Object Storage Service

Guía de operación de la consola

Edición 01

Fecha 2024-09-18

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Marcas registradas y permisos

El logotipo HUAWEI y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.
Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Es posible que la totalidad o parte de los productos, las funcionalidades y/o los servicios que figuran en el presente documento no se encuentren dentro del alcance de un contrato vigente entre Huawei Cloud y el cliente. Las funcionalidades, los productos y los servicios adquiridos se limitan a los estipulados en el respectivo contrato. A menos que un contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en el presente documento constituye garantía alguna, ni expresa ni implícita.

Huawei está permanentemente preocupada por la calidad de los contenidos de este documento; sin embargo, ninguna declaración, información ni recomendación aquí contenida constituye garantía alguna, ni expresa ni implícita. La información contenida en este documento se encuentra sujeta a cambios sin previo aviso.

Índice

1 Descripción de la función de consola

Tabla 1-1 enumera las funciones proporcionadas por OBS Console.

Tabla 1-1 Funciones de OBS Console.

Funciones	Descripción
Operaciones básicas de bucket	Permite crear y eliminar bucket de diferentes clases de almacenamiento en regiones específicas (áreas de servicio), copiar configuraciones de bucket existentes, así como cambiar clases de almacenamiento de bucket.
Operaciones básicas de objetos	Le permite gestionar objetos, incluidas cargas, cargas de varias partes, descargas, uso compartido, cambio de clase de almacenamiento, restauración de objetos archivados, y eliminación.
Encriptación del lado del servidor	Cifra los datos en los servidores para mejorar la seguridad de los datos almacenados en OBS.
WORM	Protege que los objetos se eliminen o alteren dentro de un período especificado.
Metadatos de objeto	Permite definir las propiedades de los objetos.
Monitoreo	● Cloud Eye puede monitorear las siguientes métricas de OBS: – Tráfico de descarga – Tráfico de carga – Solicitudes de GET – Solicitudes de PUT – Retraso en la descarga de primer byte – Errores 4*xx* – Errores 5*xx*
Auditoría	Con Cloud Trace Service (CTS), puede registrar las operaciones de datos asociadas con OBS para realizar consultas, auditorías y operaciones posteriores.

Funciones	Descripción
Gestión de fragmentos	Gestiona y borra fragmentos generados debido a errores de carga de objetos.
Control de versiones	Almacena varias versiones de un objeto en el mismo bucket.
Registro	Registra las solicitudes de acceso al bucket para su análisis y auditoría.
Control de permisos	Controla los permisos de acceso de OBS con permisos de IAM, políticas de bucket/objeto y listas de control de acceso (ACL) de bucket/objeto.
Gestión del ciclo de vida	Permite configurar reglas de ciclo de vida para que expiren y eliminen periódicamente objetos u objetos de transición entre clases de almacenamiento.
Replicación entre regiones	Implementa la replicación de objetos en regiones bajo la misma cuenta. Al configurar reglas de replicación entre regiones, puede habilitar OBS para copiar datos de forma automática y asincrónica desde un bucket de origen a un bucket de destino en otra región. Por lo tanto, la replicación entre regiones proporciona la capacidad de recuperación ante desastres de datos en todas las regiones, atendiendo a sus necesidades de backup de datos fuera del sitio.
Etiquetas	Identifica y clasifica los bucket en OBS.
Alojamiento de sitio web estático	Soporta el alojamiento de contenido de sitios web estáticos en las bucket y admite la redirección de solicitudes de acceso a bucket a hosts específicos.
Configuración del nombre de dominio definido por el usuario	Vincula los nombres de dominio de su sitio web a los nombres de dominio de bucket. Esta función se aplica al siguiente escenario: migrar archivos de un sitio web a OBS sin modificar el código de la página web, y mantener el enlace del sitio web sin cambios.
Volver a fuente	Le ayuda a obtener los datos solicitados de su sitio de origen si no se encuentran en OBS. Por lo general, si los datos solicitados no se encuentran en OBS, se devolverá un error 404.
Validación de URL	Proporciona validación de URL para evitar que los enlaces de objetos de OBS sean robados por otros sitios web.

Funciones	Descripción
Intercambio de recursos de origen cruzado (CORS)	Permite que un cliente web de un origen interactúe con recursos de otro. CORS es un mecanismo estándar de navegador definido por el World Wide Web Consortium (W3C). Para las solicitudes generales de páginas web, los scripts de sitios web y los contenidos de un origen no pueden interactuar con los de otro debido a las políticas del mismo origen (Same Origin Policies, SOP).
Lectura directa	Le permite descargar directamente objetos de la clase de almacenamiento Archive sin restaurarlos primero. La lectura directa es una función facturable.
Inventario de bucket	Proporciona periódicamente archivos CSV que listan información de objeto en el bucket y entrega los archivos de CSV al bucket especificado.

2 Compatibilidad del navegador web

Tabla 2-1 enumera las versiones del navegador web compatibles con OBS Console.

Tabla 2-1 Versiones de navegador web compatibles

Navegador web	Versión
Internet Explorer	● Internet Explorer 9 (IE9) ● Internet Explorer 10 (IE10) ● Internet Explorer 11 (IE11)
Firefox	Firefox 55 y posterior
Chrome	Chrome 60 y posteriores

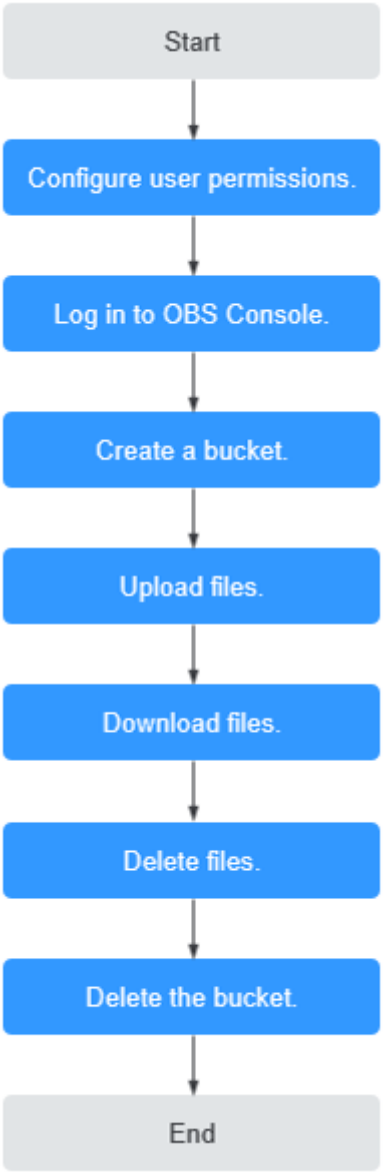
3 Pasos iniciales

3.1 Descripción del proceso

Las operaciones básicas de OBS incluyen la creación de bucket, la carga de objetos y la descarga de objetos.

Las secciones de seguimiento describen cómo completar las tareas ilustradas en **Figura 3-1**.

Figura 3-1 Inicio rápido de OBS Console



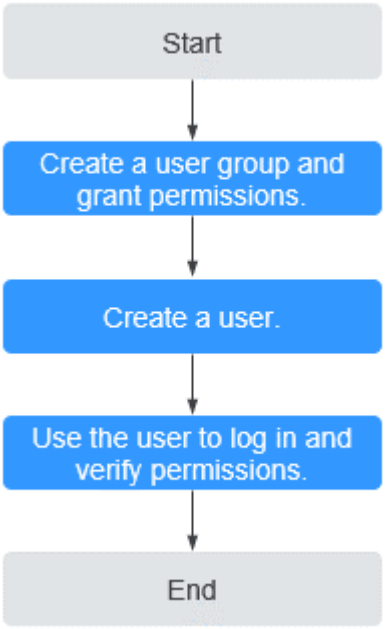
3.2 Configuración de permisos de usuario

Si su cuenta de servicio en la nube no necesita usuarios individuales de IAM, puede omitir esta sección. Sus permisos para usar las funciones de OBS no se ven afectados.

Si se requieren usuarios de IAM, debe concederles permisos de acceso en OBS, ya que OBS se despliega por separado de otros recursos en la nube.

Proceso

Figura 3-2 Proceso de concesión de permisos de OBS a un usuario de IAM



El siguiente ejemplo describe cómo conceder a un usuario de IAM el permiso **Tenant Guest** en OBS.

1. **Crear un grupo de usuarios y asignar permisos**.

   Cree un grupo de usuarios en la consola de IAM y asigne al grupo el permiso **Tenant Guest**.

2. **Crear un usuario de IAM y agregarlo al grupo de usuario**.

   Cree un usuario en la consola de IAM y agregue el usuario al grupo creado en **1**.

3. **Iniciar sesión** y verificar el permiso otorgado.

   Inicie sesión en OBS Console con el usuario recién creado y compruebe que el permiso asignado haya tenido efecto:

   – Elija **Object Storage Service** en la lista de servicios para ir a la página de inicio de OBS. Si se muestra la lista de bucket y se puede ver la información básica sobre cualquier bucket, pero no se puede crear o eliminar bucket ni realizar ninguna otra operación, el permiso **Tenant Guest** concedido ya tiene efecto.

   – Vaya a un bucket de OBS. Si se muestra la lista de objetos y se pueden descargar objetos, pero no se pueden cargar o eliminar objetos ni realizar ninguna otra operación, el permiso **Tenant Guest** concedido ya ha surtido efecto.

3.3 Logging In to OBS Console

En esta sección se describe cómo iniciar sesión en OBS Console con un navegador web.

Procedimiento

Paso 1 Visite el **sitio web oficial de Huawei Cloud**.

Paso 2 Cree un HUAWEI ID.

Si ya lo tiene, empieza desde **Paso 3**.

1. A la derecha de la barra de navegación superior, haga clic en **Regístrese**.
2. Complete la creación según las instrucciones.

   Una vez completada la creación, se le dirigirá a la página de información de ID.

Paso 3 A la derecha del menú de navegación superior, haga clic en **Log In** e introduzca el nombre de usuario y la contraseña.

Paso 4 A la derecha de la barra de navegación superior, haga clic en **Console** para ir a la consola de gestión.

Paso 5 En la esquina superior izquierda del panel de navegación, haga clic en  y elija **Storage** > **Object Storage Service**. Se muestra la página de OBS Console.

Paso 6 Se recomienda recargar su cuenta o suscribirse a OBS mediante la compra de paquetes de recursos, para que el servicio se pueda utilizar correctamente.

----Fin

3.4 Creación de un bucket

Esta sección describe cómo crear un bucket en OBS Console. Un bucket es un contenedor que almacena objetos en OBS. Para almacenar datos en OBS, es necesario crear un bucket.

NOTA

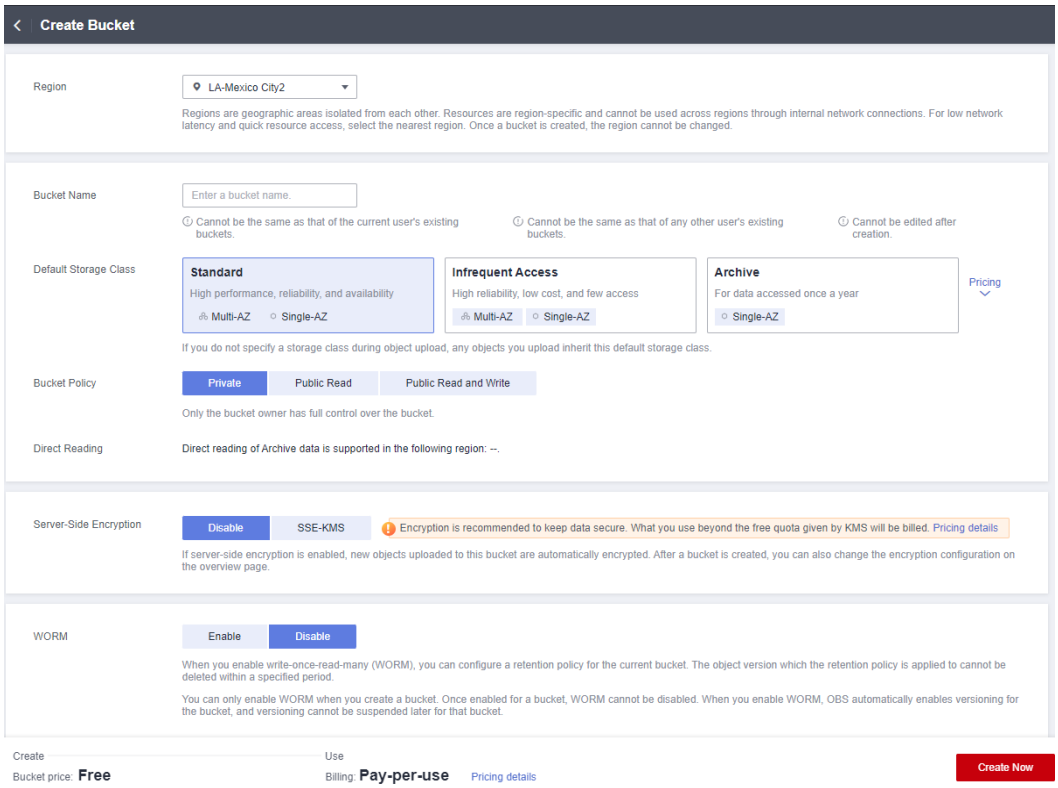
Una cuenta (incluidos todos los usuarios de IAM de esta cuenta) puede crear un máximo de 100 buckets y sistemas de archivos paralelos. Puede utilizar el control de acceso de grano fino de OBS para planificar y usar adecuadamente los bucket. Por ejemplo, puede crear carpetas en un bucket basado en prefijos de objeto y usar **control de permisos fino** para implementar el aislamiento de permisos entre departamentos.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la esquina superior derecha, haga clic en **Create Bucket**. Se muestra la página **Create Bucket**. Para obtener más información, véase **Figura 3-3**.

Figura 3-3 Creación de un bucket



Paso 3 Configure parámetros de bucket.

Tabla 3-1 Parámetros de bucket

Parámetro	Descripción
Replicate Existing Settings	Opcional. Para utilizar esta función, haga clic en **Select Bucket** y seleccione un bucket de la lista como origen de replicación. Después de seleccionar el origen de replicación, se replican las siguientes opciones en el bucket que está creando: región, política de redundancia de datos, clase de almacenamiento, política de bucket, encriptación del lado del servidor, lectura directa, proyecto de empresa y etiquetas. Todavía puede cambiar algunas o todas las configuraciones replicadas según sea necesario.
Region	Área geográfica donde reside un bucket. Para una baja latencia y un acceso más rápido, seleccione la región más cercana a usted. Una vez creado el bucket, no se puede cambiar su región. La mayoría de las funciones de OBS están disponibles en todas las regiones, pero algunas solo están disponibles para ciertas regiones. Tenga en cuenta la disponibilidad de funciones en cada región cuando seleccione una región para un bucket. Para obtener más información, consulte **Descripción de funciones**. Si su ECS necesita acceder a un bucket de OBS por la intranet, asegúrese de que el bucket y el ECS están en la misma región. Para obtener más información, consulte **Acceso a OBS por una intranet**.

Parámetro	Descripción
Bucket Name	Nombre del bucket. Un nombre de bucket debe ser único en todas las cuentas y regiones. Una vez que se crea un bucket, no se puede cambiar su nombre. De acuerdo con las reglas de nomenclatura de DNS aplicadas globalmente, un nombre de bucket de OBS: ● Debe ser único en todas las cuentas y regiones. El nombre de un bucket eliminado se puede reutilizar para otro bucket o un sistema de archivos paralelo al menos 30 minutos después de la eliminación. ● Debe contener entre 3 y 63 caracteres. Solo se permiten letras minúsculas, dígitos, guiones (-) y puntos (.). ● No puede comenzar o finalizar con un período (.) o guion (-), y no puede contener dos períodos consecutivos (..) ni contener un período (.) y un guion (-) adyacentes entre sí. ● No se puede formatear como una dirección IP. **NOTA** Cuando accedes a OBS con HTTPS usando URLs de estilo alojado virtual, si el nombre del bucket contiene un punto (.), la verificación del certificado fallará. Para evitar este problema, se recomienda no utilizar períodos (.) en los nombres de bucket.
Data Redundancy Policy	● **Multi-AZ storage**: Los datos se almacenan en múltiples AZ para lograr una mayor fiabilidad. ● **Single-AZ storage**: Los datos se almacenan en una sola AZ, con costos más bajos. Para obtener más información acerca de la comparación de rendimiento entre el almacenamiento de multi-AZ y el almacenamiento de una sola AZ, consulte **Comparación de clases de almacenamiento**. Una vez que se crea un bucket, la política de redundancia de datos no se puede cambiar, así que elija la política que pueda satisfacer sus necesidades. ● El almacenamiento de multi-AZ no está disponible para los bucket de la clase de almacenamiento Archive.
Default Storage Class	Clases de almacenamiento de un bucket. Las diferentes clases de almacenamiento cumplen con diferentes requisitos de rendimiento y costes de almacenamiento. ● La clase de almacenamiento Standard es para almacenar un gran número de archivos calientes o pequeños archivos a los que se accede con frecuencia (múltiples veces al mes en promedio) y requieren una recuperación rápida. ● La clase de almacenamiento Infrequent Access es para almacenar datos a los que se accede con menos frecuencia (menos de 12 veces al año en promedio) y requiere una recuperación rápida. ● La clase de almacenamiento Archive es para archivar datos a los que rara vez se accede (una vez al año en promedio) y no tiene requisitos para una recuperación rápida. Para obtener más información, consulte **Clases de almacenamiento**.

