Administrar los servicios de la plataforma S3

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Administrar los servicios de la plataforma S3

Servicios de la plataforma S3

Descripción general y consideraciones sobre los servicios de la plataforma

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

Para obtener información sobre S3, consulte"Utilice la API REST de S3" .

Descripción general de los servicios de la plataforma

Los servicios de la plataforma StorageGRID pueden ayudarlo a implementar una estrategia de nube híbrida al permitirle enviar notificaciones de eventos y copias de objetos S3 y metadatos de objetos a destinos externos.

Dado que la ubicación de destino de los servicios de plataforma generalmente es externa a su implementación de StorageGRID , los servicios de plataforma le brindan la potencia y la flexibilidad que brinda el uso de recursos de almacenamiento externos, servicios de notificación y servicios de búsqueda o análisis para sus datos.

Se puede configurar cualquier combinación de servicios de plataforma para un único bucket S3. Por ejemplo, puede configurar tanto el"Servicio CloudMirror" y"notificaciones" en un bucket S3 de StorageGRID para que pueda reflejar objetos específicos en Amazon Simple Storage Service (S3) y, al mismo tiempo, enviar una notificación sobre cada uno de esos objetos a una aplicación de monitoreo de terceros para ayudarlo a realizar un seguimiento de sus gastos de AWS.

El uso de los servicios de la plataforma debe ser habilitado para cada cuenta de inquilino por un administrador de StorageGRID mediante Grid Manager o la API de administración de Grid.

Cómo se configuran los servicios de la plataforma

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

Después de crear un punto final externo, puede habilitar un servicio de plataforma para un depósito agregando una configuración XML al depósito. La configuración XML identifica los objetos sobre los que debe actuar el depósito, la acción que debe realizar el depósito y el punto final que debe utilizar el depósito para el servicio.

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

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

El formato del XML de configuración está regido por las API REST de S3 utilizadas para implementar los servicios de la plataforma StorageGRID :

Servicio de plataforma	API REST de S3	Referirse a
Replicación de CloudMirror	• Obtener réplica de cubo • Replicación de PutBucket	• "Replicación de CloudMirror" • "Operaciones en buckets"
Notificaciones	• Configuración de GetBucketNotification • Configuración de notificación de PutBucket	• "Notificaciones" • "Operaciones en buckets"
Integración de búsqueda	• Configuración de notificación de metadatos del depósito GET • Configuración de notificación de metadatos del depósito PUT	• "Integración de búsqueda" • "Operaciones personalizadas de StorageGRID"

Consideraciones para el uso de servicios de plataforma

Consideración	Detalles
Monitoreo de puntos finales de destino	Debes supervisar la disponibilidad de cada punto final de destino. Si se pierde la conectividad con el punto final de destino durante un período prolongado y existe una gran acumulación de solicitudes, las solicitudes de cliente adicionales (como las solicitudes PUT) a StorageGRID fallarán. Debes volver a intentar estas solicitudes fallidas cuando el punto final sea accesible.
Limitación del punto final de destino	El software StorageGRID puede limitar las solicitudes S3 entrantes para un bucket si la velocidad a la que se envían las solicitudes excede la velocidad a la que el punto final de destino puede recibirlas. La limitación solo se produce cuando hay una acumulación de solicitudes en espera de ser enviadas al punto final de destino. El único efecto visible es que las solicitudes S3 entrantes tardarán más en ejecutarse. Si comienza a detectar un rendimiento significativamente más lento, debe reducir la tasa de ingesta o utilizar un punto final con mayor capacidad. Si la acumulación de solicitudes continúa creciendo, las operaciones S3 del cliente (como las solicitudes PUT) eventualmente fallarán. Es más probable que las solicitudes de CloudMirror se vean afectadas por el rendimiento del punto final de destino porque estas solicitudes generalmente implican más transferencia de datos que las solicitudes de integración de búsqueda o notificación de eventos.

Consideración	Detalles
Garantías de pedidos	StorageGRID garantiza el orden de las operaciones en un objeto dentro de un sitio. Siempre que todas las operaciones contra un objeto se realicen dentro del mismo sitio, el estado final del objeto (para la replicación) siempre será igual al estado en StorageGRID. StorageGRID hace todo lo posible para ordenar las solicitudes cuando se realizan operaciones en los sitios de StorageGRID . Por ejemplo, si escribe un objeto inicialmente en el sitio A y luego sobrescribe el mismo objeto en el sitio B, no se garantiza que el objeto final replicado por CloudMirror en el depósito de destino sea el objeto más nuevo.
Eliminaciones de objetos impulsadas por ILM	Para que coincida con el comportamiento de eliminación de AWS CRR y Amazon Simple Notification Service, las solicitudes de notificación de eventos y CloudMirror no se envían cuando se elimina un objeto en el bucket de origen debido a las reglas ILM de StorageGRID . Por ejemplo, no se envían solicitudes de notificaciones de eventos ni de CloudMirror si una regla ILM elimina un objeto después de 14 días. Por el contrario, las solicitudes de integración de búsqueda se envían cuando se eliminan objetos debido a ILM.
Uso de puntos finales de Kafka	Para los puntos finales de Kafka, no se admite TLS mutuo. Como resultado, si tienes `ssl.client.auth` empezar a `required` en la configuración de su agente de Kafka, podría causar problemas de configuración del punto final de Kafka. La autenticación de los puntos finales de Kafka utiliza los siguientes tipos de autenticación. Estos tipos son diferentes de los que se utilizan para la autenticación de otros puntos finales, como Amazon SNS, y requieren credenciales de nombre de usuario y contraseña. • SASL/LLANO • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Nota:** Las configuraciones del proxy de almacenamiento configuradas no se aplican a los puntos finales de los servicios de la plataforma Kafka.

