification Service™ (SNS) externo especificado.

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



Aunque la notificación de eventos se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos S3 (incluido el estado retener hasta fecha y retención legal) de los objetos no se incluirán en los mensajes de notificación.

- **Servicio de integración de búsqueda:** El [servicio de integración de búsqueda](#) Se usa para enviar metadatos de objetos de S3 a un índice de Elasticsearch especificado donde los metadatos se pueden buscar o analizar mediante el servicio externo.

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



Aunque la integración de Elasticsearch se puede configurar en un bloque con el bloqueo de objetos S3 habilitado, los metadatos del bloqueo de objetos de S3 (incluidos los Estados Retain Until Date and Legal Hold) de los objetos no se incluirán en los mensajes de notificación.

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

Se puede configurar cualquier combinación de servicios de plataforma para un único bloque de S3. Por ejemplo, podría configurar el servicio CloudMirror y las notificaciones en un bloque de StorageGRID S3 de manera que pueda reflejar objetos específicos en Amazon simple Storage Service, al tiempo que envía una

notificación sobre cada objeto de ese tipo a una aplicación de supervisión de terceros para ayudarle a realizar un seguimiento de los gastos de AWS.



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

Cómo se configuran los servicios de plataforma

Los servicios de plataforma se comunican con extremos externos que se configuran mediante el administrador de inquilinos o la API de gestión de inquilinos. Cada extremo representa un destino externo, como un bloque de StorageGRID S3, un bloque de Amazon Web Services, un tema de servicio de notificación simple (SNS) o un clúster de Elasticsearch alojado localmente, en AWS u otros lugares.

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

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

1. Si desea que todos los objetos con las claves comiencen `/images` Para replicarse en un bloque de Amazon S3, debe añadir una configuración de replicación al bloque de origen.
2. Si también desea enviar notificaciones cuando estos objetos están almacenados en el bloque, debe añadir una configuración de notificaciones.
3. Por último, si desea indexar los metadatos de estos objetos, debe agregar la configuración de notificación de metadatos que se utiliza para implementar la integración de búsquedas.

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

Servicio de plataforma	API REST DE S3
Replicación de CloudMirror	<ul style="list-style-type: none">• OBTENGA la replicación de Bucket• PUT Bucket replication
Notificaciones	<ul style="list-style-type: none">• OBTENGA la notificación DE BUCKET• NOTIFICACIÓN DE PUT Bucket
Integración de búsqueda	<ul style="list-style-type: none">• OBTENGA la configuración de notificación de metadatos del bloque de datos• PUT bucket metadata notification Configuration <p>Estas operaciones están personalizadas en StorageGRID.</p>

Consulte las instrucciones para implementar aplicaciones cliente de S3 para obtener detalles sobre cómo StorageGRID implementa estas API.

Información relacionada

[Consideraciones sobre el uso de servicios de plataforma](#)

Servicio de replicación de CloudMirror

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

La replicación de CloudMirror opera con independencia de la política de ILM activa de la cuadrícula. El servicio CloudMirror replica los objetos cuando se almacenan en el bloque de origen y los envía al Lo antes posible, de bloque de destino. La entrega de objetos replicados se activa cuando la ingesta de objetos se realiza correctamente.

Si habilita la replicación de CloudMirror para un bloque existente, solo se replican los nuevos objetos agregados a ese bloque. No se replican ningún objeto existente en el bloque. Para forzar la replicación de objetos existentes, puede actualizar los metadatos del objeto existente ejecutando una copia de objeto.



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

En StorageGRID, puede replicar los objetos de un solo bloque en varios bloques de destino. Para ello, especifique el destino de cada regla en el XML de configuración de replicación. No se puede replicar un objeto en más de un bloque a la vez.

Además, puede configurar la replicación de CloudMirror en bloques con versiones o sin versiones, y puede especificar un bloque con versiones o sin versiones como destino. Puede utilizar cualquier combinación de cubos con versiones y sin versiones. Por ejemplo, puede especificar un bloque con versiones como destino para un bloque de origen sin versiones o viceversa. También puede replicar entre cubos sin versiones.

El comportamiento de eliminación del servicio de replicación CloudMirror es el mismo que el comportamiento de eliminación del servicio de replicación entre regiones (CRR) proporcionado por Amazon S3 — al eliminar un objeto de un bloque de origen nunca se elimina un objeto replicado en el destino. Si se van a crear versiones de los cubos de origen y de destino, se replica el marcador de borrado. Si el bloque de destino no tiene versiones, al eliminar un objeto del bloque de origen no se replicará el marcador DELETE en el bloque de destino ni se eliminará el objeto de destino.