Parámetro	Descripción
Bucket Policy	Controla los permisos de lectura y escritura de los bucket. ● **Private**: No se concede ningún acceso más allá de la configuración de ACL del bucket. ● **Public Read**: Cualquiera puede leer objetos en el bucket. ● **Public Read and Write**: Cualquier persona puede leer, escribir o eliminar objetos en el bucket.
Server-Side Encryption	Seleccione **SSE-KMS**. Para el tipo de clave de encriptación, puede elegir **Default** o **Custom**. Si se utiliza **Default**, se utilizará la clave predeterminada de la región actual para cifrar los objetos. Si no existe una clave predeterminada, OBS crea una la primera vez que carga un objeto. Si se utiliza **Custom**, puede elegir una clave personalizada que haya creado en la consola de KMS para cifrar los objetos. Si se elige **SSE-OBS**, las claves creadas y gestionadas por OBS se utilizan para la encriptación. Cuando la encriptación del lado del servidor está habilitado para un bucket, puede configurar el objeto que cargue para que herede la encriptación del bucket o elegir SSE-KMS o SSE-OBS.
WORM	When you enable write-once-read-many (WORM), you can configure a retention policy for the current bucket. The object version which the retention policy is applied to cannot be deleted within a specified period. You can only enable WORM when you create a bucket. Once enabled for a bucket, WORM cannot be disabled. When you enable WORM, OBS automatically enables versioning for the bucket, and versioning cannot be suspended later for that bucket.
Direct Reading	La lectura directa le permite descargar directamente objetos de la clase de almacenamiento Archive sin restaurarlos primero. La lectura directa es una función facturable. Para obtener información detallada, consulte **Detalles de los precios de productos**. No importa qué clase de almacenamiento predeterminada seleccione, puede habilitar la lectura directa para su bucket. Por ejemplo, si selecciona la clase de almacenamiento Standard y habilita la lectura directa para el bucket, puede descargar directamente los objetos almacenados en la clase de almacenamiento Archive desde el bucket.
Enterprise Project	Puede agregar un bucket a un proyecto de empresa para la gestión unificada. Cree un proyecto de empresa haciendo referencia a **Crear un proyecto de empresa**. El proyecto de empresa predeterminado se denomina **default**. **NOTA** Solo una cuenta de empresa puede configurar proyectos de empresa. OBS ReadOnlyAccess y OBS OperateAccess son las autorizaciones detalladas del grupo de usuarios de proyecto empresarial en OBS.

Parámetro	Descripción
Tags	Opcional. Las etiquetas se utilizan para identificar y clasificar bucket en OBS. Cada etiqueta está representada por un par clave-valor. Para obtener más información, consulte **Etiquetas**.

Paso 4 Haga clic en **Create Now**.

----Fin

3.5 Carga de un objeto

Esta sección describe cómo cargar archivos locales a OBS por Internet. Estos archivos pueden ser textos, imágenes, videos o cualquier otro tipo de archivos.

Limitaciones y restricciones

OBS Console tiene restricciones sobre el tamaño y el número de archivos cargados.

- En las regiones donde se admite la carga por lotes, se puede cargar un máximo de 100 archivos a la vez, con un tamaño total máximo de 5 GB.
- En las regiones donde no se admite la carga por lotes, solo se puede cargar un archivo a la vez, con un tamaño máximo de 50 MB.

Por lo tanto, para cargar un solo archivo, su tamaño máximo puede ser de 5 GB en una carga por lotes o 50 MB en una sola carga.

Para cargar un archivo de más de 5 GB, pero no más de 48.8 TB, puede usar **OBS Browser+** u **obsutil**, o la carga de varias partes de SDK o de API de OBS.

OBS Browser+ le permite subir un máximo de 500 archivos a la vez. No hay límite en el número de archivos que puede subir usando obsutil a la vez.

Si tiene más datos que cargar, consulte **Migración de datos locales a OBS**.

NOTA

La carga por lotes solo está disponible cuando se cumplen las dos condiciones siguientes:

1. El bucket se encuentra en cualquiera de las siguientes regiones:
2. La versión del bucket es 3.0. Para ver la versión del bucket, consulte **Consulta de información básica de un bucket**.

Si el control de versiones está deshabilitado para el bucket y carga un nuevo archivo con el mismo nombre que el que cargó anteriormente en el bucket, el nuevo archivo sobrescribe automáticamente el archivo anterior y no conserva su información de ACL. Si carga una nueva carpeta con el mismo nombre que se usó con una carpeta anterior en el bucket, las dos carpetas se fusionarán y los archivos de la nueva carpeta sobrescribirán archivos con nombre en la carpeta anterior.

Después de habilitar el control de versiones para su bucket, si el nuevo archivo que subió tiene el mismo nombre que el que subió anteriormente al bucket, se agregará una nueva versión de archivo en el bucket. Para obtener más información, consulte **Control de versiones**.

Requisitos previos

- Se ha creado al menos un bucket.
- Si desea clasificar archivos, puede crear carpetas y subir archivos a diferentes carpetas. Para obtener más información sobre cómo crear una carpeta, consulte **Creación de la carpeta**

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Vaya a la carpeta en la que se cargan los objetos. Haga clic en **Upload Object**. Aparece el cuadro de diálogo **Upload Object**.

A continuación se utiliza la carga por lotes como ejemplo. Para las regiones que admiten solo una carga única, realice las operaciones según se le indique.

NOTA

Si los archivos que desea cargar en OBS se almacenan en OneDrive de Microsoft, se recomienda que los nombres de estos archivos contengan un máximo de 32 caracteres para garantizar la compatibilidad.

Figura 3-4 Carga de objetos

Paso 4 Seleccione una clase de almacenamiento. Si no especifica una clase de almacenamiento, el objeto que cargue heredará la clase de almacenamiento predeterminada del bucket.

> **NOTA**
>
> Un objeto puede tener una clase de almacenamiento diferente de su bucket. Puede especificar una clase de almacenamiento para un objeto al cargarlo, o puede cambiar la clase de almacenamiento de objeto después de cargar el objeto.

Paso 5 Agregue un archivo o carpeta para cargar arrastrándolo al área **Upload Object**.

También puede hacer clic en **add file** en el área **Upload Object** para seleccionar archivos.

Paso 6 **Server-Side Encryption**: Seleccione **Disable**, **SSE-KMS** o **SSE-OBS**. Para obtener más información, véase **Carga de un objeto en modo de encriptación del lado del servidor**.

> **NOTA**
>
> Si un bucket tiene la encriptación del lado del servidor configurada, puede seleccionar **Inherit from bucket** al cargar un objeto en el bucket, para que el objeto herede la configuración de encriptación del bucket.

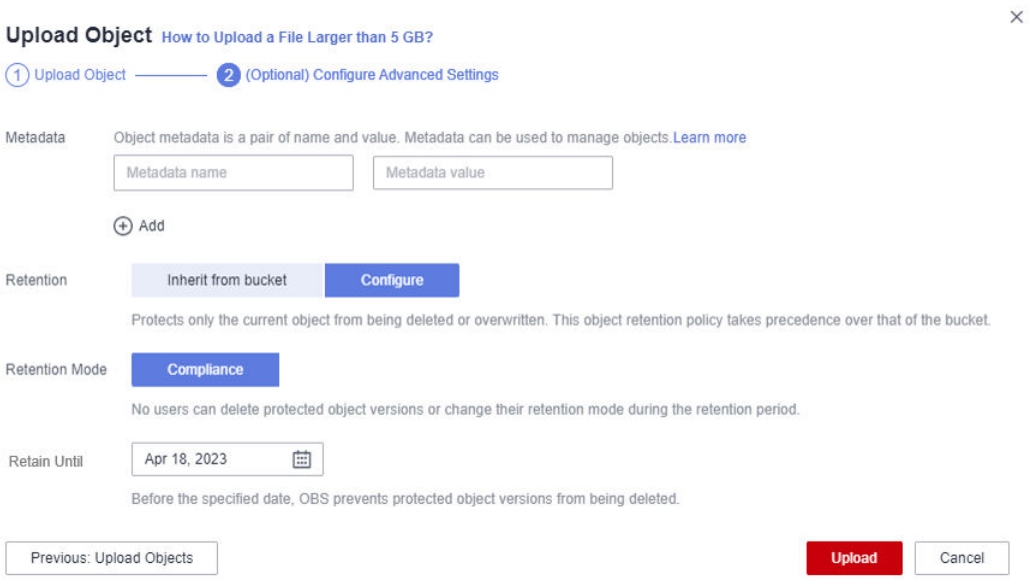
Paso 7 (Opcional) Para configurar el metadato o las políticas de retención de WORM, haga clic en **Next: (Optional) Configure Advanced Settings**.

> **NOTA**
>
> Las políticas de retención de WORM se pueden configurar en la configuración avanzada solo cuando WORM está habilitado para el bucket.

Configuración de metadatos: Agregar metadatos ContentDisposition, ContentLanguage, WebsiteRedirectLocation, ContentEncoding o ContentType según sea necesario. Para obtener más información, consulte la sección **Metadatos de objetos de OBS**. Los metadatos son un conjunto de pares nombre-valor. El valor de metadatos no se puede dejar en blanco. Puede agregar dos o más entradas de metadatos haciendo clic en **Add**.

Configuración de la retención de WORM: Elija **Inherit from bucket** o **Configure** y especifique un período de retención para proteger automáticamente los nuevos objetos cargados en el bucket de que se eliminen.

Figura 3-5 Configuración de metadatos o retención de WORM



Paso 8 Haga clic en **Upload**.

----Fin

3.6 Descarga de un objeto

Puede descargar archivos de OBS Console a su equipo local.

Limitaciones y restricciones

- Los objetos de la clase de almacenamiento Archive sólo se pueden descargar cuando están en el estado **Restored**.
- La descarga por lotes no es compatible con OBS Console. Para descargar archivos o carpetas por lotes, puede usar OBS Browser+ u obsutil.
  - **Descargar archivos o carpetas con OBS Browser+**
  - **Descargar objetos con obsutil**

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Seleccione los archivos que desea descargar y, a continuación, haga clic en **Download** o **More** > **Download As** para descargar los archivos.

NOTA

En el cuadro de diálogo **Download As**, haga clic con el botón secundario en el objeto y elija **Copy Link Address** en el menú contextual para obtener la dirección de descarga del objeto.

----Fin

3.7 Eliminación de un objeto

Puede eliminar archivos innecesarios uno por uno o por un lote en OBS Console para ahorrar espacio y dinero.

NOTA

Cuando se ha habilitado WORM para el bucket, el control de versiones también está habilitado para el bucket de forma predeterminada. Si una versión de objeto tiene alguna política de retención de WORM configurada, esta versión de objeto no se puede eliminar permanentemente durante el período de retención. En la ficha **Versions** de la página de detalles del objeto, puede elegir **More** > **Extend Retention Period** en la columna **Operation** de la fila de la versión del objeto para comprobar si esta versión se encuentra dentro del período de retención. Si no se ha configurado ninguna política de retención de WORM para una versión de objeto, puede eliminarla en la ficha **Versions** de la página de detalles del objeto.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Seleccione el archivo que desea eliminar y elija **More** > **Delete** a la derecha.

Puede seleccionar varios archivos y hacer clic en **Delete** encima de la lista de archivos para eliminar los archivos por lotes.

Paso 4 Haga clic en **Yes** para confirmar la eliminación.

----Fin

Notas importantes

En escenarios de big data, los sistemas de archivos paralelos generalmente tienen niveles de directorio profundos y cada directorio tiene un gran número de archivos. En tal caso, la eliminación de directorios de sistemas de archivos paralelos puede fallar debido al tiempo de espera. Para solucionar este problema, se recomienda configurar **una regla de ciclo de vida** para directorios para que se puedan eliminar en segundo plano basándose en la regla de ciclo de vida preestablecida.

3.8 Eliminación de un bucket

Puede eliminar bucket no deseados en OBS Console para liberar la cuota de bucket.

Requisitos previos

- Todos los objetos del bucket se han eliminado permanentemente. Se debe vaciar un bucket para poder eliminarlo.

  AVISO

  Los objetos de las fichas **Objects**, **Deleted Objects** y **Fragments** deben eliminarse.

- Un bucket solo puede ser eliminado por el propietario del bucket.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, seleccione el bucket que desea eliminar y, a continuación, haga clic en **Delete** a la derecha.

NOTA

El nombre de un bucket eliminado se puede reutilizar para un bucket o un sistema de archivos paralelo al menos 30 minutos después de la eliminación.

Paso 3 Haga clic en **Yes** para confirmar la eliminación.

----Fin

4 Storage Classes Overview

OBS supports tiered storage classes at the bucket level and object level.

OBS provides the following storage classes: Standard, Infrequent Access, and Archive.

Different storage classes meet different requirements for storage performance and costs.

- The Standard storage class features low access latency and high throughput. It is therefore suitable for storing a massive number of hot files (frequently accessed every month) or small files (less than 1 MB). The application scenarios include big data analytics, mobile apps, hot videos, and social apps.
- The Infrequent Access storage class is ideal for storing data that is semi-frequently accessed (less than 12 times a year), with requirements for quick response. The application scenarios include file synchronization, file sharing, and enterprise backup.
- The Archive storage class is suitable for archiving data that is rarely-accessed (averagely once a year). The application scenarios include data archiving and long-term data backups. The Archive storage class is secure, durable, and inexpensive, and can be used to replace tape libraries. To keep cost low, it may take hours to restore data from the Archive storage class.

Bucket Storage Classes vs. Object Storage Classes

When an object is uploaded, it inherits the storage class of the bucket by default, but you can change the default storage class when you upload the object.

Changing the storage class of a bucket does not change the storage classes of existing objects in the bucket, but newly uploaded objects will inherit the new storage class.

Comparison of Storage Classes

Compared Item	Standard	Infrequent Access	Archive
Feature	Top-notch performance, highly reliable and available	Reliable, inexpensive, and real-time storage access	Long-term storage for archived data at a very low cost

Compared Item	Standard	Infrequent Access	Archive
Application scenarios	Cloud application, data sharing, content sharing, and hot data storage	Web disk applications, enterprise backup, active archiving, and data monitoring	Archive, medical image storage, video material storage, and replacement of tape libraries
Designed durability	99.999999999%	99.999999999%	99.999999999%
Designed durability (multi-AZ)	99.9999999999%	99.9999999999%	-
Designed availability	99.99%	99%	99%
Designed availability (multi-AZ)	99.995%	99.5%	-
Minimum storage duration	Not required	30 days	90 days
Data retrieval	N/A	Billed for each GB retrieved.	Data can be restored at a standard or an expedited speed. Billed for each GB restored.
Image processing	Supported	Supported	Not supported

5 Gestión de bucket

5.1 Creación de un bucket

Un bucket es un contenedor que almacena objetos en OBS. Antes de almacenar datos en OBS, es necesario crear un bucket.