Consideraciones para utilizar el servicio de replicación CloudMirror

Consideración	Detalles
Estado de replicación	StorageGRID no es compatible con `x-amz-replication-status` encabezamiento.

Consideración	Detalles
Tamaño del objeto	El tamaño máximo de los objetos que el servicio de replicación CloudMirror puede replicar en un depósito de destino es de 5 TiB, que es el mismo que el tamaño máximo de objeto *compatible*. **Nota**: El tamaño máximo *recomendado* para una sola operación PutObject es 5 GiB (5.368.709.120 bytes). Si tiene objetos de más de 5 GiB, utilice la carga multiparte en su lugar.
Control de versiones de bucket e ID de versiones	Si el depósito S3 de origen en StorageGRID tiene habilitada la gestión de versiones, también debe habilitarla para el depósito de destino. Al utilizar versiones, tenga en cuenta que el orden de las versiones de los objetos en el depósito de destino es el máximo esfuerzo y no está garantizado por el servicio CloudMirror, debido a las limitaciones del protocolo S3. **Nota**: Los ID de versión del depósito de origen en StorageGRID no están relacionados con los ID de versión del depósito de destino.
Etiquetado de versiones de objetos	El servicio CloudMirror no replica ninguna solicitud PutObjectTagging o DeleteObjectTagging que proporcione un ID de versión, debido a limitaciones en el protocolo S3. Debido a que los ID de versión para el origen y el destino no están relacionados, no hay forma de garantizar que se replique una actualización de etiqueta a un ID de versión específico. Por el contrario, el servicio CloudMirror replica solicitudes PutObjectTagging o DeleteObjectTagging que no especifican un ID de versión. Estas solicitudes actualizan las etiquetas para la última clave (o la última versión si el depósito tiene versión). Las ingestas normales con etiquetas (no actualizaciones de etiquetas) también se replican.
Cargas multiparte y `ETag` valores	Al reflejar objetos que se cargaron mediante una carga multiparte, el servicio CloudMirror no conserva las partes. Como resultado, la `ETag` El valor del objeto reflejado será diferente al `ETag` valor del objeto original.
Objetos cifrados con SSE-C (cifrado del lado del servidor con claves proporcionadas por el cliente)	El servicio CloudMirror no admite objetos cifrados con SSE-C. Si intenta ingerir un objeto en el bucket de origen para la replicación de CloudMirror y la solicitud incluye los encabezados de solicitud SSE-C, la operación fallará.
Cubo con bloqueo de objetos S3 habilitado	La replicación no es compatible con los depósitos de origen o destino que tengan el bloqueo de objetos S3 habilitado.

Comprender el servicio de replicación CloudMirror

Puede habilitar la replicación de CloudMirror para un bucket S3 si desea que StorageGRID replique objetos específicos agregados al bucket en uno o más buckets de destino externos.

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

> La replicación de CloudMirror no es compatible si el depósito de origen tiene habilitado el bloqueo de objetos S3.

CloudMirror e ILM

La replicación de CloudMirror funciona independientemente de las políticas ILM activas de la red. El servicio CloudMirror replica los objetos a medida que se almacenan en el depósito de origen y los envía al depósito de destino lo antes posible. La entrega de objetos replicados se activa cuando la ingesta del objeto se realiza correctamente.

CloudMirror y replicación entre redes

La replicación de CloudMirror tiene similitudes y diferencias importantes con la función de replicación entre redes. Consulte "Comparar la replicación entre redes y la replicación de CloudMirror" .

Cubos de CloudMirror y S3

La replicación de CloudMirror normalmente está configurada para utilizar un depósito S3 externo como destino. Sin embargo, también puede configurar la replicación para utilizar otra implementación de StorageGRID o cualquier servicio compatible con S3.

Cubos existentes

Cuando habilita la replicación de CloudMirror para un depósito existente, solo se replican los nuevos objetos agregados a ese depósito. Cualquier objeto existente en el depósito no se replica. Para forzar la replicación de objetos existentes, puede actualizar los metadatos del objeto existente realizando una copia del objeto.

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

Cubos de destino múltiples

Para replicar objetos de un solo depósito en varios depósitos de destino, especifique el destino de cada regla en el XML de configuración de replicación. No es posible replicar un objeto en más de un bucket al mismo tiempo.

Cubos versionados o no versionados

Puede configurar la replicación de CloudMirror en depósitos versionados o no versionados. Los depósitos de destino pueden tener versiones o no. Puede utilizar cualquier combinación de depósitos versionados y no versionados. Por ejemplo, puede especificar un depósito versionado como destino para un depósito de origen no versionado, o viceversa. También puedes replicar entre depósitos sin versiones.

Eliminación, bucles de replicación y eventos

Comportamiento de eliminación

Es lo mismo que el comportamiento de eliminación del servicio Amazon S3, Replicación entre regiones (CRR). Eliminar un objeto en un depósito de origen nunca elimina un objeto replicado en el destino. Si tanto el depósito de origen como el de destino tienen versiones, se replica el marcador de eliminación. Si el depósito de destino no tiene versión, eliminar un objeto en el depósito de origen no replica el marcador de

eliminación en el depósito de destino ni elimina el objeto de destino.

Protección contra bucles de replicación

A medida que los objetos se replican en el depósito de destino, StorageGRID los marca como "réplicas". Un depósito StorageGRID de destino no volverá a replicar objetos marcados como réplicas, lo que lo protege de bucles de replicación accidentales. Esta marca de réplica es interna a StorageGRID y no le impide aprovechar AWS CRR cuando usa un bucket de Amazon S3 como destino.

> El encabezado personalizado utilizado para marcar una réplica es `x-ntap-sg-replica` . Esta marca evita que se forme un espejo en cascada. StorageGRID admite un CloudMirror bidireccional entre dos redes.