A medida que los objetos se replican en el segmento de destino, StorageGRID los Marca como «réplicas». Un bloque StorageGRID de destino no replicará objetos marcados como réplicas de nuevo, lo que le protegerá de bucles de replicación accidentales. Este marcado de réplica es interno en StorageGRID y no le impide utilizar AWS CRR cuando se utiliza un bloque de Amazon S3 como destino.



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

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

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

Comprender las notificaciones para bloques

Es posible habilitar la notificación de eventos para un bloque de S3 si desea que StorageGRID envíe notificaciones sobre eventos especificados a un servicio de notificación simple (SNS) de destino.

Puede hacerlo [configure las notificaciones de eventos](#) Asociando XML de configuración de notificación a un bloque de origen. El XML de configuración de notificaciones sigue las convenciones de S3 para configurar las notificaciones de bloques, con el tema SNS de destino especificado como URN de un extremo.

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

La singularidad y el orden de las notificaciones no están garantizados. Como resultado de las operaciones realizadas para garantizar el éxito en la entrega, se podría enviar más de una notificación de un evento al destino. Además, como la entrega es asíncrona, no se garantiza que la ordenación del tiempo de las notificaciones en el destino coincida con la ordenación de eventos del bloque de origen, especialmente en las operaciones que se originan en diferentes sitios de StorageGRID. Puede utilizar el `sequencer` Introduzca el mensaje de evento para determinar el orden de los eventos de un objeto determinado, como se describe en la documentación de Amazon S3.

Notificaciones y mensajes compatibles

Las notificaciones de eventos de StorageGRID siguen la API de Amazon S3 con las siguientes limitaciones:

- No es posible configurar una notificación para los siguientes tipos de eventos. Estos tipos de evento **no** son compatibles.
 - `s3:ReducedRedundancyLostObject`
 - `s3:ObjectRestore:Completed`
- Las notificaciones de eventos enviadas desde StorageGRID utilizan el formato JSON estándar excepto que no incluyen algunas claves y utilizan valores específicos para otros, como se muestra en la tabla:

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

Comprender el servicio de integración de búsquedas

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

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

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

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



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

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

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

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

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

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

Información relacionada

[XML de configuración para la integración de búsqueda](#)

[Metadatos de objetos incluidos en las notificaciones de metadatos](#)

[JSON generado por el servicio de integración de búsqueda](#)

[Configure el servicio de integración de búsqueda](#)

Consideraciones sobre el uso de servicios de plataforma

Antes de implementar los servicios de la plataforma, revise las recomendaciones y consideraciones sobre el uso de estos servicios.

Para obtener más información sobre S3, consulte [Use S3](#).

Consideraciones sobre el uso de servicios de plataforma

Consideración	Detalles
Supervisión del extremo de destino	Debe supervisar la disponibilidad de cada extremo de destino. Si se pierde la conectividad con el extremo de destino durante un periodo de tiempo prolongado y existe una gran acumulación de solicitudes, se producirá un error en las solicitudes de cliente adicionales (como solicitudes PUT) a StorageGRID. Debe volver a intentar estas solicitudes con errores cuando se pueda acceder al extremo.
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 que coincida con el comportamiento de eliminación de los servicios CRR y SNS de AWS, las solicitudes de notificación de CloudMirror y eventos no se envían cuando se elimina un objeto del bloque de origen debido a las reglas de ILM de StorageGRID. Por ejemplo, no se envían solicitudes de notificaciones de eventos o CloudMirror si una regla de ILM elimina un objeto después de 14 días.</p> <p>Por el contrario, las solicitudes de integración de búsqueda se envían cuando los objetos se eliminan debido a ILM.</p>

Consideraciones sobre el uso del servicio de replicación de CloudMirror

Consideración	Detalles
Estado de replicación	StorageGRID no admite el <code>x-amz-replication-status</code> encabezado.
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>Nota: El tamaño máximo <i>recomendado</i> para una operación PUT Object es de 5 GiB (5,368,709,120 bytes). Si tiene objetos que sean mayores de 5 GiB, utilice la carga de varias partes en su lugar.</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>Nota: Los ID de versión para el cucharón de origen en StorageGRID no están relacionados con los ID de versión para el cubo de destino.</p>