NOTA

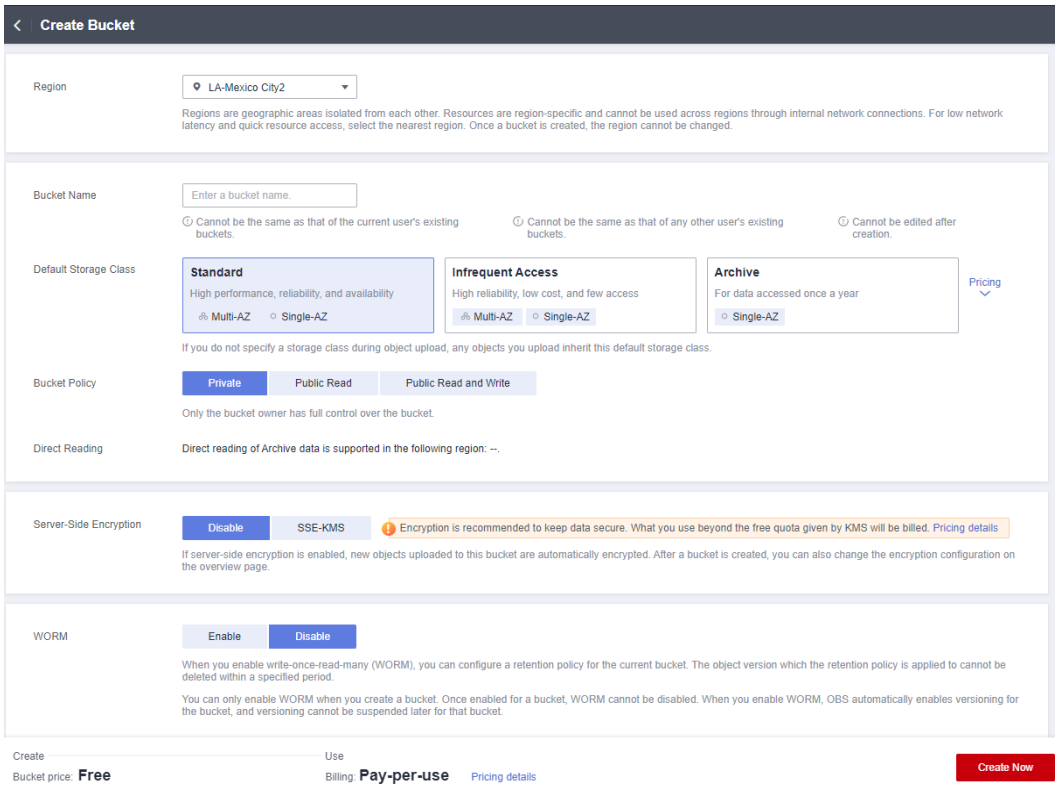
Una cuenta (incluidos todos los usuarios de IAM de esta cuenta) puede crear un máximo de 100 buckets y sistemas de archivos paralelos. Puede utilizar el control de acceso de grano fino de OBS para planificar y usar adecuadamente los bucket. Por ejemplo, puede crear carpetas en un bucket basado en prefijos de objeto y usar **control de permisos fino** para implementar el aislamiento de permisos entre departamentos.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la esquina superior derecha, haga clic en **Create Bucket**. Se muestra la página **Create Bucket**. Para obtener más información, véase **Figura 5-1**.

Figura 5-1 Creación de un bucket



Paso 3 Configure parámetros de bucket.

Tabla 5-1 Parámetros de bucket

Parámetro	Descripción
Replicate Existing Settings	Opcional. Para utilizar esta función, haga clic en **Select Bucket** y seleccione un bucket de la lista como origen de replicación. Después de seleccionar el origen de replicación, se replican las siguientes opciones en el bucket que está creando: región, política de redundancia de datos, clase de almacenamiento, política de bucket, encriptación del lado del servidor, lectura directa, proyecto de empresa y etiquetas. Todavía puede cambiar algunas o todas las configuraciones replicadas según sea necesario.
Region	Área geográfica donde reside un bucket. Para una baja latencia y un acceso más rápido, seleccione la región más cercana a usted. Una vez creado el bucket, no se puede cambiar su región. La mayoría de las funciones de OBS están disponibles en todas las regiones, pero algunas solo están disponibles para ciertas regiones. Tenga en cuenta la disponibilidad de funciones en cada región cuando seleccione una región para un bucket. Para obtener más información, consulte **Descripción de funciones**. Si su ECS necesita acceder a un bucket de OBS por la intranet, asegúrese de que el bucket y el ECS están en la misma región. Para obtener más información, consulte **Acceso a OBS por una intranet**.

Parámetro	Descripción
Bucket Name	Nombre del bucket. Un nombre de bucket debe ser único en todas las cuentas y regiones. Una vez que se crea un bucket, no se puede cambiar su nombre. De acuerdo con las reglas de nomenclatura de DNS aplicadas globalmente, un nombre de bucket de OBS: ● Debe ser único en todas las cuentas y regiones. El nombre de un bucket eliminado se puede reutilizar para otro bucket o un sistema de archivos paralelo al menos 30 minutos después de la eliminación. ● Debe contener entre 3 y 63 caracteres. Solo se permiten letras minúsculas, dígitos, guiones (-) y puntos (.). ● No puede comenzar o finalizar con un período (.) o guion (-), y no puede contener dos períodos consecutivos (..) ni contener un período (.) y un guion (-) adyacentes entre sí. ● No se puede formatear como una dirección IP. **NOTA** Cuando accedes a OBS con HTTPS usando URLs de estilo alojado virtual, si el nombre del bucket contiene un punto (.), la verificación del certificado fallará. Para evitar este problema, se recomienda no utilizar períodos (.) en los nombres de bucket.
Data Redundancy Policy	● **Multi-AZ storage**: Los datos se almacenan en múltiples AZ para lograr una mayor fiabilidad. ● **Single-AZ storage**: Los datos se almacenan en una sola AZ, con costos más bajos. Para obtener más información acerca de la comparación de rendimiento entre el almacenamiento de multi-AZ y el almacenamiento de una sola AZ, consulte **Comparación de clases de almacenamiento**. Una vez que se crea un bucket, la política de redundancia de datos no se puede cambiar, así que elija la política que pueda satisfacer sus necesidades. ● El almacenamiento de multi-AZ no está disponible para los bucket de la clase de almacenamiento Archive.
Default Storage Class	Clases de almacenamiento de un bucket. Las diferentes clases de almacenamiento cumplen con diferentes requisitos de rendimiento y costes de almacenamiento. ● La clase de almacenamiento Standard es para almacenar un gran número de archivos calientes o pequeños archivos a los que se accede con frecuencia (múltiples veces al mes en promedio) y requieren una recuperación rápida. ● La clase de almacenamiento Infrequent Access es para almacenar datos a los que se accede con menos frecuencia (menos de 12 veces al año en promedio) y requiere una recuperación rápida. ● La clase de almacenamiento Archive es para archivar datos a los que rara vez se accede (una vez al año en promedio) y no tiene requisitos para una recuperación rápida. Para obtener más información, consulte **Clases de almacenamiento**.

Parámetro	Descripción
Bucket Policy	Controla los permisos de lectura y escritura de los bucket. ● **Private**: No se concede ningún acceso más allá de la configuración de ACL del bucket. ● **Public Read**: Cualquiera puede leer objetos en el bucket. ● **Public Read and Write**: Cualquier persona puede leer, escribir o eliminar objetos en el bucket.
Server-Side Encryption	Seleccione **SSE-KMS**. Para el tipo de clave de encriptación, puede elegir **Default** o **Custom**. Si se utiliza **Default**, se utilizará la clave predeterminada de la región actual para cifrar los objetos. Si no existe una clave predeterminada, OBS crea una la primera vez que carga un objeto. Si se utiliza **Custom**, puede elegir una clave personalizada que haya creado en la consola de KMS para cifrar los objetos. Si se elige **SSE-OBS**, las claves creadas y gestionadas por OBS se utilizan para la encriptación. Cuando la encriptación del lado del servidor está habilitado para un bucket, puede configurar el objeto que cargue para que herede la encriptación del bucket o elegir SSE-KMS o SSE-OBS.
WORM	When you enable write-once-read-many (WORM), you can configure a retention policy for the current bucket. The object version which the retention policy is applied to cannot be deleted within a specified period. You can only enable WORM when you create a bucket. Once enabled for a bucket, WORM cannot be disabled. When you enable WORM, OBS automatically enables versioning for the bucket, and versioning cannot be suspended later for that bucket.
Direct Reading	La lectura directa le permite descargar directamente objetos de la clase de almacenamiento Archive sin restaurarlos primero. La lectura directa es una función facturable. Para obtener información detallada, consulte **Detalles de los precios de productos**. No importa qué clase de almacenamiento predeterminada seleccione, puede habilitar la lectura directa para su bucket. Por ejemplo, si selecciona la clase de almacenamiento Standard y habilita la lectura directa para el bucket, puede descargar directamente los objetos almacenados en la clase de almacenamiento Archive desde el bucket.
Enterprise Project	Puede agregar un bucket a un proyecto de empresa para la gestión unificada. Cree un proyecto de empresa haciendo referencia a **Crear un proyecto de empresa**. El proyecto de empresa predeterminado se denomina **default**. **NOTA** Solo una cuenta de empresa puede configurar proyectos de empresa. OBS ReadOnlyAccess y OBS OperateAccess son las autorizaciones detalladas del grupo de usuarios de proyecto empresarial en OBS.

Parámetro	Descripción
Tags	Opcional. Las etiquetas se utilizan para identificar y clasificar bucket en OBS. Cada etiqueta está representada por un par clave-valor. Para obtener más información, consulte **Etiquetas**.

Paso 4 Haga clic en **Create Now**.

----Fin

Operaciones relacionadas

Después de crear el bucket, puede cambiar su clase de almacenamiento realizando los siguientes pasos:

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, localice el bucket que desee y haga clic en **Change Storage Class** a la derecha.

Paso 3 Seleccione la clase de almacenamiento deseada y haga clic en **OK**.

NOTA

- Cambiar la clase de almacenamiento de un bucket no se cambia la clase de almacenamiento de los objetos existentes en el bucket.
- Un objeto hereda la clase de almacenamiento de bucket de forma predeterminada, si no se especifica ninguna otra clase de almacenamiento para el objeto al cargarlo. Cuando se cambia la clase de almacenamiento de bucket, los objetos recién cargados heredan la nueva clase de almacenamiento de bucket de forma predeterminada.

----Fin

5.2 Consulta de información básica de un bucket

En OBS Console, puede ver detalles sobre un bucket, que incluyen información y configuraciones básicas de bucket.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Overview**.

Paso 4 En **Basic Information**, vea la información básica del bucket.

Figura 5-2 Información básica sobre el bucket

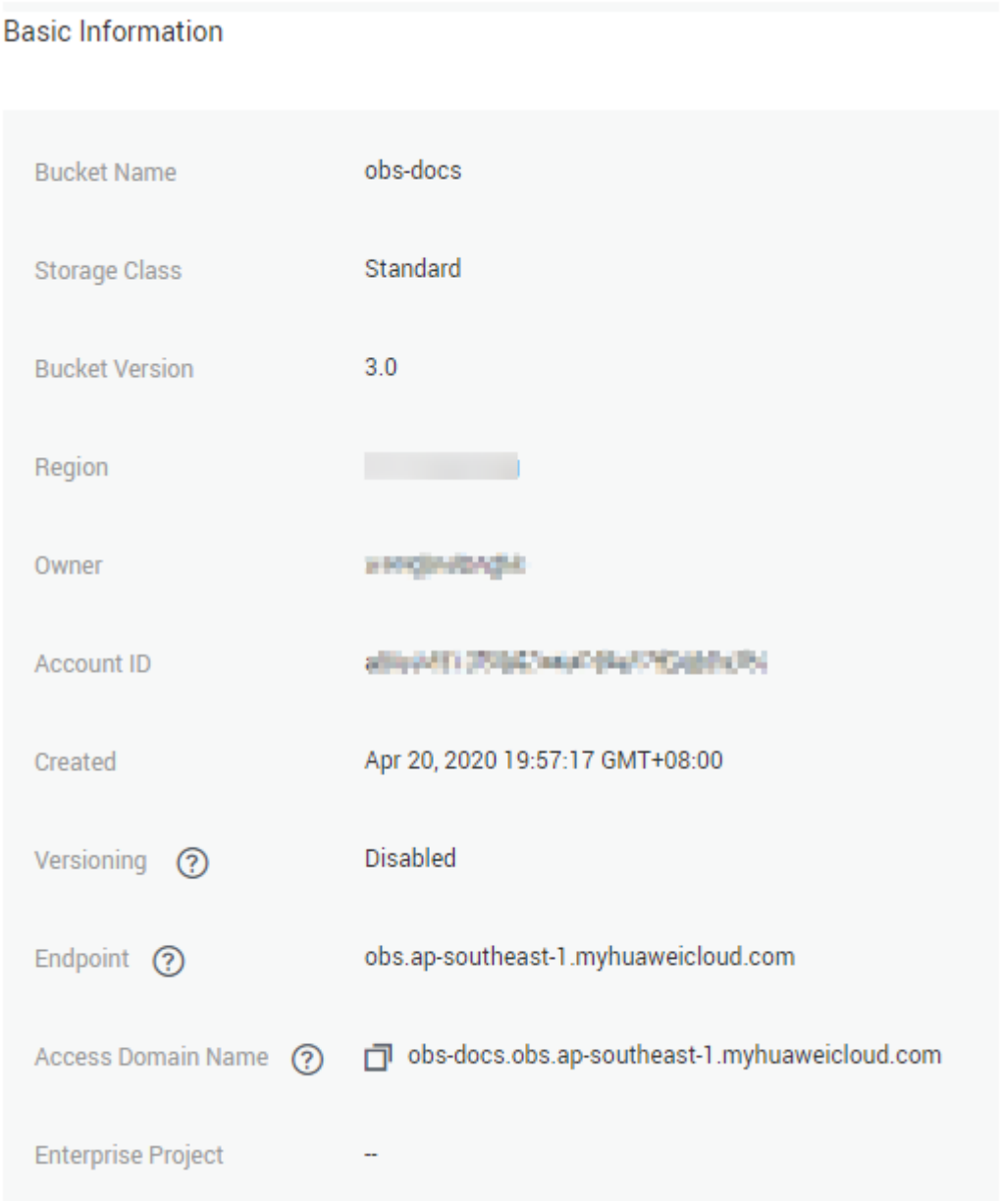


Tabla 5-2 Descripción del parámetro

Parámetro	Descripción
Bucket Name	Nombre del bucket.
Storage Class	Clase de almacenamiento del bucket, que puede ser **Standard**, **Infrequent Access** o **Archive**.
Bucket Version	ID de versión de un bucket. **3.0** indica la última versión del bucket y **--** indica versiones anteriores a la 3.0.
Region	Región donde reside el bucket.
Owner	Propietario se refiere a la cuenta que creó el bucket.

Parámetro	Descripción
Account ID	Identidad única del propietario del bucket, que es la misma que el **Account ID** en la página **My Credentials**.
Created	Tiempo en el que se completa la creación de un bucket.
Versioning	Estado de control de versiones
Endpoint	Este parámetro especifica el punto de conexión de la región donde se encuentra el bucket. OBS proporciona un punto de conexión para cada región. Un punto de conexión es un nombre de dominio para acceder a OBS en una región y se utiliza para procesar solicitudes de acceso de esa región. Un punto de conexión de OBS se mantiene sin cambios tanto en redes internas como externas. Después de configurar el **acceso con la intranet**, puede acceder a OBS con una red interna.
Access Domain Name	OBS asigna a cada bucket un nombre de dominio predeterminado. Un nombre de dominio es la dirección de un bucket en el Internet. Se puede utilizar para acceder a un bucket por Internet. Es aplicable al desarrollo de aplicaciones en la nube y escenarios de intercambio de datos. Estructura: *BucketName.Endpoint*
Data Redundancy Policy	Política de almacenamiento de redundancia de datos de un bucket. Se puede configurar para almacenamiento multi-AZ o almacenamiento de un solo-AZ. Esta configuración no se puede cambiar después de crear el bucket.
Enterprise Project	Proyecto de empresa al que pertenece un bucket

NOTA

Las estadísticas de **Used Capacity** y **Objects** no son datos en tiempo real, que generalmente se actualizan con 15 minutos de retraso.

----Fin

5.3 Búsqueda de bucket

Puede buscar un bucket por caracteres contenidos en su nombre.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En el cuadro de búsqueda situado en la esquina superior derecha sobre la lista de bucket, introduzca los caracteres incluidos en el nombre del bucket deseado.

Paso 3 Haga clic en  .

Los buckets que cumplen los criterios de búsqueda se muestran en la lista de bucket.