Eventos en el bucket de destino

No se garantiza la singularidad ni el orden de los eventos en el depósito de destino. Es posible que se entregue más de una copia idéntica de un objeto de origen al destino como resultado de las operaciones realizadas para garantizar el éxito de la entrega. En casos excepcionales, cuando el mismo objeto se actualiza simultáneamente desde dos o más sitios StorageGRID diferentes, el orden de las operaciones en el depósito de destino podría no coincidir con el orden de los eventos en el depósito de origen.

Comprender las notificaciones de los buckets

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

Por ejemplo, puede configurar alertas para que se envíen a los administradores sobre cada objeto agregado a un depósito, donde los objetos representan archivos de registro asociados con un evento crítico del sistema.

Las notificaciones de eventos se crean en el depósito de origen según lo especificado en la configuración de notificación y se envían al destino. Si un evento asociado con un objeto tiene éxito, se crea una notificación sobre ese evento y se pone en cola para su entrega.

No se garantiza la singularidad ni el orden de las notificaciones. Es posible que se envíe más de una notificación de un evento al destino como resultado de las operaciones realizadas para garantizar el éxito de la entrega. Y debido a que la entrega es asincrónica, no se garantiza que el orden temporal de las notificaciones en el destino coincida con el orden de los eventos en el depósito de origen, en particular para las operaciones que se originan en diferentes sitios de StorageGRID . Puedes utilizar el `sequencer` Introduzca la clave en el mensaje de evento para determinar el orden de los eventos para un objeto en particular, como se describe en la documentación de Amazon S3.

Las notificaciones de eventos de StorageGRID siguen la API de Amazon S3 con algunas limitaciones.

- Se admiten los siguientes tipos de eventos:
  - s3:ObjetoCreado:
  - s3:ObjetoCreado:Poner
  - s3:ObjetoCreado:Publicación
  - s3:ObjetoCreado:Copiar
  - s3:Objeto creado:Carga multiparte completa
  - s3:Objeto eliminado:

- s3:ObjetoEliminado:Eliminar
- s3:Objeto eliminado:Eliminar marcador creado
- s3:Restaurar objeto:Publicar

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

Nombre de la clave	Valor de StorageGRID
Fuente del evento	`sgws:s3`
Región de AWS	*no incluido*
x-amz-id-2	*no incluido*
arn	`urn:sgws:s3:::bucket_name`

Comprender el servicio de integración de búsqueda

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

El servicio de integración de búsqueda es un servicio StorageGRID personalizado que envía de forma automática y asincrónica metadatos de objetos S3 a un punto final de destino cada vez que se crea o elimina un objeto, o se actualizan sus metadatos o etiquetas. Luego, puede utilizar herramientas sofisticadas de búsqueda, análisis de datos, visualización o aprendizaje automático proporcionadas por el servicio de destino para buscar, analizar y obtener información de los datos de sus objetos.

Por ejemplo, puede configurar sus depósitos para enviar metadatos de objetos S3 a un servicio Elasticsearch remoto. Luego, puede usar Elasticsearch para realizar búsquedas en diferentes grupos y realizar análisis sofisticados de patrones presentes en los metadatos de sus objetos.

Si bien la integración de Elasticsearch se puede configurar en un bucket con S3 Object Lock habilitado, los metadatos de S3 Object Lock (incluidos Conservar hasta la fecha y el estado de Retención legal) de los objetos no se incluirán en los metadatos enviados a Elasticsearch.

> Debido a que el servicio de integración de búsqueda hace que se envíen metadatos de objetos a un destino, su XML de configuración se denomina "XML de configuración de notificación *metadata*". Este XML de configuración es diferente del "XML de configuración de notificación" utilizado para habilitar las notificaciones de *eventos*.

Integración de búsquedas y buckets S3

Puede habilitar el servicio de integración de búsqueda para cualquier depósito con o sin versión. La integración de búsqueda se configura asociando el XML de configuración de notificación de metadatos con el depósito que especifica sobre qué objetos actuar y el destino de los metadatos del objeto.

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

Para las etiquetas y los metadatos del usuario, StorageGRID pasa fechas y números a Elasticsearch como cadenas o como notificaciones de eventos S3. Para configurar Elasticsearch para que interprete estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para el mapeo de campos dinámicos y para el mapeo de formatos de fecha. Debe habilitar las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Una vez indexado un documento, no es posible editar los tipos de campos del documento en el índice.

Notificaciones de búsqueda

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

- Se crea un objeto.
- Se elimina un objeto, incluso cuando se eliminan objetos como resultado de la operación de la política ILM de la red.
- Se agregan, actualizan o eliminan metadatos o etiquetas de objetos. Al actualizar, siempre se envía el conjunto completo de metadatos y etiquetas, no solo los valores modificados.

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

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

Servicio de integración de búsqueda y Elasticsearch

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

Administrar puntos finales de servicios de la plataforma

Configurar puntos finales de servicios de la plataforma

Antes de poder configurar un servicio de plataforma para un bucket, debe configurar al menos un punto final para que sea el destino del servicio de plataforma.

El acceso a los servicios de la plataforma lo habilita un administrador de StorageGRID por inquilino. Para crear o usar un punto final de servicios de plataforma, debe ser un usuario inquilino con permiso de acceso Administrar puntos finales o Raíz, en una red cuya red haya sido configurada para permitir que los nodos de almacenamiento accedan a recursos de puntos finales externos. Para un solo inquilino, puede configurar un máximo de 500 puntos finales de servicios de plataforma. Comuníquese con su administrador de StorageGRID para obtener más información.

¿Qué es un punto final de servicios de plataforma?

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

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

Cada tipo de servicio de plataforma requiere su propio punto final, por lo que debe configurar al menos un punto final para cada servicio de plataforma que planea utilizar. Después de definir un punto final de servicios de plataforma, utilice el URN del punto final como destino en el XML de configuración utilizado para habilitar el servicio.