Consideración	Detalles
Etiquetado para versiones de objetos	<p>El servicio CloudMirror no replica ninguna solicitud DE etiquetado de objetos PUT ni ELIMINA solicitudes de etiquetado de objetos que proporcionen un ID de versión, debido a las limitaciones en el protocolo S3. Como los ID de versión del origen y del destino no están relacionados, no hay manera de garantizar que se replique una actualización de etiqueta a un ID de versión específico.</p> <p>Por el contrario, el servicio CloudMirror replica las solicitudes DE etiquetado PUT Object o ELIMINA las solicitudes de etiquetado de objetos que no especifican un ID de versión. Estas solicitudes actualizan las etiquetas de la clave más reciente (o la versión más reciente si el bloque está versionado). También se replican búsquedas normales con etiquetas (no actualizaciones de etiquetado).</p>
Cargas en varias partes y ETag valores	Cuando se crea un mirroring de objetos cargados con una carga de varias partes, el servicio CloudMirror no conserva las piezas. Como resultado, el ETag el valor del objeto reflejado será diferente al ETag valor del objeto original.
Objetos cifrados con SSE-C (cifrado en el lado del servidor con claves proporcionadas por el cliente)	El servicio CloudMirror no admite objetos cifrados con SSE-C. Si intenta procesar un objeto en el bloque de origen para la replicación de CloudMirror y la solicitud incluye los encabezados de solicitud de SSE-C, se produce un error en la operación.
Bloque con S3 Object Lock habilitado	Si el bloque de destino S3 para la replicación de CloudMirror tiene la función S3 Object Lock habilitada, el intento de configurar la replicación de bucket (PUT Bucket replication) producirá un error ACCESSDENIED.

Configure los extremos de servicios de la plataforma

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

El acceso a servicios de la plataforma está habilitado por inquilino por un administrador de StorageGRID. Para crear o utilizar un extremo de servicios de plataforma, debe ser un usuario inquilino con permiso Administrar extremos o acceso raíz, en una cuadrícula cuya red se haya configurado para permitir que los nodos de almacenamiento accedan a recursos de extremo externos. Si desea obtener más información, póngase en contacto con el administrador de StorageGRID.

¿Qué es un extremo de servicios de plataforma?

Al crear un extremo de servicios de plataforma, se especifica la información que StorageGRID necesita para acceder al destino externo.

Por ejemplo, si desea replicar objetos de un bloque de StorageGRID en un bloque de AWS S3, debe crear un extremo de servicios de plataforma que incluya la información y las credenciales que StorageGRID necesita para acceder al bloque de destino en AWS.

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

habilitar el servicio.

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

Extremos para la replicación de CloudMirror

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

Extremos para notificaciones

StorageGRID admite los extremos del servicio de notificación simple (SNS). No se admiten extremos de AWS Lambda o simple Queue Service (SQS).

Extremos del servicio de integración de búsqueda

StorageGRID admite extremos de integración de búsqueda que representan clústeres de Elasticsearch. Estos clústeres de Elasticsearch pueden estar en un centro de datos local o en los clouds de AWS u otros lugares.

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

Información relacionada

[Administre StorageGRID](#)

Especifique URN para el extremo de servicios de la plataforma

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

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

URN elementos

El URN de un extremo de servicios de plataforma debe comenzar con cualquiera de los dos `arn:aws` o `urn:mystore`, como se indica a continuación:

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

Por ejemplo, si especifica el URN para un extremo de CloudMirror alojado en StorageGRID, el URN podría comenzar con `urn:sgws`.

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

Servicio	Tipo
Replicación de CloudMirror	s3
Notificaciones	sns
Integración de búsqueda	es

Por ejemplo, para seguir especificando URN para un extremo de CloudMirror alojado en StorageGRID, debería añadir `s3` para conseguirlo `urn:sgws:s3`.

El elemento final del URN identifica el recurso de destino específico en el URI de destino.

Servicio	Recurso específico
Replicación de CloudMirror	nombre del bloque
Notificaciones	sns-topic-name
Integración de búsqueda	domain-name/index-name/type-name Nota: Si el clúster Elasticsearch está no configurado para crear índices automáticamente, debe crear el índice manualmente antes de crear el punto final.