Por ejemplo, si desea buscar los bucket cuyos nombres contengan **test** solo tiene que escribir **test** en el cuadro de búsqueda y hacer clic en  . A continuación, se muestran todas los bucket que contienen **test** en sus nombres.

----Fin

5.4 Eliminación de un bucket

Puede eliminar bucket no deseados en OBS Console para liberar la cuota de bucket.

Requisitos previos

- Todos los objetos del bucket se han eliminado permanentemente. Se debe vaciar un bucket para poder eliminarlo.

  AVISO

  Los objetos de las fichas **Objects**, **Deleted Objects** y **Fragments** deben eliminarse.

- Un bucket solo puede ser eliminado por el propietario del bucket.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, seleccione el bucket que desea eliminar y, a continuación, haga clic en **Delete** a la derecha.

NOTA

El nombre de un bucket eliminado se puede reutilizar para un bucket o un sistema de archivos paralelo al menos 30 minutos después de la eliminación.

Paso 3 Haga clic en **Yes** para confirmar la eliminación.

----Fin

6 Gestión de objetos

6.1 Creación de la carpeta

Esta sección describe cómo crear una carpeta en OBS Console. Las carpetas facilitan la gestión de datos en OBS.

Información de referencia

- A diferencia de un sistema de archivos, OBS no implica los conceptos de archivo y carpeta. Para una fácil gestión de datos, OBS proporciona un método para simular carpetas. En OBS, un objeto se simula como una carpeta agregando una barra diagonal (/) al final del nombre del objeto en OBS Console.If you call the API to list objects, paths of objects are returned. In an object path, the content following the last slash (/) is the object name. If a path ends with a slash (/), it indicates that the object is a folder. The hierarchical depth of the object does not affect the performance of accessing the object.
- OBS Console no admite la descarga de carpetas. Puede usar OBS Browser+ para descargar carpetas.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Haga clic en **Create Folder** o haga clic en una carpeta de la lista de objetos para abrirlo y, a continuación, haga clic en **Create Folder**.

Paso 4 En el cuadro de texto **Folder Name**, escriba un nombre para la carpeta.

- Puede crear carpetas de un solo nivel o de varios niveles.
- El nombre no puede contener las siguientes characters especiales: \:*?"<>|+
- El nombre no puede comenzar o terminar con un punto (.) o una barra diagonal (/).
- La ruta de acceso absoluta de la carpeta no puede sobrepasar los 1023 caracteres.
- La barra (/) separa y crea múltiples niveles de carpetas en el acto.
- El nombre no puede contener dos o más barras (/) consecutivas.

Paso 5 Haga clic en **OK**.

----Fin

Procedimiento de seguimiento

Puede hacer clic en **Copy Path** a la derecha para copiar la ruta de la carpeta. Puede compartir la ruta con otros usuarios. A continuación, abren el bucket donde se almacena el objeto e introducen la ruta en el cuadro de búsqueda para encontrar el objeto.

6.2 Carga de un objeto

Esta sección describe cómo cargar archivos locales a OBS por Internet. Estos archivos pueden ser textos, imágenes, videos o cualquier otro tipo de archivos.

Limitaciones y restricciones

OBS Console tiene restricciones sobre el tamaño y el número de archivos cargados.

- En las regiones donde se admite la carga por lotes, se puede cargar un máximo de 100 archivos a la vez, con un tamaño total máximo de 5 GB.
- En las regiones donde no se admite la carga por lotes, solo se puede cargar un archivo a la vez, con un tamaño máximo de 50 MB.

Por lo tanto, para cargar un solo archivo, su tamaño máximo puede ser de 5 GB en una carga por lotes o 50 MB en una sola carga.

Para cargar un archivo de más de 5 GB, pero no más de 48.8 TB, puede usar **OBS Browser+** u **obsutil**, o la carga de varias partes de SDK o de API de OBS.

OBS Browser+ le permite subir un máximo de 500 archivos a la vez. No hay límite en el número de archivos que puede subir usando obsutil a la vez.

Si tiene más datos que cargar, consulte **Migración de datos locales a OBS**.

NOTA

La carga por lotes solo está disponible cuando se cumplen las dos condiciones siguientes:

1. El bucket se encuentra en cualquiera de las siguientes regiones:
2. La versión del bucket es 3.0. Para ver la versión del bucket, consulte **Consulta de información básica de un bucket**.

Si el control de versiones está deshabilitado para el bucket y carga un nuevo archivo con el mismo nombre que el que cargó anteriormente en el bucket, el nuevo archivo sobrescribe automáticamente el archivo anterior y no conserva su información de ACL. Si carga una nueva carpeta con el mismo nombre que se usó con una carpeta anterior en el bucket, las dos carpetas se fusionarán y los archivos de la nueva carpeta sobrescribirán archivos con nombre en la carpeta anterior.

Después de habilitar el control de versiones para su bucket, si el nuevo archivo que subió tiene el mismo nombre que el que subió anteriormente al bucket, se agregará una nueva versión de archivo en el bucket. Para obtener más información, consulte **Control de versiones**.

Requisitos previos

- Se ha creado al menos un bucket.
- Si desea clasificar archivos, puede crear carpetas y subir archivos a diferentes carpetas. Para obtener más información sobre cómo crear una carpeta, consulte **Creación de la carpeta**

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Vaya a la carpeta en la que se cargan los objetos. Haga clic en **Upload Object**. Aparece el cuadro de diálogo **Upload Object**.

A continuación se utiliza la carga por lotes como ejemplo. Para las regiones que admiten solo una carga única, realice las operaciones según se le indique.

NOTA

Si los archivos que desea cargar en OBS se almacenan en OneDrive de Microsoft, se recomienda que los nombres de estos archivos contengan un máximo de 32 caracteres para garantizar la compatibilidad.

Figura 6-1 Carga de objetos

Paso 4 Seleccione una clase de almacenamiento. Si no especifica una clase de almacenamiento, el objeto que cargue heredará la clase de almacenamiento predeterminada del bucket.

> **NOTA**
>
> Un objeto puede tener una clase de almacenamiento diferente de su bucket. Puede especificar una clase de almacenamiento para un objeto al cargarlo, o puede cambiar la clase de almacenamiento de objeto después de cargar el objeto.

Paso 5 Agregue un archivo o carpeta para cargar arrastrándolo al área **Upload Object**.

También puede hacer clic en **add file** en el área **Upload Object** para seleccionar archivos.

Paso 6 **Server-Side Encryption**: Seleccione **Disable**, **SSE-KMS** o **SSE-OBS**. Para obtener más información, véase **Carga de un objeto en modo de encriptación del lado del servidor**.

> **NOTA**
>
> Si un bucket tiene la encriptación del lado del servidor configurada, puede seleccionar **Inherit from bucket** al cargar un objeto en el bucket, para que el objeto herede la configuración de encriptación del bucket.

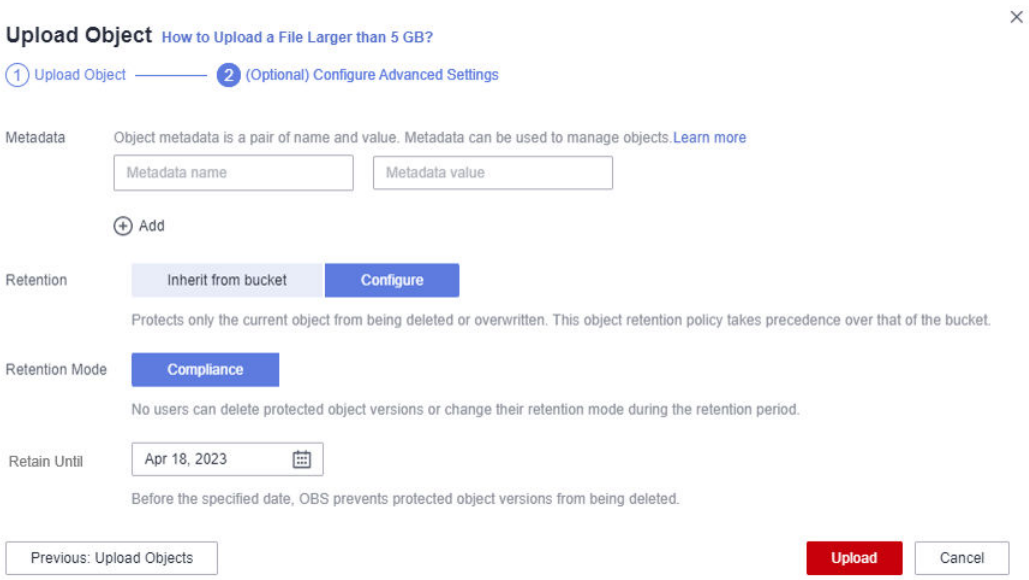
Paso 7 (Opcional) Para configurar el metadato o las políticas de retención de WORM, haga clic en **Next: (Optional) Configure Advanced Settings**.

> **NOTA**
>
> Las políticas de retención de WORM se pueden configurar en la configuración avanzada solo cuando WORM está habilitado para el bucket.

Configuración de metadatos: Agregar metadatos ContentDisposition, ContentLanguage, WebsiteRedirectLocation, ContentEncoding o ContentType según sea necesario. Para obtener más información, consulte la sección **Metadatos de objetos de OBS**. Los metadatos son un conjunto de pares nombre-valor. El valor de metadatos no se puede dejar en blanco. Puede agregar dos o más entradas de metadatos haciendo clic en **Add**.

Configuración de la retención de WORM: Elija **Inherit from bucket** o **Configure** y especifique un período de retención para proteger automáticamente los nuevos objetos cargados en el bucket de que se eliminen.

Figura 6-2 Configuración de metadatos o retención de WORM



Paso 8 Haga clic en **Upload**.

----Fin

Operaciones relacionadas

Al cargar un objeto, puede especificar una clase de almacenamiento para él. Después de cargar el objeto, también puede cambiar su clase de almacenamiento. El procedimiento es el siguiente:

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Seleccione el objeto de destino y elija **More** > **Change Storage Class** a la derecha.

NOTA

También puede seleccionar varios objetos a la vez y elegir **More** > **Change Storage Class** encima de la lista de objetos, para cambiar la clase de almacenamiento de objetos por un lote.

Las clases de almacenamiento de los objetos de Archive no se pueden cambiar si no se restauran.

Paso 4 Seleccione la clase de almacenamiento deseada y haga clic en **OK**.

----Fin

NOTA

- Los objetos se pueden cambiar de la clase de almacenamiento de Standard a la de Infrequent Access o de Archive, o de Infrequent Access a la clase de almacenamiento Standard or Archive. Los objetos de Archive deben restaurarse antes de cambiarse a la clase de almacenamiento de Standard o Infrequent Access. Cambie de Infrequent Access o Archive a otras clases de almacenamiento conlleva cargos de restauración. Seleccione una opción de cambio adecuada en función de sus necesidades reales.
- Cuando la clase de almacenamiento se cambia a Archive, el estado de restauración del objeto cambia a **Unrestored**.
- También puede configurar una regla de ciclo de vida para cambiar la clase de almacenamiento de un objeto. Para obtener más información, véase **Configuración de una regla de ciclo de vida**.

Procedimiento de seguimiento

Puede hacer clic en **More** > **Copy Path** a la derecha de un objeto para copiar su ruta.

Puede compartir la ruta con otros usuarios. A continuación, abren el bucket donde se almacena el objeto e introducen la ruta en el cuadro de búsqueda para encontrar el objeto.

6.3 Descarga de un objeto

Puede descargar archivos desde OBS Console a la ruta de acceso predeterminada del sistema o a una ruta de descarga personalizada del equipo local.

Limitaciones y restricciones

- Los objetos de la clase de almacenamiento Archive sólo se pueden descargar cuando están en el estado **Restored**.

- La descarga por lotes no es compatible con OBS Console. Para descargar archivos o carpetas por lotes, puede usar OBS Browser+ u obsutil.
  - **Descargar archivos o carpetas con OBS Browser+**
  - **Descargar objetos con obsutil**

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Seleccione el archivo que desea descargar. A continuación, haga clic en **Download** o **More** > **Download As** a la derecha.

También puede seleccionar varios archivos y elegir **More** > **Download** encima de la lista de archivos.

NOTA

En el cuadro de diálogo **Download As**, haga clic con el botón secundario en el objeto y elija **Copy Link Address** en el menú contextual para obtener la dirección de descarga del objeto.

----Fin

6.4 Compartir un objeto

Escenarios

Puede compartir los URL temporales de sus objetos con otros para que accedan a los objetos almacenados en OBS.

Información de antecedentes

El uso compartido de archivos es temporal. Todos los URL de uso compartido solo son válidos por un período de tiempo limitado.

Un URL temporal consiste en el nombre de dominio de acceso y la información de autenticación temporal de un archivo. Ejemplo:

```
https://bucketname.obs.ap-southeast-1.myhuaweicloud.com:443/image.png?
AccessKeyId=xxx&Expires=xxx&response-content-disposition=xxx&x-obs-security-
token=xxx&Signature=xxx
```

La información de autenticación temporal contiene los parámetros **AccessKeyId**, **Expires**, **x-obs-security-token**, y **Signature**. **AccessKeyId**, **x-obs-security-token** y **Signature** se utilizan para la autenticación. El parámetro **Expires** especifica el período de validez de la autenticación. Para obtener más información acerca de los métodos y parámetros de autenticación temporal, consulte **Autenticación de firma en un URL** en la *Referencia de API de OBS*.

Después de compartir un objeto en OBS Console, el sistema generará un URL que contiene la información de autenticación temporal, válida durante cinco minutos desde su generación de forma predeterminada. Cada vez que cambia el período de validez de una URL, OBS obtiene la información de autenticación de nuevo para generar un nuevo URL para compartir, que tiene efecto desde el momento en que se cambia el período de validez.

Limitaciones y restricciones

- Un objeto compartido desde OBS Console puede ser válido durante un minuto a 18 horas. Si necesita un período de validez más largo para un objeto compartido, utilice la herramienta cliente OBS Browser+ que permite un período de validez de hasta un año. Si desea que un objeto compartido sea válido de forma permanente, utilice una política de bucket para conceder permisos de lectura públicos a usuarios anónimos en el objeto haciendo referencia a la **Concesión de permisos de lectura públicos en objetos a usuarios anónimos**.
- Solo los bucket de la versión 3.0 admiten el uso compartido de archivos. Puede ver la versión del bucket en el área **Basic Information** de la página **Overview** de un bucket.
- Los objetos de Archive sólo se pueden compartir después de que se hayan restaurado.
- Deep Archive objects can be shared only after they have been restored.
- El uso compartido de objetos está disponible en todas las regiones excepto en CN Southwest-Guiyang1.

Procedimiento

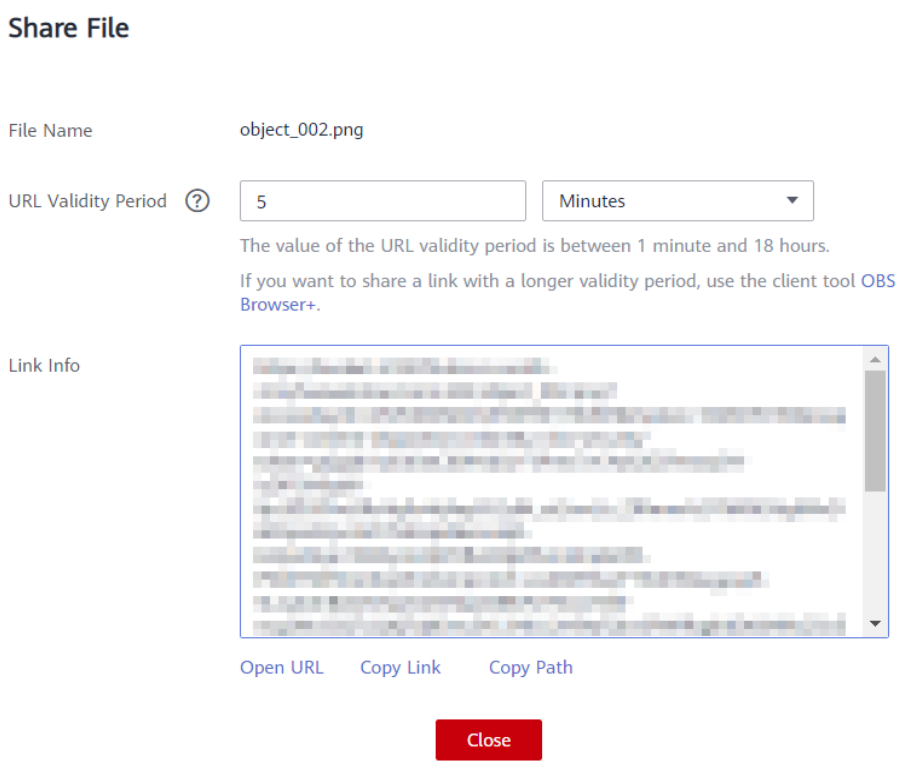
Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Busque el archivo que desea compartir y haga clic en **Share** en la columna **Operation**.