Puede utilizar el mismo punto final como destino para más de un depósito de origen. Por ejemplo, puede configurar varios depósitos de origen para enviar metadatos de objetos al mismo punto final de integración de búsqueda para poder realizar búsquedas en varios depósitos. También puede configurar un bucket de origen para usar más de un punto final como destino, lo que le permite hacer cosas como enviar notificaciones sobre la creación de objetos a un tema de Amazon Simple Notification Service (Amazon SNS) y notificaciones sobre la eliminación de objetos a un segundo tema de Amazon SNS.

Puntos finales para la replicación de CloudMirror

StorageGRID admite puntos finales de replicación que representan depósitos S3. Estos depósitos pueden estar alojados en Amazon Web Services, en el mismo StorageGRID o en una implementación remota del mismo, o en otro servicio.

Puntos finales para notificaciones

StorageGRID admite puntos finales de Amazon SNS y Kafka. No se admiten los puntos finales de Simple Queue Service (SQS) ni de AWS Lambda.

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

Puntos finales para el servicio de integración de búsqueda

StorageGRID admite puntos finales de integración de búsqueda que representan clústeres de Elasticsearch. Estos clústeres de Elasticsearch pueden estar en un centro de datos local o alojados en una nube de AWS o en otro lugar.

El punto final de integración de búsqueda hace referencia a un índice y tipo de Elasticsearch específicos. Debe crear el índice en Elasticsearch antes de crear el punto final en StorageGRID, de lo contrario la creación del punto final fallará. No es necesario crear el tipo antes de crear el punto final. StorageGRID creará el tipo si es necesario cuando envíe metadatos del objeto al punto final.

Información relacionada

"Administrar StorageGRID"

Especificar URN para el punto final de los servicios de la plataforma

Cuando crea un punto final de servicios de plataforma, debe especificar un nombre de recurso único (URN). Utilizará la URN para hacer referencia al punto final cuando cree

un XML de configuración para el servicio de la plataforma. La URN de cada punto final debe ser única.

StorageGRID valida los puntos finales de los servicios de la plataforma a medida que los crea. Antes de crear un punto final de servicios de plataforma, confirme que el recurso especificado en el punto final exista y que se pueda acceder a él.

Elementos URN

El URN para un punto final de servicios de plataforma debe comenzar con `arn:aws` o `urn:mysite` , de la siguiente manera:

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

Por ejemplo, si está especificando el URN para un punto final de CloudMirror alojado en StorageGRID, el URN podría comenzar con `urn:sgws` .

El siguiente elemento de la URN especifica el tipo de servicio de plataforma, de la siguiente manera:

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

Por ejemplo, para continuar especificando el URN para un punto final de CloudMirror alojado en StorageGRID, agregaría `s3` Llegar `urn:sgws:s3` .

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

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

URN para servicios alojados en AWS y GCP

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

- Replicación de CloudMirror:

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

- Notificaciones:

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

- Integración de búsqueda:

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

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

URN para servicios alojados localmente

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

- Replicación de CloudMirror:

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

  Para un punto final de CloudMirror alojado en StorageGRID, puede especificar un URN válido que comience con `urn:sgws` :

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

- Notificaciones:

  Especifique un punto final de Amazon Simple Notification Service:

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

  Especifique un punto final de Kafka:

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

- Integración de búsqueda:

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

> Para los puntos finales de integración de búsqueda alojados localmente, el `domain-name` El elemento puede ser cualquier cadena siempre que la URN del punto final sea única.

Crear punto final de servicios de plataforma

Debe crear al menos un punto final del tipo correcto antes de poder habilitar un servicio de plataforma.

Antes de empezar

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

    > Si planea utilizar un depósito alojado en un sistema StorageGRID como punto final para la replicación de CloudMirror, comuníquese con el administrador de la red para determinar los valores que debe ingresar.

  - Nombre único de recurso (URN)

    "Especificar URN para el punto final de los servicios de la plataforma"

  - Credenciales de autenticación (si es necesario):

Puntos finales de integración de búsqueda

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

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

Puntos finales de replicación de CloudMirror

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

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

Puntos finales de Amazon SNS

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

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

Puntos finales de Kafka

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

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

  - Certificado de seguridad (si se utiliza un certificado CA personalizado)

- Si las funciones de seguridad de Elasticsearch están habilitadas, tiene el privilegio de clúster de monitorización para realizar pruebas de conectividad y el privilegio de escritura de índice o los privilegios de índice y eliminación de índice para las actualizaciones de documentos.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Puntos finales de servicios de plataforma**. Aparece la página de puntos finales de servicios de la plataforma.
2. Seleccione **Crear punto final**.
3. Ingrese un nombre para mostrar para describir brevemente el punto final y su propósito.

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

4. En el campo **URI**, especifique el Identificador único de recurso (URI) del punto final.

   Utilice uno de los siguientes formatos:

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

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

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

Por ejemplo, el URI de un depósito alojado en StorageGRID podría ser:

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

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

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

De manera similar, el URI de un bucket alojado en AWS podría ser:

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

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

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

> No se puede cambiar el URN de un punto final una vez creado el punto final.

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

Puntos finales de integración de búsqueda

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

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

Tipo de autenticación	Descripción	Cartas credenciales
Anónimo	Proporciona acceso anónimo al destino. Sólo funciona para puntos finales que tienen la seguridad deshabilitada.	Sin autenticación.
Tecla de acceso	Utiliza credenciales de estilo AWS para autenticar las conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta
HTTP básico	Utiliza un nombre de usuario y una contraseña para autenticar las conexiones al destino.	• Nombre de usuario • Password

Puntos finales de replicación de CloudMirror

Ingrese o cargue las credenciales para un punto final de replicación de CloudMirror.