Urnas para servicios alojados en AWS y GCP

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

- Replicación de CloudMirror:

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

- Notificaciones:

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

- Integración de búsqueda:

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



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

Servicios alojados localmente

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

- Replicación de CloudMirror:

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

En el caso de un extremo de CloudMirror alojado en StorageGRID, es posible especificar una URN válida que comience por `urn:sgws:`

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

- Notificaciones:

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

- Integración de búsqueda:

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```



Para los extremos de integración de búsqueda alojados localmente, el `domain-name` Element puede ser cualquier cadena siempre que el URN del extremo sea único.

Cree un extremo de servicios de plataforma

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

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un [navegador web compatible](#).
- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar endpoints.
- Se debe haber creado el recurso al que hace referencia el extremo de servicios de la plataforma:
 - Replicación de CloudMirror: Bloque de S3

- Notificación de eventos: Tema SNS
- Notificación de búsqueda: Índice de Elasticsearch, si el clúster de destino no está configurado para crear índices automáticamente.
- Debe tener la información sobre el recurso de destino:
 - Host y puerto para el Identificador uniforme de recursos (URI)



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

- Nombre del recurso único (URN)

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

- Credenciales de autenticación (si es necesario):
 - Clave de acceso: ID de clave de acceso y clave de acceso secreta
 - Basic HTTP: Nombre de usuario y contraseña
 - CAP (C2S Access Portal): URL de credenciales temporales, certificados de servidor y de cliente, claves de cliente y una contraseña de clave privada de cliente opcional.
- Certificado de seguridad (si se utiliza un certificado de CA personalizado)

Pasos

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

Aparece la página de extremos de servicios de plataforma.

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.

0 endpoints

Create endpoint

Delete endpoint

	Display name ?	Last error ?	Type ?	URI ?	URN ?
No endpoints found					
Create endpoint					

2. Seleccione **Crear punto final**.

Create endpoint


1 Enter details


2 Select authentication type
Optional


3 Verify server
Optional

Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name 

URI 

URN 

[Cancel](#)[Continue](#)

- Introduzca un nombre para mostrar para describir brevemente el extremo y su propósito.

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

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

Utilice uno de los siguientes formatos:

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

Si no especifica un puerto, el puerto 443 se utiliza para los URI HTTPS y el puerto 80 se utiliza para los URI HTTP.

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

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

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

de carga.



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

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

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



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

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



No es posible cambiar el URN de un extremo una vez que se creó el extremo.

6. Seleccione **continuar**.

7. Seleccione un valor para **Tipo de autenticación** y, a continuación, introduzca o cargue las credenciales necesarias.

Create endpoint

1 Enter details 2 Select authentication type Optional 3 Verify server Optional

Authentication type ?

Select the method used to authenticate connections to the endpoint.

Anonymous

Anonymous

Access Key

Basic HTTP

CAP (C2S Access Portal)

Previous Continue

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"> • ID de clave de acceso • Clave de acceso secreta
HTTP básico	Utiliza un nombre de usuario y una contraseña para autenticar las conexiones al destino.	<ul style="list-style-type: none"> • Nombre de usuario • Contraseña
CAP (Portal de acceso C2S)	Usa certificados y claves para autenticar las conexiones al destino.	<ul style="list-style-type: none"> • URL de credenciales temporales • Certificado de CA de servidor (carga de archivo PEM) • Certificado de cliente (carga de archivo PEM) • Clave privada de cliente (carga de archivo PEM, formato cifrado OpenSSL o formato de clave privada no cifrado) • Contraseña de clave privada de cliente (opcional)

8. Seleccione **continuar**.

9. Seleccione un botón de opción para **verificar servidor** para elegir cómo se verifica la conexión TLS con el extremo.



Se produce un error en la creación de extremos si los servicios de plataforma no están habilitados para su cuenta de inquilino. Póngase en contacto con el administrador de StorageGRID.

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

Información relacionada

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

[Configure la replicación de CloudMirror](#)

[Configure las notificaciones de eventos](#)

[Configure el servicio de integración de búsqueda](#)

Probar la conexión para el extremo de servicios de la plataforma

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

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un [navegador web compatible](#).
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar endpoints.

Acerca de esta tarea

StorageGRID no valida que las credenciales tengan los permisos correctos.

Pasos

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

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







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.

4 endpoints

Create endpoint


Delete endpoint

<input type="checkbox"/>	Display name 	Last error 	Type 	URI 	URN 
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. Seleccione el extremo cuya conexión desea probar.

Aparece la página de detalles del extremo.