Una vez que se abre el cuadro de diálogo **Share File**, la dirección URL es efectiva y válida durante cinco minutos de forma predeterminada. Si cambia el período de validez, la información de autenticación en el URL cambia en consecuencia, y el nuevo período de validez del URL comienza con el cambio.

Figura 6-3 Compartir un archivo



Paso 4 Opere el URL de la siguiente manera:

- Haga clic en **Open URL** para obtener una vista previa del archivo en una nueva página o descargarlo directamente a su ruta de descarga predeterminada.
- Haga clic en **Copy Link** para compartir el enlace con otros para que puedan acceder a este archivo mediante un navegador.
- Haga clic en **Copy Path** para compartir la ruta de acceso del archivo con los usuarios que tienen permisos de acceso a bucket. A continuación, los usuarios pueden buscar el archivo pegando la ruta compartida en el cuadro de búsqueda del bucket.

NOTA

Dentro del período de validez del URL, cualquier persona que tenga el URL puede acceder al archivo.

----Fin

6.5 Compartir una carpeta

Escenarios

Puede compartir sus carpetas en OBS con otros usuarios.

Información de antecedentes

El uso compartido de carpetas es temporal y tiene un período de validez. Puede compartir temporalmente carpetas por código de acceso o URL:

- Por código de acceso: especifique un código de acceso de seis dígitos antes de crear una tarea de uso compartido. Después de crear la tarea de uso compartido, OBS agrega los enlaces de descarga de todos los objetos de la carpeta a un sitio web estático que está alojado en un bucket de OBS público. Entonces cualquier persona que tenga el URL temporal creado y el código de acceso puede acceder al sitio web estático y descargar los archivos compartidos.
- Por URL: Especifique un período de validez y, a continuación, comparta el enlace generado con otros. Cualquier persona puede usar una firma para acceder a todos los objetos de la carpeta compartida.

Limitaciones y restricciones

- Una carpeta compartida desde OBS Console puede ser válida durante un minuto a 18 horas. Si necesita un período de validez más largo para una carpeta compartida, utilice la herramienta de cliente de OBS Browser+ que permite un período de validez de hasta un año. Si desea que una carpeta compartida sea válido de forma permanente, utilice una política de bucket para conceder permisos de lectura públicos a usuarios anónimos en la carpeta haciendo referencia a la **Concesión de permisos de lectura públicos en objetos a usuarios anónimos**.
- La función de uso compartido de carpetas solo está restringida a algunas regiones.
- Solo los bucket de la versión 3.0 o posterior admiten la función de compartir carpetas. Puede ver la versión del bucket en el área **Basic Information** de la página **Overview** de un bucket.
- Los objetos archivados en una carpeta deben restaurarse en el bucket antes de poder descargarlos.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

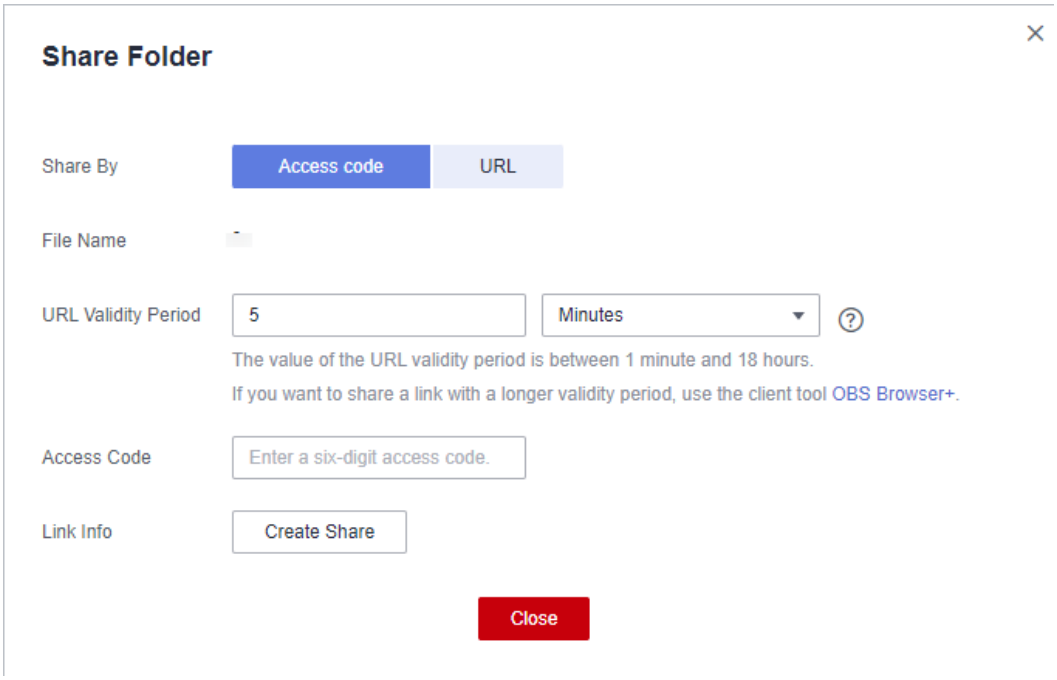
Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Busque la carpeta que desea compartir y haga clic en **Share** en la columna **Operation**. Aparece el cuadro de diálogo **Share Folder**.

Paso 4 Comparta la carpeta por código de acceso o URL.

Paso 5 Método 1: Compartir la carpeta por código de acceso.

Figura 6-4 Compartir por código de acceso



1. Elija **Access code** para **Share By**.
2. Configure los parámetros.

   Tabla 6-1 Parámetros para compartir una carpeta con un código de acceso

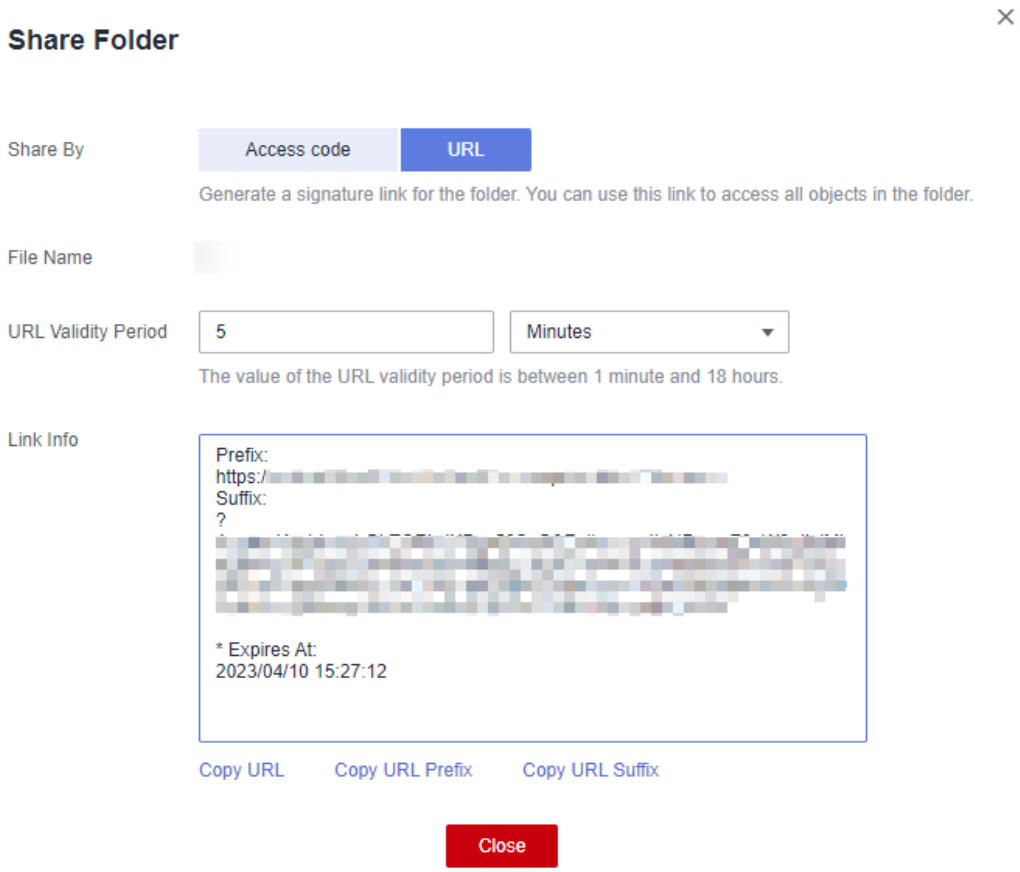
Parámetro	Descripción
URL Validity Period	El período de validez se mide por minutos u horas, y varía de un minuto a 18 horas. El valor predeterminado es cinco minutos. Dentro del período de validez del URL, cualquier persona que tenga el URL puede acceder a la carpeta.
Access Code	Un código de seis dígitos. Se requiere un código de acceso para acceder a los objetos de la carpeta compartida.

3. Haga clic en **Create Share** para generar el URL de uso compartido de la carpeta.
4. Envíe el URL y el código de acceso a otros para que accedan a la carpeta.
5. Verifique que otros usuarios puedan realizar las siguientes operaciones:
   a. Acceda a la carpeta compartida en un explorador.
      i. Abra el URL compartido en un navegador web.
      ii. En el cuadro de diálogo que se muestra, escriba el código de acceso y los objetos de acceso en la carpeta compartida.
   b. Acceda a la carpeta compartida en OBS Browser+.
      i. Inicie OBS Browser+.

ii. En la página de inicio de sesión, haga clic en **Authorization Code Login**.
iii. Introduzca el código de autorización y el código de acceso.
iv. Haga clic en **Log In** para acceder a la carpeta compartida.

Paso 6 Método 2: Compartir la carpeta por URL.

Figura 6-5 Compartir por URL



1. Elige **URL** para **Share By**.
2. Configure los parámetros.

Tabla 6-2 Parámetros para compartir una carpeta por URL

Parámetro	Descripción
URL Validity Period	Un período de validez es de un minuto a 18 horas. El valor predeterminado es cinco minutos. Dentro del período de validez del URL, cualquier persona que tenga el URL puede acceder a la carpeta.

3. Haga clic en **Copy URL** y comparta el URL con otro usuario. El usuario puede utilizar este URL para acceder a todos los objetos de esta carpeta. El enlace para compartir consiste en el nombre de dominio del bucket (prefijo) y la información de firma (sufijo). Los usuarios pueden agregar una ruta de acceso a un objeto después del prefijo de un

enlace compartido para acceder o descargar el objeto especificado en una carpeta, como se muestra en **Figura 6-6**.

4. Compruebe que un usuario puede usar el URL de uso compartido para acceder a todos los objetos de la carpeta.
   a. Abra el navegador.
   b. Introduzca el URL de uso compartido en el cuadro de dirección y pulse **Enter** para listar todos los objetos de la carpeta.
   c. Copie la ruta del objeto y péguela después del prefijo.
   d. Presione **Enter**. A continuación, puede acceder al objeto especificado y descargarlo.

Figura 6-6 Acceso a un objeto con un URL compartido

----Fin

6.6 Búsqueda de un objeto o una carpeta

Esta sección describe cómo buscar un archivo o carpeta por el prefijo de nombre en OBS Console.

Búsqueda por prefijos de nombres de objetos

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el cuadro de búsqueda situado encima de la lista de objetos, escriba el prefijo de nombre del archivo o carpeta que desea buscar.

En el directorio raíz del bucket se muestran los archivos y carpetas cuyo nombre comienza con el prefijo especificado.

NOTA

Si desea buscar objetos dentro de una carpeta, puede utilizar cualquiera de los métodos siguientes:

- En el cuadro de búsqueda del directorio raíz, escriba *folder path*/*object name prefix*. Por ejemplo, si escribe **abc/123/example**, se muestran todos los archivos y carpetas cuyo nombre tiene el prefijo **example** en la carpeta **abc/123**.
- Alternativamente, puede abrir la carpeta específica e introducir el prefijo del nombre de objeto en el cuadro de búsqueda de esa carpeta. Por ejemplo, puede abrir la carpeta **abc/123** e introducir **example** en el cuadro de búsqueda. A continuación, se muestran todos los archivos y carpetas cuyo nombre tiene el prefijo **example** en la carpeta **abc/123**.

Paso 4 Haga clic en . Los resultados de la búsqueda se muestran en la lista de objetos.

----Fin

Operaciones relacionadas

En la lista de objetos, haga clic en junto al nombre del objeto, el tamaño o la última hora de modificación para ordenar los objetos.

6.7 Enumeración de objetos

En OBS Console, cuando va a la página de lista de objetos de un bucket, los objetos se muestran por nombre de forma predeterminada. También puede ordenar los objetos por su tamaño o por la última hora de modificación.

Listado de objetos en OBS Console

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Vea los objetos mostrados. Todos los objetos del bucket aparecerán en una lista y cada página tiene 50 objetos mostrados de forma predeterminada.

----Fin

Listado de objetos con herramientas de OBS

- Las operaciones a nivel de bucket en OBS Browser+ son similares a las de OBS Console. Puede enumerar objetos siguiendo las instrucciones en OBS Browser+. Para obtener más información sobre el navegador OBS+, consulte la **Introducción a OBS Browser+**.
- Los SDK de Java, Python, C, .NET, Node.js y Android se pueden usar para listar objetos en un bucket.
- Para utilizar la herramienta de línea de comandos obsutil para enumerar objetos de un bucket, consulte **Listado de objetos con obsutil**.
- Para invocar a una API para enumerar objetos en un bucket, consulte **Listado de objetos en un bucket**.

Notas importantes

- No se permite enumerar objetos especificando un número de página.
- Los objetos no se pueden enumerar por hora en la que se cargaron. Puede buscar objetos por el prefijo solamente. Para obtener más información, véase **Búsqueda de un objeto o una carpeta**.
- El tamaño y la última hora de modificación en la lista de objetos ordenan solo los objetos de la página actual.

6.8 Acceso a un objeto mediante su URL

Puede conceder a los usuarios anónimos el permiso de lectura de un objeto para que puedan tener acceso al objeto mediante la dirección URL del objeto compartido.

Requisitos previos

Los usuarios anónimos tienen el permiso de lectura para el objeto.

Para obtener más información sobre la concesión de permisos, consulte **Conceder permisos de lectura pública en objetos a usuarios anónimos**.

NOTA

Los objetos cifrados no se pueden compartir.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Haga clic en el objeto que desea compartir. La información del objeto se muestra en la parte superior de la página. El **Link** muestra el vínculo compartido del objeto. Para más detalles, consulte **Figura 6-7**.

Los usuarios anónimos pueden acceder al objeto haciendo clic en el URL. La dirección URL del objeto tiene el formato **https://***bucket name*.*domain name*/*directory level*/*object name*. Si el objeto reside en el directorio raíz del bucket, su URL no contiene el nivel de directorio. Para obtener más información sobre nombres de dominio, consulte **Nombres de dominio de OBS**.

Figura 6-7 Enlace de objeto

NOTA

- Para permitir que los usuarios anónimos tengan acceso a objetos en el almacenamiento de Archive mediante las direcciones URL, asegúrese de que estos objetos estén en el estado **Restored**.
- El método de uso de un navegador para acceder a objetos varía en función del tipo de objeto. Puede abrir directamente archivos**.txt** y**.html** usando un navegador. Sin embargo, cuando abre archivos **.exe** y **.dat** con un explorador, los archivos se descargan automáticamente en el equipo local.

----Fin

6.9 Restauración de objetos del almacenamiento Archive

Debe restaurar un objeto en la clase de almacenamiento Archive antes de poder descargarlo o acceder a él con un URL.

Para obtener más información sobre la duración y los precios de la restauración de datos, consulte **Detalles de precios del producto**.