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

Tipo de autenticación	Descripción	Cartas credenciales
Anónimo	Proporciona acceso anónimo al destino. Sólo funciona para puntos finales que tienen la seguridad deshabilitada.	Sin autenticación.
Tecla de acceso	Utiliza credenciales de estilo AWS para autenticar las conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta

Tipo de autenticación	Descripción	Cartas credenciales
CAP (Portal de acceso C2S)	Utiliza certificados y claves para autenticar las conexiones al destino.	• URL de credenciales temporales • Certificado de CA del servidor (carga de archivo PEM) • Certificado de cliente (carga de archivo PEM) • Clave privada del cliente (carga de archivo PEM, formato cifrado OpenSSL o formato de clave privada sin cifrar) • Frase de contraseña de la clave privada del cliente (opcional)

Puntos finales de Amazon SNS

Ingrese o cargue las credenciales para un punto final de Amazon SNS.

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

Tipo de autenticación	Descripción	Cartas credenciales
Anónimo	Proporciona acceso anónimo al destino. Sólo funciona para puntos finales que tienen la seguridad deshabilitada.	Sin autenticación.
Tecla de acceso	Utiliza credenciales de estilo AWS para autenticar las conexiones con el destino.	• ID de clave de acceso • Clave de acceso secreta

Puntos finales de Kafka

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

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

Tipo de autenticación	Descripción	Cartas credenciales
Anónimo	Proporciona acceso anónimo al destino. Sólo funciona para puntos finales que tienen la seguridad deshabilitada.	Sin autenticación.
SASL/LLANO	Utiliza un nombre de usuario y una contraseña con texto sin formato para autenticar las conexiones al destino.	• Nombre de usuario • Password

Tipo de autenticación	Descripción	Cartas credenciales
SASL/SCRAM-SHA-256	Utiliza un nombre de usuario y una contraseña mediante un protocolo de desafío-respuesta y hash SHA-256 para autenticar las conexiones al destino.	• Nombre de usuario • Password
SASL/SCRAM-SHA-512	Utiliza un nombre de usuario y una contraseña mediante un protocolo de desafío-respuesta y hash SHA-512 para autenticar las conexiones al destino.	• Nombre de usuario • Password

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

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

Tipo de verificación del certificado	Descripción
Utilice un certificado CA personalizado	Utilice un certificado de seguridad personalizado. Si selecciona esta configuración, copie y pegue el certificado de seguridad personalizado en el cuadro de texto **Certificado CA**.
Utilice el certificado CA del sistema operativo	Utilice el certificado CA de Grid predeterminado instalado en el sistema operativo para proteger las conexiones.
No verificar el certificado	El certificado utilizado para la conexión TLS no está verificado. Esta opción no es segura.

10. Seleccione **Probar y crear punto final**.
    - Aparece un mensaje de éxito si se puede acceder al punto final utilizando las credenciales especificadas. La conexión al punto final se valida desde un nodo en cada sitio.
    - Aparece un mensaje de error si falla la validación del punto final. Si necesita modificar el punto final para corregir el error, seleccione **Regresar a los detalles del punto final** y actualice la información. Luego, seleccione **Probar y crear punto final**.

> La creación de puntos finales falla si los servicios de la plataforma no están habilitados para su cuenta de inquilino. Comuníquese con su administrador de StorageGRID .

Después de haber configurado un punto final, puede usar su URN para configurar un servicio de plataforma.

Información relacionada

- "Especificar URN para el punto final de los servicios de la plataforma"
- "Configurar la replicación de CloudMirror"
- "Configurar notificaciones de eventos"
- "Configurar el servicio de integración de búsqueda"

Conexión de prueba para el punto final de servicios de la plataforma

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

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Administrar puntos finales o permisos de acceso raíz" .

Acerca de esta tarea

StorageGRID no valida que las credenciales tengan los permisos correctos.

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Puntos finales de servicios de plataforma**.

   Aparece la página Puntos finales de servicios de la plataforma y muestra la lista de puntos finales de servicios de la plataforma que ya se han configurado.

2. Seleccione el punto final cuya conexión desea probar.

   Aparece la página de detalles del punto final.

3. Seleccione **Probar conexión**.
   - Aparece un mensaje de éxito si se puede acceder al punto final utilizando las credenciales especificadas. La conexión al punto final se valida desde un nodo en cada sitio.
   - Aparece un mensaje de error si falla la validación del punto final. Si necesita modificar el punto final para corregir el error, seleccione **Configuración** y actualice la información. Luego, seleccione **Probar y guardar cambios**.

Editar el punto final de los servicios de la plataforma

Puede editar la configuración de un punto final de servicios de la plataforma para cambiar su nombre, URI u otros detalles. Por ejemplo, es posible que necesite actualizar credenciales vencidas o cambiar la URI para que apunte a un índice de Elasticsearch de respaldo para conmutación por error. No se puede cambiar el URN de un punto final de servicios de plataforma.

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Administrar puntos finales o permisos de acceso raíz" .

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Puntos finales de servicios de plataforma**.

   Aparece la página Puntos finales de servicios de la plataforma y muestra la lista de puntos finales de servicios de la plataforma que ya se han configurado.

2. Seleccione el punto final que desea editar.

   Aparece la página de detalles del punto final.

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

   > No se puede cambiar el URN de un punto final una vez creado el punto final.

   a. Para cambiar el nombre para mostrar del punto final, seleccione el ícono de edición .
   b. Según sea necesario, cambie la URI.
   c. Según sea necesario, cambie el tipo de autenticación.
      - Para la autenticación de la clave de acceso, cambie la clave según sea necesario seleccionando **Editar clave S3** y pegando una nueva ID de clave de acceso y una clave de acceso secreta. Si necesita cancelar sus cambios, seleccione **Revertir edición de clave S3**.
      - Para la autenticación CAP (Portal de acceso C2S), cambie la URL de las credenciales temporales o la frase de contraseña de la clave privada del cliente opcional y cargue nuevos archivos de certificado y clave según sea necesario.