Overview

Display name: **my-endpoint-1** 

Type: **S3 Bucket**

URI: **http://10.96.104.167:10443**

URN: **urn:sgws:s3:::bucket1**

Connection

Configuration

Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

3. Seleccione **probar conexión**.

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

Editar extremo de servicios de plataforma

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

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un [navegador web compatible](#).
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar endpoints. Consulte [Permisos de gestión de inquilinos](#).

Pasos

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

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

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.

4 endpoints Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. Seleccione el extremo que desea editar.

Aparece la página de detalles del extremo.

3. Seleccione **Configuración**.

Overview

Display name: **my-endpoint-3** 

Type: **Notifications**

URI: **http://10.96.104.202:8080/**

URN: **arn:aws:sns:us-west-2::example1**

Connection

Configuration

Edit configuration

Endpoint details

URI 

http://10.96.104.202:8080/

URN 

arn:aws:sns:us-west-2::example1

Authentication type

Basic HTTP 

Username 

testme

Password 

••••••••

Edit password

Verify server

- ☐ Use custom CA certificate
- ☒ Use operating system CA certificate
- ☐ Do not verify certificate


```
-----BEGIN CERTIFICATE-----
abcdefghijklmnopqrstuvwxyz
123456/7890ABCDEFabcdefghijklmnopqrstuvwxyz
-----END CERTIFICATE-----
```

Test and save changes

4. Según sea necesario, cambie la configuración del extremo.



No es posible cambiar el URN de un extremo una vez que se creó el extremo.

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



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

- d. Según sea necesario, cambie el método para verificar el servidor.

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

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

Eliminar extremo de servicios de plataforma

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

Lo que necesitará

- Debe iniciar sesión en el administrador de inquilinos mediante un [navegador web compatible](#).
- Debe pertenecer a un grupo de usuarios que tenga el permiso **Administrar endpoints**. Consulte [Permisos de gestión de inquilinos](#).

Pasos

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

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

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.

4 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name ?	Last error ?	Type ?	URI ?	URN ?
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. Seleccione la casilla de comprobación de cada extremo que desea eliminar.



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

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

Aparecerá un mensaje de confirmación.

Delete endpoint



Are you sure you want to delete endpoint my-endpoint-10?

This might take a few minutes.

When you delete an endpoint, you can no longer use it to access external resources.

Cancel

Delete endpoint


4. Seleccione **Eliminar punto final**.

Solucionar errores de extremos de servicios de plataforma

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

Determine si se ha producido un error

Si se han producido errores de extremo de servicios de plataforma en los últimos 7 días, la consola del administrador de inquilinos muestra un mensaje de alerta. Puede ir a la página de extremos de servicios de plataforma para ver más detalles sobre el error.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

El mismo error que aparece en el panel también aparece en la parte superior de la página de extremos de servicios de plataforma. Para ver un mensaje de error más detallado:

Pasos

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

 ocurrió en los últimos 7 días.

Overview

Display name:

my-endpoint-2

Type:

Search

URI:

http://10.96.104.30:9200

URN:

urn:sgws:es:::mydomain/sveloso/_doc

Connection

Configuration

Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

Last error details

✖

2 hours ago

Endpoint failure: Endpont has an AWS failure: RequestError: send request failed; caused by: url.Error; caused by: net:OpError; caused by: os.SyscallError (logID: 143H5UDUUKMGDRWJ)

Compruebe si el error sigue estando actualizado

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

Pasos

1. Seleccione el extremo.

Aparece la página de detalles del extremo.

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

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

Resolver errores de punto final

Puede utilizar el mensaje **último error** de la página de detalles del punto final para ayudar a determinar qué está causando el error. Es posible que algunos errores requieran que edite el extremo para resolver el

problema. Por ejemplo, se puede producir un error CloudMirroring si StorageGRID no puede acceder al bloque de S3 de destino porque no tiene los permisos de acceso correctos o si la clave de acceso ha caducado. El mensaje es "es necesario actualizar las credenciales del punto final o el acceso al destino" y los detalles son "ACCESSDENIED" o "InvalidAccessKeyId".

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

Pasos

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

Credenciales de extremo con permisos insuficientes

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

Solución de problemas de servicios de plataforma adicionales

Para obtener información adicional sobre la solución de problemas de los servicios de la plataforma, consulte las instrucciones para administrar StorageGRID.