Limitaciones y restricciones

- No puede suspender ni eliminar la tarea de restauración si se está restaurando un objeto de Archive.
- No se puede volver a restaurar un objeto en el estado **Restoring**.
- Después de restaurar un objeto, se generará una copia de objeto en la clase de almacenamiento Standard. De esta manera, hay un objeto de Archive y una copia de objeto de Standard en el bucket al mismo tiempo. Durante el período de validez de la restauración, se le cobrará por el espacio ocupado tanto por el objeto como por su copia. La copia se eliminará automáticamente una vez que expire la restauración.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

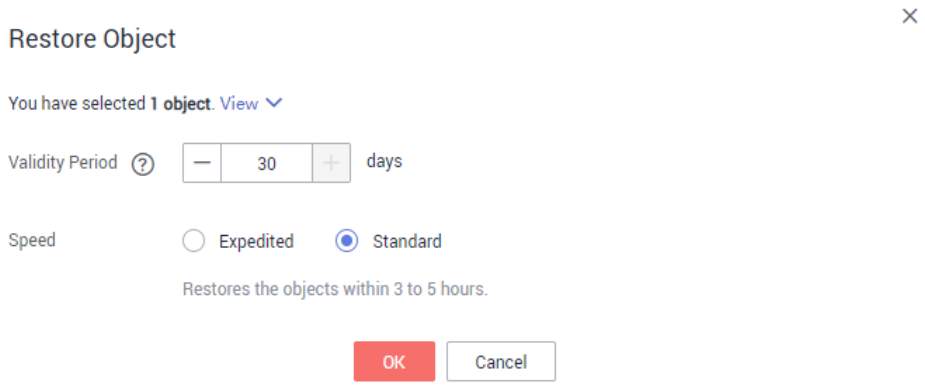
Paso 3 Seleccione el archivo que desea restaurar y haga clic en **Restore** a la derecha. Se muestra el siguiente cuadro de diálogo que se muestra en **Figura 6-8**.

Puede seleccionar varios archivos y elegir **More** > **Restore** encima de la lista de archivos para restaurarlos por lotes.

NOTA

Los objetos que se están restaurando no se pueden agregar para la restauración por lotes.

Figura 6-8 Restaurar un objeto



Paso 4 Configure el período de validez y la velocidad de la restauración. La tabla siguiente describe los parámetros.

Tabla 6-3 Parámetros para restaurar objetos

Parámetro	Descripción
Validity Period	Cuánto tiempo permanecerá el objeto en el estado **Restored**. Se inicia una vez que se restaura el objeto. El valor es un entero que oscila entre 1 y 30 (días). El valor predeterminado es **30**. Por ejemplo, si establece **Validity Period** en **20** al restaurar un objeto, 20 días después de restaurarlo correctamente, su estado cambiará de **Restored** a **Unrestored**.
Speed	Qué tan rápido se restaurará un objeto. ● **Expedited**: Los objetos de Archive se pueden restaurar en 1 a 5 minutos, y los objetos de Deep Archive se pueden restaurar en 3 a 5 horas. ● **Standard**: Los objetos de Archive se pueden restaurar en un plazo de 3 a 5 horas y los objetos de Deep Archive se pueden restaurar en un plazo de 5 a 12 horas.

Paso 5 Haga clic en **OK**.

La columna **Restoration Status** de la lista de objetos muestra los estados de restauración de los objetos.

Puede hacer clic en para actualizar manualmente el estado de restauración.

NOTA

El sistema comprueba el estado de restauración de archivos a las 00:00 UTC todos los días. El sistema comienza a contar el tiempo de caducidad desde el momento en que se completa la última comprobación.

----Fin

Operaciones relacionadas

Dentro del período de validez de un objeto restaurado, puede restaurar el objeto de nuevo. El período de validez se extiende porque comenzará de nuevo cuando se complete la última restauración.

NOTA

Si un objeto restaurado se restaura de nuevo, su tiempo de caducidad debe ser posterior al tiempo establecido para la restauración anterior. Supongamos que un objeto se restaura el 1 de enero y caducará 30 días después (el 30 de enero). Si el objeto se restaura de nuevo el 10 de enero y se hace que expire antes del 30 de enero (menos de 20 días después), esta acción de restauración se considera no válida.

6.10 Eliminación de un objeto o una carpeta

Escenarios

En OBS Console, puede eliminar manualmente archivos o carpetas que no sean necesarios para liberar espacio y reducir costos.

También puede configurar reglas de ciclo de vida para eliminar periódicamente y automáticamente algunos o todos los archivos y carpetas de un bucket. Para obtener más información, véase **Configuración de una regla de ciclo de vida**.

En escenarios de big data, los sistemas de archivos paralelos generalmente tienen niveles de directorio profundos y cada directorio tiene un gran número de archivos. En tal caso, la eliminación de directorios de sistemas de archivos paralelos puede fallar debido al tiempo de espera. Para solucionar este problema, se recomienda eliminar los directorios de cualquiera de las siguientes maneras:

1. En el cliente Hadoop que tiene OBSA, un complemento de cliente de OBS, incrustado, ejecuta el comando **hadoop fs - rmr obs://{***Name of a parallel file system***}/{***Directory name***}**.
2. Configure **una regla de ciclo de vida** para directorios para que se puedan eliminar en segundo plano según la regla de ciclo de vida preestablecida.

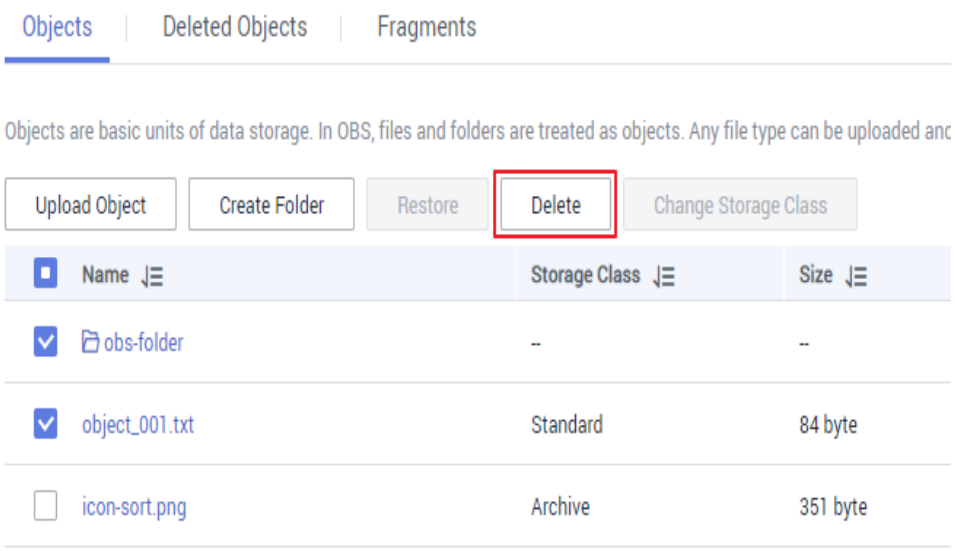
Información de antecedentes

Eliminación de objetos con control de versiones habilitado

Cuando el control de versiones está habilitado para un bucket, OBS funciona ligeramente diferente cuando se eliminan diferentes objetos.

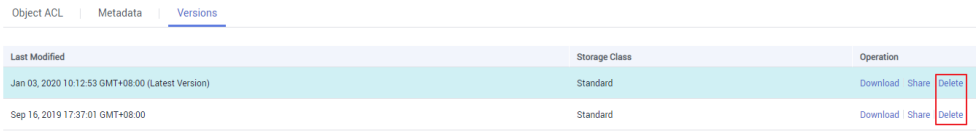
- Eliminación de un archivo o carpeta: El archivo o carpeta no se elimina permanentemente, sino que se conserva en la lista **Deleted Objects** y se marca con **Delete Marker**. En el cuadro **Deleted Objects**, haga clic en el nombre del objeto. En la ficha **Versions**, puede ver que la última versión del objeto tiene el marcador de eliminación.

Figura 6-9 Eliminación de un archivo o una carpeta



  - Para eliminar permanentemente el archivo o carpeta, elimínelo de nuevo de la lista **Deleted Objects**. Para obtener más información, véase **Procedimiento**.
  - Para recuperar el archivo eliminado, recupérelo desde la lista **Deleted Objects**. Para obtener más información, véase **Recuperación de un objeto**.
- Eliminación de una versión de objeto: La versión se eliminará permanentemente. Si la versión eliminada es la más reciente, la siguiente última versión se convierte en la última versión.

Figura 6-10 Eliminación de una versión de un objeto



Procedimiento

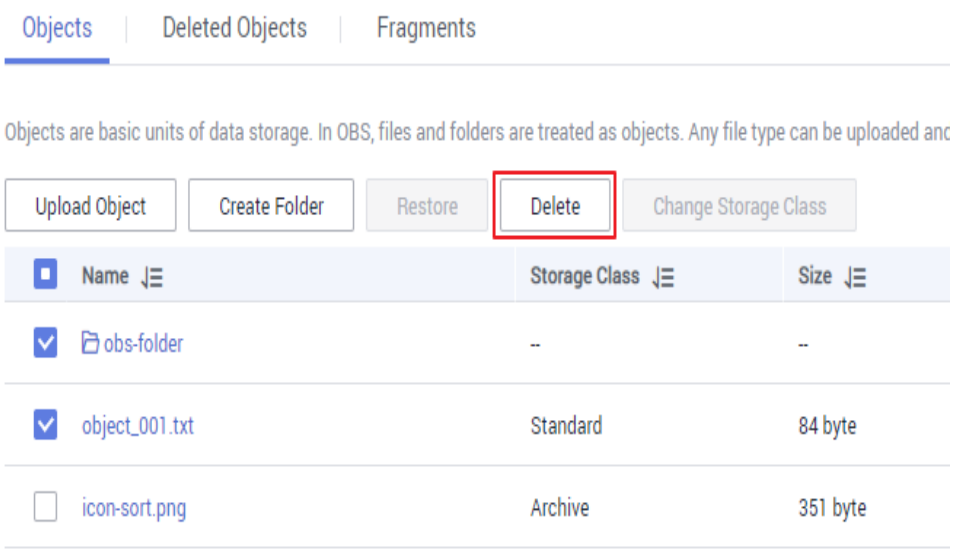
Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Seleccione el archivo o carpeta que desea eliminar y elija **More** > **Delete** a la derecha.

Puede seleccionar varios archivos o carpetas y hacer clic en **Delete** encima de la lista de objetos para eliminarlos por lotes.

Figura 6-11 Eliminación de un archivo o una carpeta



Paso 4 Haga clic en **Yes** para confirmar la eliminación.

Paso 5 Si el control de versiones está habilitado para el bucket, elimine de nuevo los archivos o carpetas eliminados de la lista **Deleted Objects** para eliminarlos permanentemente.

NOTA

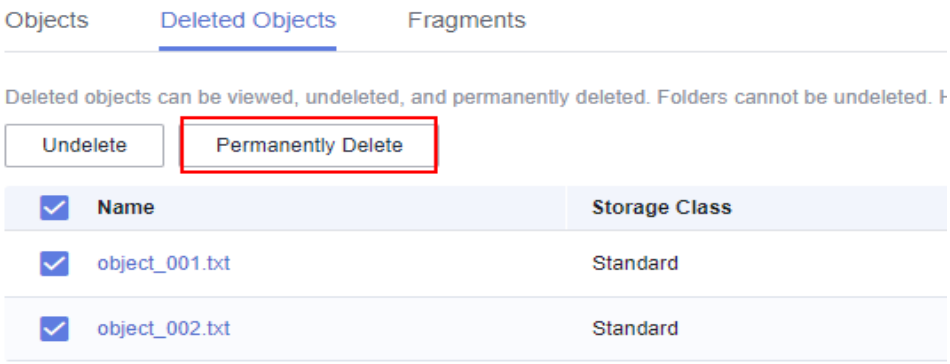
En un bucket con WORM habilitado, los objetos no se pueden eliminar permanentemente de la lista **Deleted Objects**. Puede eliminar permanentemente un objeto en la página de detalles del objeto. Para obtener más información, véase **Operaciones relacionadas**.

Del mismo modo, las carpetas tampoco se pueden eliminar permanentemente de la lista **Deleted Objects**. Para eliminar permanentemente una carpeta, solo puede **configurar una regla de ciclo de vida**.

1. Haga clic en **Deleted Objects**.
2. En la columna **Operation** del archivo o carpeta que se va a eliminar, haga clic en **Permanently Delete**.

   También puede seleccionar varios archivos o carpetas y hacer clic en **Permanently Delete** encima de la lista de objetos para eliminarlos por lotes.

Figura 6-12 Eliminar un archivo o carpeta de forma permanente

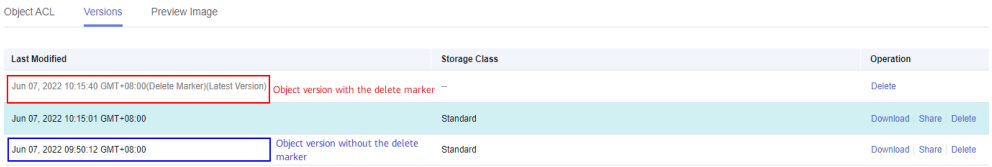


----Fin

Operaciones relacionadas

Cuando el control de versiones está habilitado, los archivos de la lista **Deleted Objects** también tienen varias versiones. Tenga en cuenta los siguientes puntos al eliminar diferentes versiones de archivos:

Figura 6-13 Versiones de archivos en la lista **Deleted Objects**



- Al eliminar una versión con el **Delete Marker** realmente recupera esta versión en lugar de eliminarla permanentemente. Para obtener más información, véase **Recuperación de un objeto**.
- Al eliminar una versión sin el **Delete Marker** se elimina esta versión de forma permanente. Esta versión no se recuperará incluso si el objeto se recupera más tarde.

6.11 Recuperación de un objeto

Escenarios

Si un bucket tiene activado el **control de versiones**, puede recuperar un objeto eliminado deshaciéndolo.

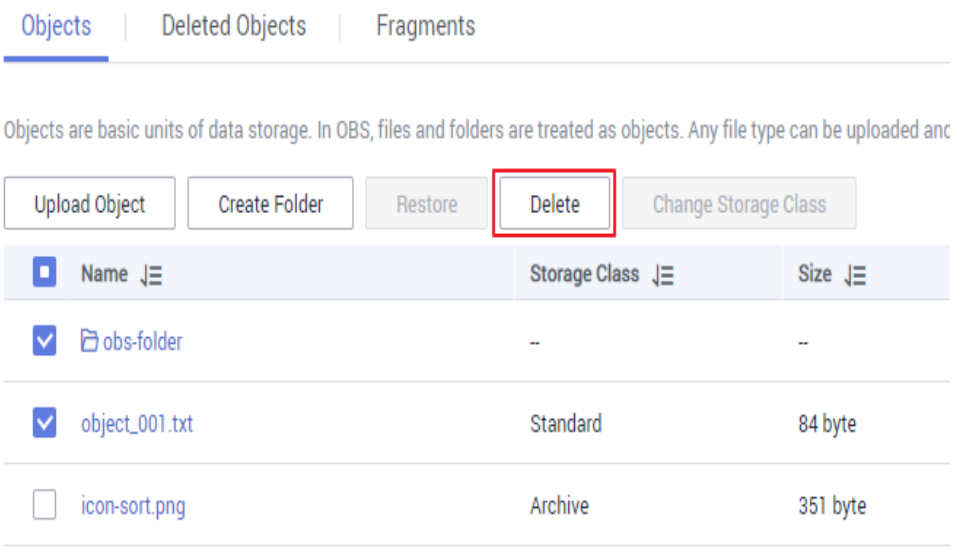
Información de referencia

Eliminación de objetos con control de versiones habilitado

Cuando el control de versiones está habilitado para un bucket, OBS funciona ligeramente diferente cuando se eliminan diferentes objetos.

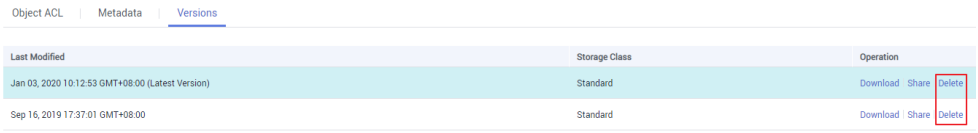
- Eliminación de un archivo o carpeta: El archivo o carpeta no se elimina permanentemente, sino que se conserva en la lista **Deleted Objects** y se marca con **Delete Marker**.