        > La clave privada del cliente debe estar en formato cifrado OpenSSL o en formato de clave privada sin cifrar.

   d. Según sea necesario, cambie el método para verificar el servidor.
5. Seleccione **Probar y guardar cambios**.
   - Aparece un mensaje de éxito si se puede acceder al punto final utilizando las credenciales especificadas. La conexión al punto final se verifica desde un nodo en cada sitio.
   - Aparece un mensaje de error si falla la validación del punto final. Modifique el punto final para corregir el error y luego seleccione **Probar y guardar cambios**.

Eliminar el punto final de los servicios de la plataforma

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

Antes de empezar

- Ha iniciado sesión en el Administrador de inquilinos mediante un"navegador web compatible" .
- Perteneces a un grupo de usuarios que tiene la"Administrar puntos finales o permisos de acceso raíz" .

Pasos

1. Seleccione **ALMACENAMIENTO (S3)** > **Puntos finales de servicios de plataforma**.

   Aparece la página Puntos finales de servicios de la plataforma y muestra la lista de puntos finales de servicios de la plataforma que ya se han configurado.

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

Si elimina un punto final de servicios de plataforma que está en uso, el servicio de plataforma asociado se deshabilitará para cualquier depósito que use el punto final. Cualquier solicitud que aún no se haya completado será descartada. Se seguirán generando nuevas solicitudes hasta que usted cambie la configuración de su depósito para que ya no haga referencia al URN eliminado. StorageGRID informará estas solicitudes como errores irrecuperables.

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

   Aparece un mensaje de confirmación.

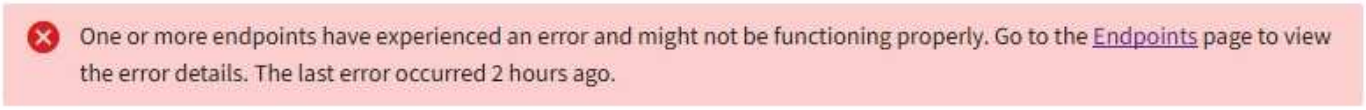
4. Seleccione **Eliminar punto final**.

Solucionar errores de puntos finales de servicios de la plataforma

Si se produce un error cuando StorageGRID intenta comunicarse con un punto final de servicios de la plataforma, se muestra un mensaje en el panel. En la página de puntos finales de servicios de la plataforma, la columna Último error indica cuánto tiempo hace que ocurrió el error. No se muestra ningún error si los permisos asociados con las credenciales de un punto final son incorrectos.

Determinar si se ha producido un error

Si se produjo algún error en los puntos finales de los servicios de la plataforma en los últimos 7 días, el panel del Administrador de inquilinos muestra un mensaje de alerta. Puede ir a la página de puntos finales de servicios de la plataforma para ver más detalles sobre el error.



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

Pasos

1. De la lista de puntos finales, seleccione el punto final que tiene el error.
2. En la página de detalles del punto final, seleccione **Conexión**. Esta pestaña muestra solo el error más reciente de un punto final e indica cuánto tiempo hace que ocurrió el error. Errores que incluyen el icono X rojo ocurrió dentro de los últimos 7 días.

Comprobar si el error sigue vigente

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

Pasos

1. Seleccione el punto final.

   Aparece la página de detalles del punto final.

2. Seleccione **Conexión** > **Probar conexión**.

Al seleccionar **Probar conexión**, StorageGRID valida que el punto final de servicios de la plataforma existe y que se puede acceder a él con las credenciales actuales. La conexión al punto final se valida desde un nodo en cada sitio.

Resolver errores de puntos finales

Puede utilizar el mensaje **Último error** en la página de detalles del punto final para ayudar a determinar qué está causando el error. Algunos errores podrían requerir que edites el punto final para resolver el problema. Por ejemplo, puede ocurrir un error de CloudMirroring si StorageGRID no puede acceder al bucket S3 de destino porque no tiene los permisos de acceso correctos o la clave de acceso ha expirado. El mensaje es "Es necesario actualizar las credenciales del punto final o el acceso al destino" y los detalles son "Acceso denegado" o "InvalidAccessKeyId".

Si necesita editar el punto final para resolver un error, seleccionar **Probar y guardar cambios** hace que StorageGRID valide el punto final actualizado y confirme que se puede acceder a él con las credenciales actuales. La conexión al punto final se valida desde un nodo en cada sitio.

Pasos

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

Credenciales de punto final con permisos insuficientes

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

Información relacionada

- **Administrar StorageGRID › Solucionar problemas de servicios de la plataforma**
- "Crear punto final de servicios de plataforma"
- "Conexión de prueba para el punto final de servicios de la plataforma"
- "Editar el punto final de los servicios de la plataforma"

Configurar la replicación de CloudMirror

Para habilitar la replicación de CloudMirror para un depósito, debe crear y aplicar un XML de configuración de replicación de depósito válido.

Antes de empezar

- Un administrador de StorageGRID habilitó los servicios de plataforma para su cuenta de inquilino.
- Ya ha creado un depósito para que actúe como fuente de replicación.
- El punto final que desea utilizar como destino para la replicación de CloudMirror ya existe y tiene su URN.
- Perteneces a un grupo de usuarios que tiene la"Administrar todos los depósitos o permisos de acceso raíz" . Estos permisos anulan las configuraciones de permisos en las políticas de grupo o de depósito

cuando se configura el depósito mediante el Administrador de inquilinos.

Acerca de esta tarea

La replicación de CloudMirror copia objetos de un depósito de origen a un depósito de destino que se especifica en un punto final.