[Administre StorageGRID](#)

Información relacionada

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

[Probar la conexión para el extremo de servicios de la plataforma](#)

[Editar extremo de servicios de plataforma](#)

Configure la replicación de CloudMirror

La [Servicio de replicación de CloudMirror](#) Es uno de los tres servicios de plataforma de StorageGRID. Puede usar la replicación de CloudMirror para replicar automáticamente objetos en un bloque de S3 externo.

Lo que necesitará

- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe haber creado un bloque para actuar como origen de replicación.
- El extremo que pretende usar como destino de la replicación de CloudMirror ya debe existir y debe tener su URN.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz, que le permite administrar la configuración de todos los segmentos S3 de su cuenta de inquilino.

Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

La replicación de CloudMirror copia los objetos de un bloque de origen en un bloque de destino que se especifique en un extremo. Para habilitar la replicación de CloudMirror en un bloque, debe crear y aplicar un XML de configuración de replicación de bloques válido. El XML de configuración de replicación debe usar la URN de un extremo de bloque de S3 para cada destino.



La replicación no es compatible con buckets de origen o destino con el bloqueo de objetos S3 habilitado.

Para obtener información general sobre la replicación de bloques y cómo configurarla, consulte la documentación de Amazon Simple Storage Service (S3) sobre la replicación entre regiones (CRR). Para obtener más información sobre cómo StorageGRID implementa la API de configuración de la replicación de bloques de S3, consulte [Instrucciones para implementar aplicaciones cliente de S3](#).

Si habilita la replicación de CloudMirror en un bloque que contiene objetos, se replican los objetos nuevos agregados al bloque, pero no los objetos existentes en el bloque. Debe actualizar los objetos existentes para activar la replicación.

Si se especifica una clase de almacenamiento en el XML de configuración de replicación, StorageGRID utiliza esa clase al realizar operaciones en el extremo de S3 de destino. El extremo de destino también debe admitir la clase de almacenamiento especificada. Asegúrese de seguir las recomendaciones que proporciona el proveedor del sistema de destino.

Pasos

1. Habilite la replicación para su bloque de origen:

Utilice un editor de texto para crear el XML de configuración de replicación necesario para habilitar la replicación, tal y como se especifica en la API de replicación de S3. Al configurar XML:

- Tenga en cuenta que StorageGRID solo admite V1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso de `Filter` Elemento para reglas y sigue las convenciones V1 para eliminar versiones de objetos. Consulte la documentación de Amazon sobre la configuración de replicación para obtener más información.
- Use el URN de un extremo de bloque de S3 como destino.
- Si lo desea, puede agregar el `<StorageClass>` y especifique una de las siguientes opciones:
 - `STANDARD`: La clase de almacenamiento predeterminada. Si no se especifica una clase de almacenamiento al cargar un objeto, el `STANDARD` se utiliza la clase de almacenamiento.
 - `STANDARD_IA`: (Estándar - acceso poco frecuente.) Utilice esta clase de almacenamiento para los datos a los que se accede con menor frecuencia; sin embargo, este proceso requiere un acceso rápido cuando sea necesario.
 - `REDUCED_REDUNDANCY`: Utilice esta clase de almacenamiento para datos no críticos y reproducibles que se pueden almacenar con menos redundancia que el `STANDARD` clase de almacenamiento.
- Si especifica un `Role` En el XML de configuración se ignorará. StorageGRID no utiliza este valor.

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

2. En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3) > Cuchos**.
3. Seleccione el nombre del bloque de origen.

Aparece la página de detalles bucket.

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

Bucket options

Bucket access

Platform services

Replication

Disabled

Enable the CloudMirror replication service to copy objects from a source bucket to a destination bucket that is specified in an endpoint.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for each destination bucket.
- You must specify the URN of each endpoint in the replication configuration XML for the source bucket.

☒ Enable replication

Clear

```

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

```

Save changes



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:

- 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".

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

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

Información relacionada

[Use S3](#)

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

Configure las notificaciones de eventos

El servicio de notificaciones es uno de los tres servicios de la plataforma StorageGRID. Puede habilitar las notificaciones de un bloque para enviar información acerca de los eventos especificados a un servicio de destino que admita AWS simple Notification Service™ (SNS).

Lo que necesitará

- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe haber creado un bloque para que actúe como el origen de las notificaciones.
- Debe haber el extremo que se pretende usar como destino de las notificaciones de eventos y su URN debe estar presente.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz, que le permite administrar la configuración de todos los segmentos S3 de su cuenta de inquilino. Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

Después de configurar las notificaciones de eventos, cada vez que se produce un evento especificado para un objeto del bloque de origen, se genera una notificación y se envía al tema Servicio de notificación simple (SNS) que se utiliza como extremo de destino. Para habilitar las notificaciones para un bloque, debe crear y aplicar un XML de configuración de notificación válido. El XML de configuración de notificaciones debe usar el URN de un extremo de notificaciones de eventos para cada destino.