Figura 6-14 Eliminación de un archivo o una carpeta



  - Para eliminar permanentemente el archivo o carpeta, elimínelo de nuevo de la lista **Deleted Objects**. Para obtener más información, véase **Eliminación de un objeto o una carpeta**.
  - Para recuperar el archivo eliminado, recuperarlo de la lista **Deleted Objects**. Para obtener más información, véase **Procedimiento**.
- Eliminación de una versión de objeto: La versión se eliminará permanentemente. Si la versión eliminada es la más reciente, la siguiente última versión se convierte en la última versión.

Figura 6-15 Eliminación de una versión de un objeto



Recuperación de objetos con control de versiones habilitado

Cuando un bucket tiene activada la función de control de versiones, eliminar un archivo desde la lista **Objects** no significa que lo elimina permanentemente. El archivo eliminado se conservará con el **Delete Marker** en la lista **Deleted Objects**. Puede recuperar el archivo eliminado utilizando la operación **Undelete**.

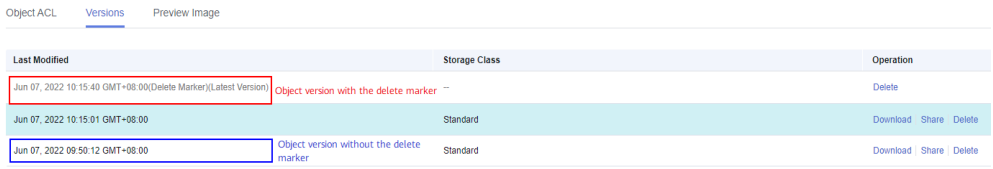
Tenga en cuenta los siguientes puntos al recuperar objetos:

1. Solo se pueden recuperar los archivos eliminados, pero no las carpetas.

   Después de recuperar un archivo eliminado, el archivo se recupera y aparecerá en la lista **Objects**. A continuación, puede realizar operaciones básicas en el archivo como normalmente lo hace con otros objetos. Si el archivo se almacenó en una carpeta antes de la eliminación, se recuperará a su ruta original después de recuperarlo.
2. Los archivos eliminados en **Deleted Objects** también conservan varias versiones. Al eliminar diferentes versiones de archivos, tenga en cuenta los siguientes puntos:

– Si elimina una versión con **Delete Marker**, en realidad recupera esta versión en lugar de eliminarla permanentemente. Para obtener más información, véase **Operaciones relacionadas**.
– Si elimina una versión sin **Delete Marker**, se eliminará de forma permanente. Esta versión no se recuperará, incluso si el objeto se recupera más tarde.

Figura 6-16 Versiones de archivos en la lista **Deleted Objects**



3. Un objeto eliminado debe tener al menos una versión sin el **Delete Marker** en la lista **Deleted Objects**. De lo contrario, el objeto no se puede recuperar.

Requisitos previos

- Se ha habilitado el control de versiones para el bucket. Para obtener más información, véase **Configuración del control de versiones**.
- El archivo que se va a recuperar está en la lista **Deleted Objects** y tiene al menos una versión sin **Delete Marker**.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

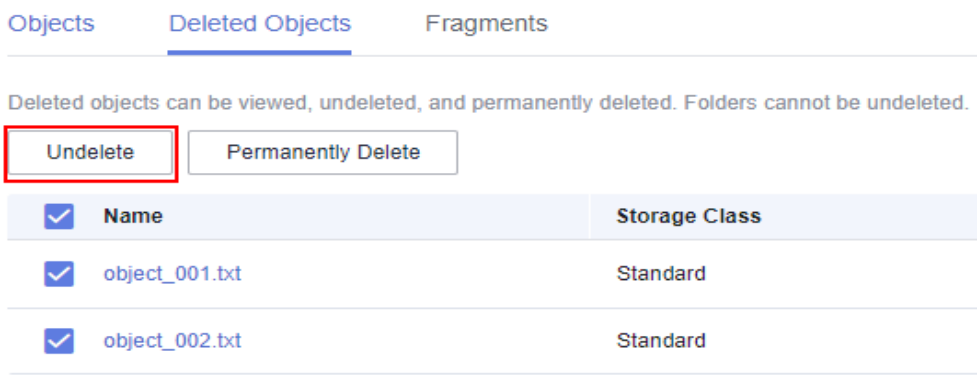
Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Haga clic en **Deleted Objects**.

Paso 4 En la fila del objeto eliminado que desea recuperar, haga clic en **Undelete** a la derecha.

Puede seleccionar varios archivos y haga clic en **Undelete** encima de la lista de objetos para recuperarlos por lotes.

Figura 6-17 Recuperar un archivo



----Fin

Operaciones relacionadas

Recuperar un archivo eliminando su versión con Delete Marker:

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

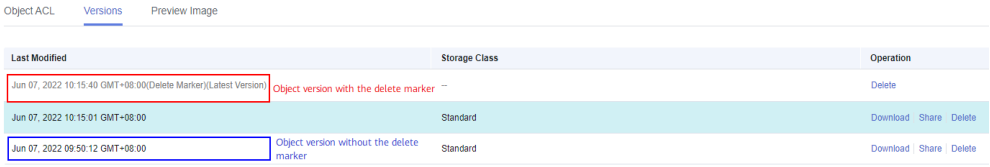
Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Haga clic en **Deleted Objects**.

Paso 4 Haga clic en el archivo eliminado que desea recuperar. Se muestra la información del archivo.

Paso 5 En la ficha **Versions**, vea todas las versiones del archivo.

Figura 6-18 Versiones de archivos en la lista **Deleted Objects**



- Si elimina una versión con **Delete Marker**, el archivo se recupera y se conserva en la lista **Objects**.
- Si elimina una versión sin **Delete Marker**, se eliminará de forma permanente.

----Fin

6.12 Gestión de fragmentos

Información de referencia

Los datos se pueden cargar en OBS mediante cargas de varias partes. Se generan fragmentos, si una carga multiparte falla debido a las siguientes razones (incluidas pero no limitadas a):

- La red se encuentra en malas condiciones y la conexión con el servidor de OBS se interrumpe con frecuencia.
- La tarea de carga se suspende manualmente.
- El dispositivo presenta fallas.
- El dispositivo se apaga repentinamente.

En OBS Console, se carga el almacenamiento utilizado por los fragmentos. Limpie los fragmentos cuando no sean necesarios. Si una tarea de carga de archivos falla, vuelva a cargar el archivo.

AVISO

Los fragmentos generados ocupan espacio de almacenamiento que es facturable.

Limitaciones y restricciones

Actualmente, OBS Console no admite la eliminación de todos los fragmentos por un lote. Puede usar OBS Browser+ para eliminar todos los fragmentos a la vez. Para obtener más información, consulte **Gestión de fragmentos**.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Haga clic en **Fragments**, seleccione el fragmento que desea eliminar y, a continuación, haga clic en **Delete** a la derecha del fragmento.

También puede seleccionar varios fragmentos y hacer clic en **Delete** encima de la lista de fragmentos para eliminarlos por lotes.

Paso 4 Haga clic en **Yes** para confirmar la eliminación.

----Fin

7 Gestión de paquetes de recursos

Escenarios

Vea el uso del paquete de recursos en la página **Resource Packages** de OBS Console. En esta página, puede obtener rápidamente información sobre el estado, la capacidad restante, la hora de inicio/finalización, el ID de pedido y otra información de sus paquetes.

Información de referencia

OBS le ofrece enfoques de pago por uso y anuales/mensuales para los paquetes de recursos de precios. Los paquetes anuales/mensuales le proporcionan cierta cuota de recursos y duración, que es más favorable que el pago por uso.

Para obtener más información acerca de los tipos y funciones de paquetes de recursos de OBS, consulte **Descripción del paquete de recursos**.

Requisitos previos

Ha comprado al menos un paquete de recursos. Para obtener más información, consulte **Compra de paquetes de recursos**.

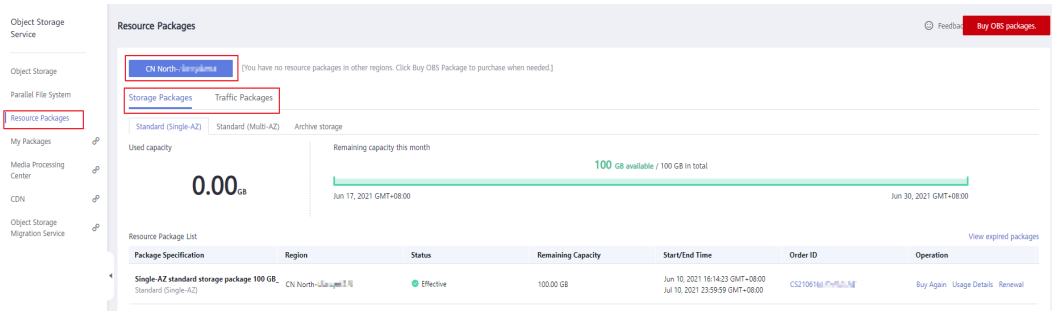
Consulta de detalles del paquete de recursos

Paso 1 En el panel de navegación de OBS Console, seleccione **Resource Packages**.

Paso 2 Seleccione la región y el tipo de su paquete para ver sus detalles.

La información detallada incluye la especificación del paquete, región, estado, capacidad restante, hora de inicio/final, ID de pedido y detalles de uso.

Figura 7-1 Consulta de los detalles del paquete de recursos



----Fin

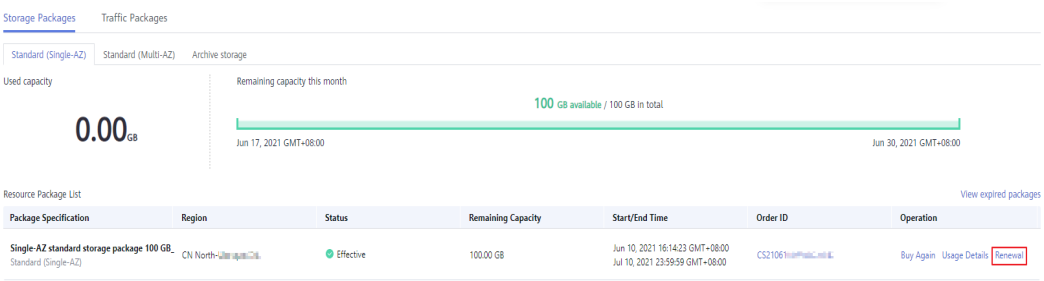
Renovación de un paquete de recursos

Paso 1 En el panel de navegación de OBS Console, seleccione **Resource Packages**.

Paso 2 Seleccione la región y el tipo del paquete de recursos que desea renovar.

Paso 3 En la fila que contiene el paquete de destino, haga clic en **Renewal** en la columna **Operation**.

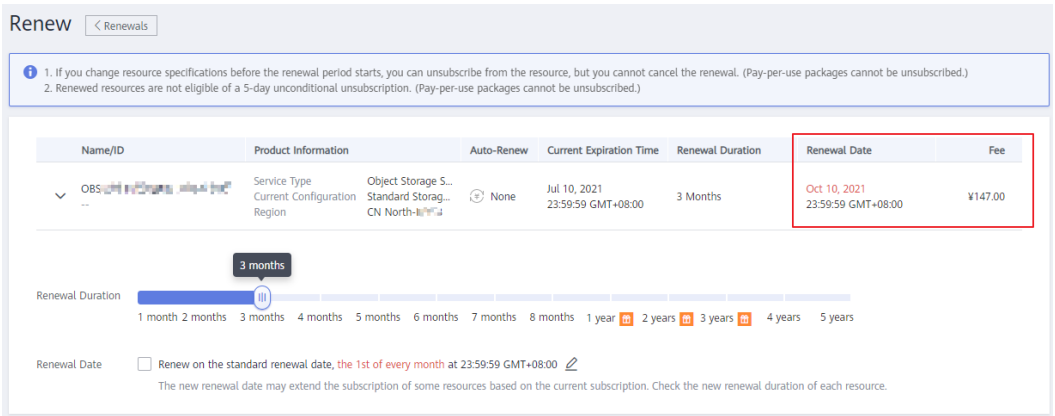
Figura 7-2 Renovación de un paquete de recursos



Paso 4 Seleccione una duración de renovación.

Se muestra la hora en que el paquete de recursos caducará y la tarifa de renovación correspondiente.

Figura 7-3 Selección de una duración de renovación



Paso 5 (Opcional) Establezca la fecha de renovación en el primer día de cada mes según sea necesario.

Seleccione **Renew on the standard renewal date** puede resultar en días de renovación adicionales e incurrir en cargos adicionales en consecuencia. Una vez que seleccione esta opción, asegúrese de tener claro la duración de la renovación y la tarifa.

Paso 6 Compruebe que todas las configuraciones son correctas y haga clic en **Pay Now** y, a continuación, complete el pago.

----Fin

8 Configuración de encriptación del lado del servidor

8.1 Server-Side Encryption Overview

After server-side encryption is enabled, objects to be uploaded will be encrypted and stored on the server. When objects are downloaded, they will be decrypted on the server first and then returned in plaintext to you.

Key Management Service (KMS) uses Hardware Secure Modules (HSMs) to ensure key security, enabling users to easily create and manage encryption keys. Keys are not displayed in plaintext outside HSMs, which prevents key disclosure. All operations performed on keys are controlled and logged, and usage of all keys is recorded, meeting regulatory compliance requirements.

The objects to be uploaded can be encrypted from the server side using the encryption service provided by KMS. You need to create a key using KMS or use the default key provided by KMS. Then you can use the key to perform server-side encryption when uploading objects to OBS.

OBS supports both SSE-KMS and server-side encryption with customer-provided keys (SSE-C) by calling APIs. In SSE-C mode, OBS encrypts objects on the server side using the keys and MD5 values provided by customers. Both methods use the AES-256 encryption algorithm.

8.2 Configuración de encriptación predeterminada del bucket

OBS le permite configurar la encriptación predeterminada para un bucket. Después de la configuración, los objetos cargados en este bucket se cifran automáticamente con la clave especificada, lo que hace que el almacenamiento de datos sea más seguro.

Puede elegir SSE-KMS o SSE-OBS para la encriptación al crear un bucket (consulte **Creación de un bucket**). También puede habilitar o deshabilitar la encriptación para un bucket una vez creado.

OBS cifra solo los objetos cargados después de que el cifrado predeterminado esté habilitado, y no cifra los cargados anteriormente. Después de deshabilitar la encriptación predeterminada, el estado de encriptación de los objetos existentes se mantiene sin cambios y aún puede cifrar objetos manualmente al cargarlos.

Habilitación de la encriptación predeterminada para un bucket

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

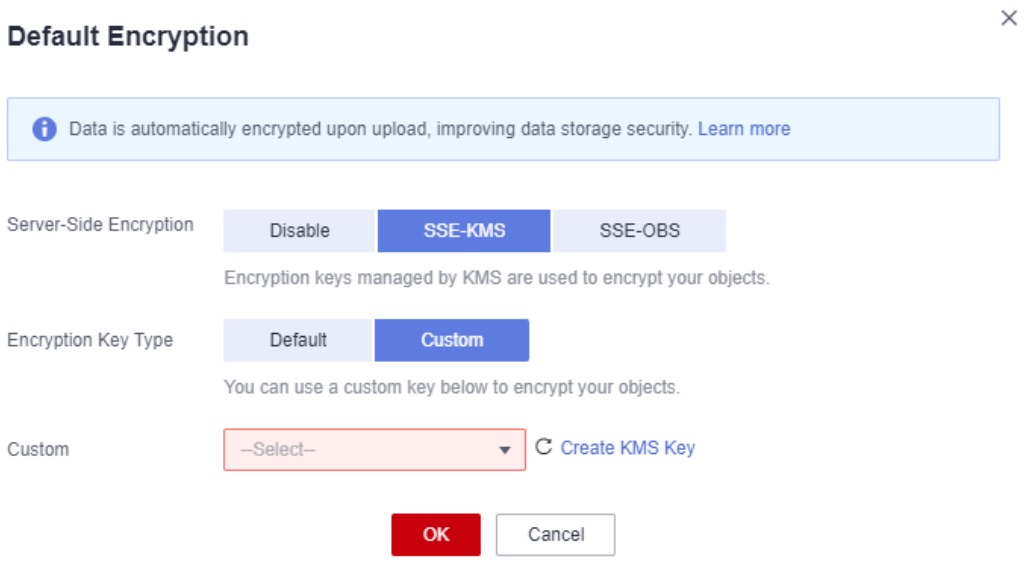
Paso 3 En el panel de navegación, elija **Overview**.