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

> La replicación de CloudMirror tiene similitudes y diferencias importantes con la función de replicación entre redes. Para obtener más información, consulte"Comparar la replicación entre redes y la replicación de CloudMirror" .

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

- Cuando crea y aplica un XML de configuración de replicación de bucket válido, debe utilizar el URN de un punto final de bucket S3 para cada destino.
- La replicación no es compatible con los depósitos de origen o destino que tengan el bloqueo de objetos S3 habilitado.
- Si habilita la replicación de CloudMirror en un depósito que contiene objetos, los objetos nuevos agregados al depósito se replican, pero los objetos existentes en el depósito no se replican. Debe actualizar los objetos existentes para activar la replicación.
- Si especifica una clase de almacenamiento en el XML de configuración de replicación, StorageGRID utiliza esa clase al realizar operaciones contra el punto final S3 de destino. El punto final de destino también debe admitir la clase de almacenamiento especificada. Asegúrese de seguir todas las recomendaciones proporcionadas por el proveedor del sistema de destino.

Pasos

1. Habilite la replicación para su depósito de origen:
   - Utilice un editor de texto para crear el XML de configuración de replicación necesario para habilitar la replicación, como se especifica en la API de replicación S3.
   - Al configurar el XML:
     - Tenga en cuenta que StorageGRID solo admite la versión 1 de la configuración de replicación. Esto significa que StorageGRID no admite el uso de `Filter` elemento para reglas y sigue las convenciones V1 para la eliminación de versiones de objetos. Consulte la documentación de Amazon sobre la configuración de replicación para obtener más detalles.
     - Utilice la URN de un punto final del bucket S3 como destino.
     - Opcionalmente agregue el `<StorageClass>` elemento y especifique uno de los siguientes:
       - `STANDARD`:La clase de almacenamiento predeterminada. Si no especifica una clase de almacenamiento cuando carga un objeto, el `STANDARD` Se utiliza la clase de almacenamiento.
       - `STANDARD_IA`:(Estándar - acceso poco frecuente). Utilice esta clase de almacenamiento para datos a los que se accede con menos frecuencia, pero que aún requieren acceso rápido cuando sea necesario.
       - `REDUCED_REDUNDANCY`:Utilice esta clase de almacenamiento para datos no críticos y reproducibles que se pueden almacenar con menos redundancia que la `STANDARD` clase de almacenamiento.

- Si especifica un `Role` En el XML de configuración se ignorará. StorageGRID no utiliza este valor.

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

2. Seleccione **Ver depósitos** en el panel de control o seleccione **ALMACENAMIENTO (S3)** > **Depósitos**.
3. Seleccione el nombre del depósito de origen.

   Aparece la página de detalles del depósito.

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

> Los servicios de la plataforma deben ser habilitados para cada cuenta de inquilino por un administrador de StorageGRID mediante Grid Manager o Grid Management API. Comuníquese con su administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Verifique que la replicación esté configurada correctamente:
   a. Agregue un objeto al depósito de origen que cumpla con los requisitos de replicación según lo especificado en la configuración de replicación.

      En el ejemplo mostrado anteriormente, se replican los objetos que coinciden con el prefijo "2020".

   b. Confirme que el objeto se haya replicado en el depósito de destino.

      Para objetos pequeños, la replicación ocurre rápidamente.

Información relacionada

"Crear punto final de servicios de plataforma"

Configurar notificaciones de eventos

Puede habilitar las notificaciones para un depósito creando un XML de configuración de notificaciones y utilizando el Administrador de inquilinos para aplicar el XML a un depósito.

Antes de empezar

- Un administrador de StorageGRID habilitó los servicios de plataforma para su cuenta de inquilino.
- Ya has creado un depósito que actuará como fuente de notificaciones.
- El punto final que desea utilizar como destino para las notificaciones de eventos ya existe y tiene su URN.
- Perteneces a un grupo de usuarios que tiene la"Administrar todos los depósitos o permisos de acceso raíz" . Estos permisos anulan las configuraciones de permisos en las políticas de grupo o de depósito cuando se configura el depósito mediante el Administrador de inquilinos.

Acerca de esta tarea

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

Para obtener información general sobre las notificaciones de eventos y cómo configurarlas, consulte la "Documentación de Amazon" . Para obtener información sobre cómo StorageGRID implementa la API de configuración de notificaciones de bucket S3, consulte"Instrucciones para implementar aplicaciones cliente S3" .

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

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

Pasos

1. Habilitar notificaciones para su depósito de origen:
    - Utilice un editor de texto para crear el XML de configuración de notificación necesario para habilitar las notificaciones de eventos, como se especifica en la API de notificación S3.
    - Al configurar el XML, utilice la URN de un punto final de notificaciones de eventos como tema de destino.

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

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

   Aparece la página de detalles del depósito.

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

   > Los servicios de la plataforma deben ser habilitados para cada cuenta de inquilino por un administrador de StorageGRID mediante Grid Manager o Grid Management API. Comuníquese con su administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Verifique que las notificaciones de eventos estén configuradas correctamente:

   a. Realizar una acción en un objeto en el depósito de origen que cumpla con los requisitos para activar una notificación según lo configurado en el XML de configuración.

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

   b. Confirme que se ha enviado una notificación al tema de destino de Amazon SNS o Kafka.

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

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```


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

Información relacionada

"Comprender las notificaciones de los buckets"

"Utilice la API REST de S3"

"Crear punto final de servicios de plataforma"

Configurar el servicio de integración de búsqueda

Puede habilitar la integración de búsqueda para un depósito creando un XML de integración de búsqueda y utilizando el Administrador de inquilinos para aplicar el XML al depósito.