Para obtener información general sobre las notificaciones de eventos y cómo configurarlas, consulte la documentación de Amazon. Para obtener más información sobre cómo StorageGRID implementa la API de configuración de notificaciones de bloques de S3, consulte las instrucciones para implementar aplicaciones de cliente S3.

Si habilita las notificaciones de eventos para un bloque que contiene objetos, las notificaciones se envían solo para las acciones que se realizan una vez guardada la configuración de notificación.

Pasos

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

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

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

3. Seleccione el nombre del bloque de origen.

Aparece la página de detalles bucket.

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

5. Active la casilla de verificación **Activar notificaciones de eventos**.

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

Bucket options

Bucket access

Platform services

Replication

Disabled

▼

Event notifications

Disabled

▲

Enable the event notification service for an S3 bucket if you want StorageGRID to send notifications about specified events to a destination Amazon Simple Notification Service (SNS).

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the destination of event notifications.
- You must specify the URN of that endpoint in the notification configuration XML for the source bucket.

☒ Enable event notifications

Clear

```

<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>
  </TopicConfiguration>
</NotificationConfiguration>

```

Save changes



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:

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

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

- b. Confirme que se ha entregado una notificación al tema SNS de destino.

Por ejemplo, si el tema de destino está alojado en el servicio de notificación simple (SNS) de AWS, puede configurar el servicio para que le envíe un correo electrónico cuando se entrega la notificación.

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "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 S3](#)

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

Utilice el servicio de integración de búsqueda

El servicio de integración de búsqueda es uno de los tres servicios de la plataforma StorageGRID. Este servicio puede habilitar el envío de metadatos de objetos a un índice de búsqueda de destino siempre que se cree, se elimine o actualice los metadatos o las etiquetas de un objeto.

Puede configurar la integración de búsqueda mediante el Administrador de inquilinos para aplicar XML de configuración de StorageGRID personalizado a un bloque.



Debido a que el servicio de integración de búsqueda hace que los metadatos de objeto se envíen a un destino, su XML de configuración se denomina XML_ de configuración de notificación de metadatos. Este XML de configuración es diferente al *notification Configuration XML* utilizado para habilitar las notificaciones de eventos.

Consulte [Instrucciones para implementar aplicaciones cliente de S3](#) Para obtener detalles sobre las siguientes operaciones personalizadas de la API de REST de StorageGRID S3:

- DELETE bucket metadata notification Configuration
- OBTENGA la solicitud de configuración de notificación de metadatos del bloque
- PUT bucket metadata notification Configuration

Información relacionada

[XML de configuración para la integración de búsqueda](#)

[Metadatos de objetos incluidos en las notificaciones de metadatos](#)

[JSON generado por el servicio de integración de búsqueda](#)

[Configure el servicio de integración de búsqueda](#)

[Use S3](#)

XML de configuración para la integración de búsqueda

El servicio de integración de búsqueda se configura mediante un conjunto de reglas contenidas en `<MetadataNotificationConfiguration>` y `</MetadataNotificationConfiguration>` etiquetas. Cada regla especifica los objetos a los que se aplica la regla y el destino al que StorageGRID debe enviar los metadatos de esos objetos.

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

Los destinos deben especificarse mediante el URN de un extremo de StorageGRID que se ha creado para el servicio de integración de búsqueda. Estos extremos se refieren a un índice y tipo definidos en un clúster de Elasticsearch.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

En la tabla se describen los elementos del XML de configuración de notificaciones de metadatos.

Nombre	Descripción	Obligatorio
MetadataNotificationConfiguration	Etiqueta de contenedor para las reglas que se usan para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o más elementos Regla.	Sí
Regla	Código de contenedor de una regla que identifica los objetos cuyos metadatos deben agregarse a un índice especificado. Se rechazan las reglas con prefijos superpuestos. Incluido en el elemento MetadataNotificationConfiguration.	Sí
ID	Identificador único de la regla. Incluido en el elemento Regla.	No

Nombre	Descripción	Obligatorio
Estado	<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
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"> • es debe ser el tercer elemento. • El URN debe terminar con el índice y el tipo donde se almacenan los metadatos, en el formulario <code>domain-name/myindex/mytype</code>. <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"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mystore:es:::mydomain/myindex/mytype</code> <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

Utilice el XML de configuración de notificación de metadatos de ejemplo para aprender a crear su propio XML.

La configuración de notificaciones de metadatos se aplica a todos los objetos

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

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

Configuración de notificaciones de metadatos con dos reglas

En este ejemplo, metadatos de objeto para objetos que coinciden con el prefijo `/images` se envía a un destino, mientras que los metadatos de objetos de los objetos que coinciden con el prefijo `/videos` se envía a un segundo destino.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Información relacionada

[Use S3](#)

[Metadatos de objetos incluidos en las notificaciones de metadatos](#)

[JSON generado por el servicio de integración de búsqueda](#)

[Configure el servicio de integración de búsqueda](#)

Configure el servicio de integración de búsqueda

El servicio de integración de búsqueda envía metadatos de objetos a un índice de búsqueda de destino cada vez que se crea, se elimina o se actualizan sus metadatos o etiquetas.

Lo que necesitará

- Un administrador de StorageGRID debe habilitar los servicios de plataforma para su cuenta de inquilino.
- Debe haber creado un bloque de S3 cuyo contenido desea indexar.
- El extremo que pretende usar como destino del servicio de integración de búsqueda ya debe existir y debe tener su URN.
- Debe pertenecer a un grupo de usuarios que tenga el permiso Administrar todos los cucharones o acceso raíz, que le permite administrar la configuración de todos los segmentos S3 de su cuenta de inquilino. Estos permisos anulan la configuración de permisos de las directivas de grupo o de bloque al configurar el bloque mediante el Administrador de inquilinos.

Acerca de esta tarea

Después de configurar el servicio de integración de búsqueda para un bloque de origen, al crear un objeto o actualizar los metadatos o las etiquetas de un objeto se activan los metadatos de objeto que se enviarán al extremo de destino. Si habilita el servicio de integración de búsqueda para un bloque que ya contiene objetos, las notificaciones de metadatos no se envían automáticamente para los objetos existentes. Debe actualizar estos objetos existentes para asegurarse de que sus metadatos se agregan al índice de búsqueda de destino.

Pasos

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

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:1111111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

2. En el Administrador de inquilinos, seleccione **ALMACENAMIENTO (S3) > Cuchos**.
3. Seleccione el nombre del bloque de origen.

Aparece la página de detalles bucket.

4. Seleccione **Servicios de plataforma > integración de búsqueda**

5. Active la casilla de verificación **Activar integración de búsqueda**.
6. Pegue la configuración de notificación de metadatos en el cuadro de texto y seleccione **Guardar cambios**.

Platform services

Replication Disabled

Event notifications Disabled

Search integration Disabled

Enable the search integration service to send object metadata to a destination search index whenever an object is created, deleted, or its metadata or tags are updated.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the search integration service.
- You must specify the URN of that endpoint in the search integration configuration XML for the bucket you want to index.

☒ Enable search integration

Clear

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Save changes



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

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

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

de metadatos.

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

Después de terminar

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

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

Información relacionada

[Comprender el servicio de integración de búsquedas](#)

[XML de configuración para la integración de búsqueda](#)

[Use S3](#)

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

JSON generado por el servicio de integración de búsqueda

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

Este ejemplo muestra un ejemplo de JSON que se podría generar cuando un objeto con la clave SGWS/Tagging.txt se crea en un bloque llamado test. La test el bloque no tiene versiones, por lo que el versionId la etiqueta está vacía.

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

Metadatos de objetos incluidos en las notificaciones de metadatos

En la tabla se enumeran todos los campos que se incluyen en el documento JSON que se envían al extremo de destino cuando la integración de búsqueda está habilitada.

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

Tipo	Nombre y descripción del artículo
Información sobre bloques y objetos	bucket: Nombre del cubo
key: Nombre de clave de objeto	versionID: Versión de objeto, para objetos en cubos con versiones
region: Región de cucharón, por ejemplo us-east-1	Metadatos del sistema
size: Tamaño del objeto (en bytes) visible para un cliente HTTP	md5: Hash de objeto
Metadatos del usuario	metadata: Todos los metadatos de usuario del objeto, como pares clave-valor key:value
Etiquetas	tags: Todas las etiquetas de objeto definidas para el objeto, como pares clave-valor key:value



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

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.