Antes de empezar

- Un administrador de StorageGRID habilitó los servicios de plataforma para su cuenta de inquilino.
- Ya ha creado un bucket S3 cuyo contenido desea indexar.
- El punto final que desea utilizar como destino para el servicio de integración de búsqueda ya existe y tiene su URN.
- Perteneces a un grupo de usuarios que tiene la"Administrar todos los depósitos o permisos de acceso raíz" . Estos permisos anulan las configuraciones de permisos en las políticas de grupo o de depósito cuando se configura el depósito mediante el Administrador de inquilinos.

Acerca de esta tarea

Después de configurar el servicio de integración de búsqueda para un depósito de origen, la creación de un objeto o la actualización de los metadatos o las etiquetas de un objeto activa el envío de metadatos del objeto al punto final de destino.

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

Pasos

1. Habilitar la integración de búsqueda para un depósito:
    - Utilice un editor de texto para crear el XML de notificación de metadatos necesario para habilitar la integración de búsqueda.
    - Al configurar el XML, utilice la URN de un punto final de integración de búsqueda como destino.

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

      Según sea necesario, consulte laEjemplos para la configuración de metadatos XML .

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

Elementos en el XML de configuración de notificación de metadatos:

Nombre	Descripción	Requerido
Configuración de notificación de metadatos	Etiqueta contenedora para reglas utilizadas para especificar los objetos y el destino de las notificaciones de metadatos. Contiene uno o más elementos de regla.	Sí
Regla	Etiqueta contenedora para una regla que identifica los objetos cuyos metadatos deben agregarse a un índice específico. Se rechazan las reglas con prefijos superpuestos. Incluido en el elemento MetadataNotificationConfiguration.	Sí
IDENTIFICACIÓN	Identificador único de la regla. Incluido en el elemento Regla.	No
Estado	El estado puede ser 'Habilitado' o 'Deshabilitado'. No se realiza ninguna acción para las reglas que están deshabilitadas. Incluido en el elemento Regla.	Sí
Prefijo	Los objetos que coinciden con el prefijo se ven afectados por la regla y sus metadatos se envían al destino especificado. Para que coincida con todos los objetos, especifique un prefijo vacío. Incluido en el elemento Regla.	Sí
Destino	Etiqueta de contenedor para el destino de una regla. Incluido en el elemento Regla.	Sí

Nombre	Descripción	Requerido
Urna	URN del destino donde se envían los metadatos del objeto. Debe ser la URN de un punto final de StorageGRID con las siguientes propiedades: • `es`Debe ser el tercer elemento. • La URN debe terminar con el índice y tipo donde se almacenan los metadatos, en el formato `domain-name/myindex/mytype` . Los puntos finales se configuran mediante el Administrador de inquilinos o la API de administración de inquilinos. Toman la siguiente forma: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` El punto final debe configurarse antes de enviar el XML de configuración; de lo contrario, la configuración fallará con un error 404. URN está incluido en el elemento Destino.	Sí

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

   Aparece la página de detalles del depósito.

4. Seleccione **Servicios de plataforma** > **Integración de búsqueda**
5. Seleccione la casilla de verificación **Habilitar integración de búsqueda**.
6. Pegue la configuración de notificación de metadatos en el cuadro de texto y seleccione **Guardar cambios**.

   Los servicios de plataforma deben ser habilitados para cada cuenta de inquilino por un administrador de StorageGRID mediante Grid Manager o la API de administración. Comuníquese con su administrador de StorageGRID si se produce un error al guardar el XML de configuración.

7. Verifique que el servicio de integración de búsqueda esté configurado correctamente:
   a. Agregue un objeto al depósito de origen que cumpla con los requisitos para activar una notificación de metadatos según lo especificado en el XML de configuración.

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

   b. Confirme que se agregó un documento JSON que contiene los metadatos y las etiquetas del objeto al índice de búsqueda especificado en el punto final.

Después de terminar

Según sea necesario, puede deshabilitar la integración de búsqueda para un depósito utilizando cualquiera de los siguientes métodos:

- Seleccione **ALMACENAMIENTO (S3)** > **Cubos** y desmarque la casilla **Habilitar integración de búsqueda**.
- Si está utilizando la API S3 directamente, utilice una solicitud de notificación de metadatos de DELETE Bucket. Consulte las instrucciones para implementar aplicaciones cliente S3.

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

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

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

Ejemplo: Configuración de notificación de metadatos con dos reglas

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

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Formato de notificación de metadatos

Cuando habilita el servicio de integración de búsqueda para un depósito, se genera un documento JSON y se envía al punto final de destino cada vez que se agregan, actualizan o eliminan metadatos o etiquetas de objeto.

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

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

Campos incluidos en el documento JSON

El nombre del documento incluye el nombre del depósito, el nombre del objeto y el ID de la versión, si está presente.

Información de depósito y objeto

`bucket`: Nombre del bucket

`key`: Nombre de la clave del objeto

`versionID`:Versión del objeto, para objetos en depósitos versionados

`region`: Región del cubo, por ejemplo `us-east-1`

Metadatos del sistema

`size`:Tamaño del objeto (en bytes) tal como lo ve un cliente HTTP

`md5`: Hash de objeto

Metadatos del usuario

`metadata`:Todos los metadatos del usuario para el objeto, como pares clave-valor

`key:value`

Etiquetas

`tags`:Todas las etiquetas de objeto definidas para el objeto, como pares clave-valor

`key:value`

Cómo ver resultados en Elasticsearch

Para las etiquetas y los metadatos del usuario, StorageGRID pasa fechas y números a Elasticsearch como

cadenas o como notificaciones de eventos S3. Para configurar Elasticsearch para que interprete estas cadenas como fechas o números, siga las instrucciones de Elasticsearch para el mapeo de campos dinámicos y para el mapeo de formatos de fecha. Habilite las asignaciones de campos dinámicos en el índice antes de configurar el servicio de integración de búsqueda. Una vez indexado un documento, no es posible editar los tipos de campos del documento en el índice.

Información de copyright

Información de la marca comercial