Paso 4 En el área **Basic Configurations**, haga clic en **Default Encryption**. Aparece el cuadro de diálogo **Default Encryption**.

Paso 5 Elija **SSE-KMS** o **SSE-OBS**.

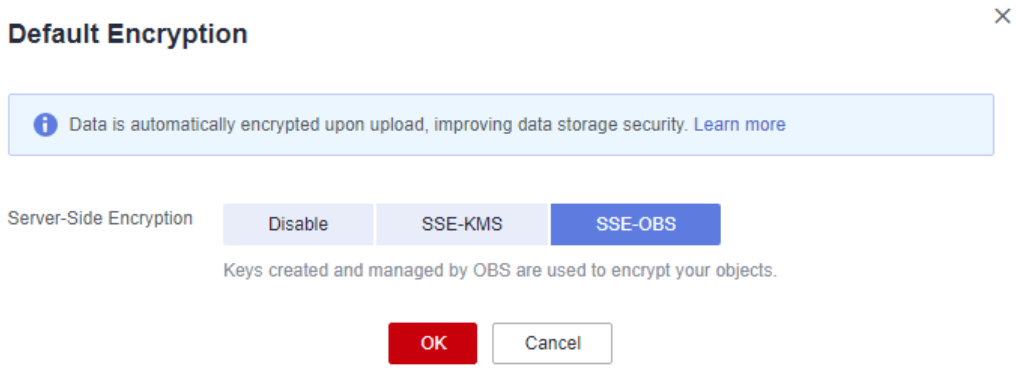
Si elige **SSE-KMS** para la encriptación, debe especificar un tipo de clave de encriptación. Para el tipo de clave de encriptación, puede elegir **Default** o **Custom**. Si se utiliza **Default**, se utilizará la clave predeterminada de la región actual para cifrar los objetos. Si no existe una clave predeterminada, OBS crea una la primera vez que carga un objeto. Si se utiliza **Custom**, puede elegir una clave personalizada que haya creado en la consola de KMS para cifrar los objetos.

Figura 8-1 Elegir SSE-KMS para un bucket



Cuando se elige **SSE-OBS**, las claves creadas y gestionadas por OBS se utilizan para la encriptación.

Figura 8-2 Elegir SSE-OBS para un bucket



Paso 6 Haga clic en **OK**.

----Fin

Desactivación de la encriptación predeterminada para un bucket

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

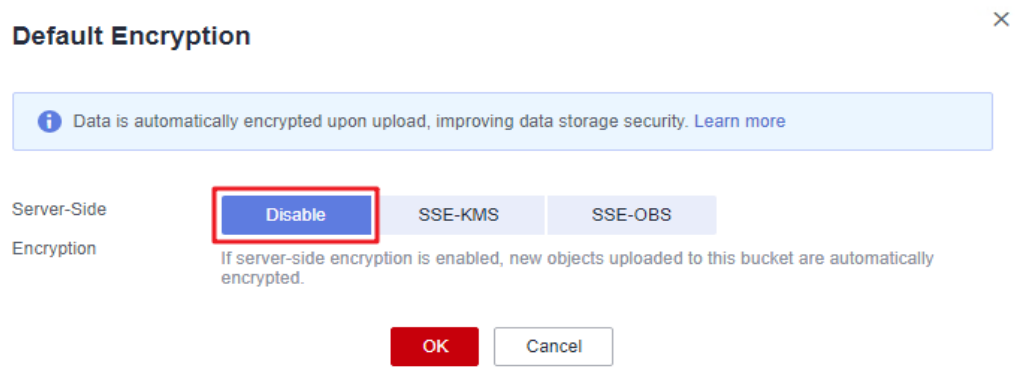
Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Overview**.

Paso 4 En el área **Basic Configurations**, haga clic en **Default Encryption**. Aparece el cuadro de diálogo **Default Encryption**.

Paso 5 Seleccione **Disable**.

Figura 8-3 Deshabilitar la encriptación para un bucket



Paso 6 Haga clic en **OK**.

----Fin

8.3 Carga de un objeto en modo de encriptación del lado del servidor

OBS le permite cifrar objetos con encriptación del lado del servidor para que los objetos se puedan almacenar de forma segura en OBS.

En un bucket con encriptación del lado del servidor deshabilitado, los objetos cargados en él no se cifran de forma predeterminada. Puede configurar la encriptación del lado del servidor al cargar objetos. En un bucket con encriptación del lado del servidor habilitado, los objetos cargados heredan la configuración de encriptación del bucket. También puede configurar por separado la encriptación para los objetos.

Limitaciones y restricciones

- No se puede cambiar el estado de encriptación del objeto.
- No se puede eliminar una clave en uso. De lo contrario, el objeto cifrado con esta clave no se puede descargar.
- Si un objeto está cifrado en el lado del servidor y no tiene ninguna delegación de IAM, otras cuentas y usuarios no pueden acceder al objeto aunque puedan leer este objeto.

Requisitos previos

En la región donde se despliega OBS, se ha agregado el permiso **KMS Administrator** al grupo de usuarios. Para obtener más información acerca de cómo agregar el permiso, consulte **Asignar permisos a un usuario de IAM**. Si la cuenta actual o el usuario es el concesionario, también requiere el permiso **KMS Administrator**.

Para obtener más información sobre los precios de DEW, consulte **Detalles de precios del producto**.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Haga clic en **Upload Object**. Aparece el cuadro de diálogo **Upload Object**.

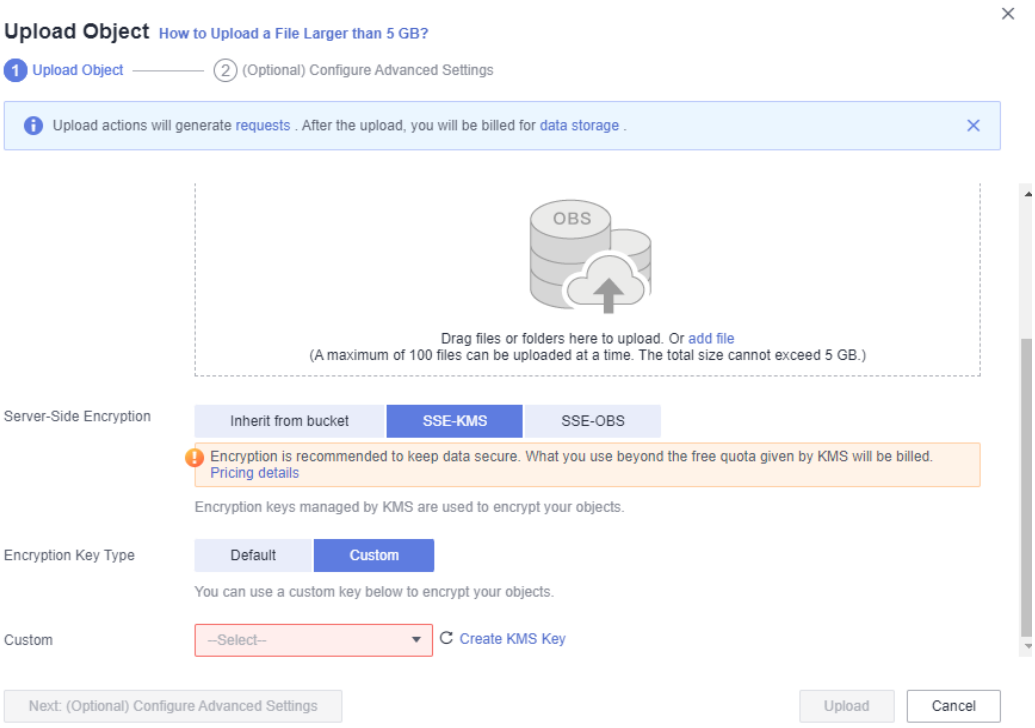
Paso 4 Agregue los archivos que se van a cargar.

Paso 5 Seleccione **SSE-KMS** o **SSE-OBS**.

Si elige **SSE-KMS** para la encriptación, debe especificar un tipo de clave de encriptación. Para el tipo de clave de encriptación, puede elegir **Default** o **Custom**. Si se utiliza **Default**, se utilizará la clave predeterminada de la región actual para cifrar los objetos. Si no existe una clave predeterminada, OBS crea una la primera vez que carga un objeto. Si se utiliza **Custom**, puede elegir una clave personalizada que haya creado en la consola de KMS para cifrar los objetos.

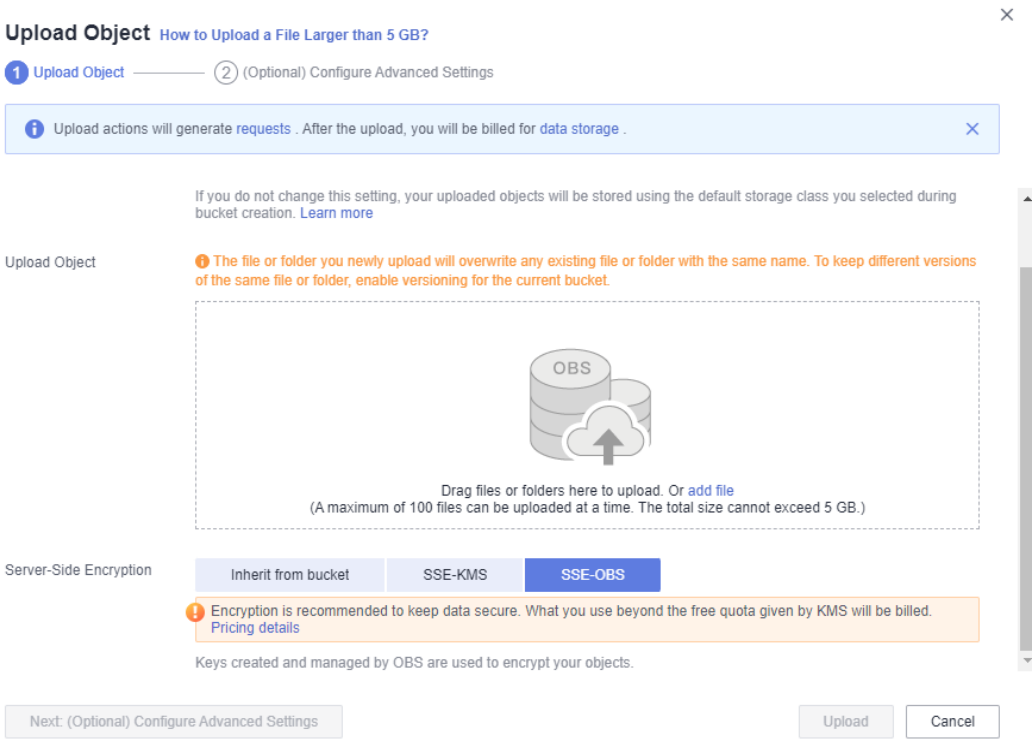
Para obtener más información sobre cómo crear una clave principal de cliente, consulte **Creación de una clave**.

Figura 8-4 Elección de **SSE-KMS** para la encriptación del lado del servidor



Cuando se elige **SSE-OBS**, las claves creadas y gestionadas por OBS se utilizan para la encriptación.

Figura 8-5 Elección de **SSE-OBS** para la encriptación del lado del servidor



Paso 6 Haga clic en **Upload**.

Después de cargar el objeto correctamente, puede ver su estado de cifrado en la lista de objetos.

----Fin

9 WORM

9.1 Descripción de WORM

OBS proporciona write-once-read-many (WORM) para proteger los objetos de ser eliminados o manipulados dentro de un período especificado. WORM funciona tanto a nivel de bucket como de objeto en modo de cumplimiento.

Escenarios

En el modo de cumplimiento, nadie puede sobrescribir o eliminar una versión de objeto protegida por WORM, incluido el usuario root de su cuenta.

Cuando WORM está configurado para un bucket, la protección se aplica a todos los objetos del bucket. Cuando se configura WORM para una versión de objeto, la protección solo se aplica a la versión de objeto actual. No importa qué tipo de protección WORM desee usar, primero debe habilitar WORM para el bucket. Una política de retención de WORM solo tiene efecto para los objetos cargados después de que la política surta efecto. Si un objeto está protegido por una política de WORM de nivel de bucket y una política de WORM de nivel de objeto al mismo tiempo, la política de WORM de nivel de objeto tiene prioridad.

Precauciones

- Cuando habilita WORM para un bucket, OBS activa automáticamente el control de versiones y el control de versiones no se puede suspender más tarde para ese bucket. WORM protege los objetos basándose en los ID de versión del objeto. Solo se pueden proteger las versiones de objetos con cualquier política de retención de WORM configurada. Supongamos que el objeto **test.txt 001** está protegido por WORM. Si se carga otro archivo con el mismo nombre, se generará una nueva versión de objeto **test.txt 002** sin política de WORM configurada. En tal caso, **test.txt 002** no están protegidas y se pueden eliminar. Cuando descargue un objeto sin especificar un ID de versión, se descargará la versión actual del objeto (**test.txt 002**).
- Una regla de ciclo de vida no puede eliminar objetos protegidos por WORM, pero puede realizar la transición de su clase de almacenamiento. Una vez que un objeto ya no está protegido, se eliminará cuando cumpla la regla de caducidad en una configuración de ciclo de vida.

- Una vez que habilita WORM para un bucket, no puede deshabilitarlo ni suspender el control de versiones para el bucket, pero puede deshabilitar la política predeterminada de WORM para el bucket.
- Los buckets con WORM habilitado no admiten la replicación entre regiones.
- Si ha dado de baja su cuenta o su cuenta ha sido congelada, los objetos protegidos por WORM se eliminarán permanentemente.
- La protección basada en WORM no está disponible para la migración.
- Los metadatos de un objeto protegido con WORM todavía se pueden modificar.

Cómo usarlo

Puede realizar operaciones relacionadas con WORM con OBS Console y la API OBS.

Herramienta	Referencia
OBS Console	**Creación de un bucket** **Carga de un objeto** **Configuración de la retención de WORM**
API	**Creación de un bucket** **Configuración de una política de WORM predeterminada para un bucket** **Obtención de la política de WORM predeterminada de un bucket** **Configuración de la retención de WORM para un objeto** Obtenga la configuración de retención de WORM a nivel de objeto según **Consulta de metadatos de objeto**.

9.2 Configuración de la retención de WORM

Puede configurar las políticas de retención de WORM al crear un bucket (consulte **Creación de un bucket**) o después de crear un bucket. A continuación se describe cómo configurar la retención de WORM después de crear un bucket con WORM habilitado.

Requisitos previos

Ha habilitado WORM para el bucket cuando lo crea.

Configuración de WORM para un bucket

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Overview**.

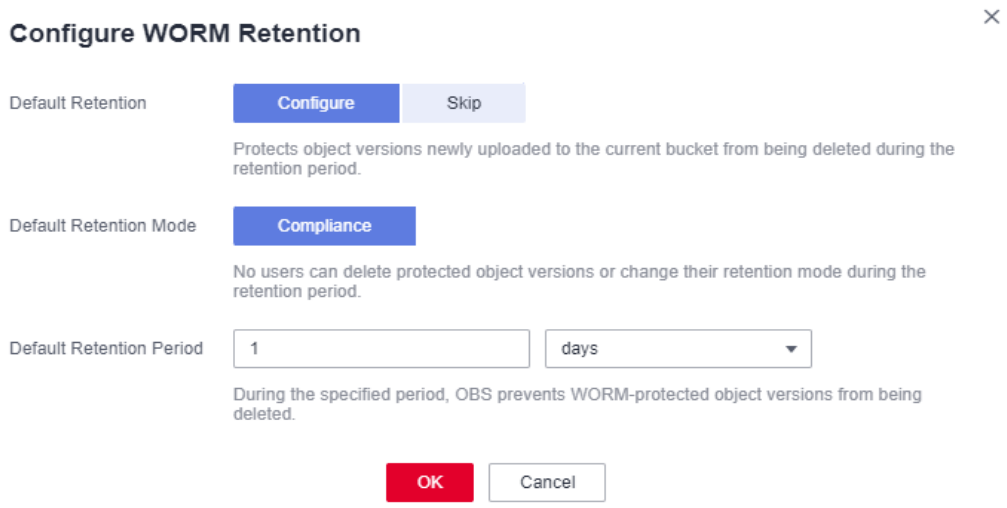
Paso 4 En el área **Basic Configurations**, haga clic en **WORM Retention**. Aparece el cuadro de diálogo **Configure WORM Retention**.

Paso 5 Elija **Configure** y especifique un período de retención predeterminado. El modo de retención predeterminado es **Compliance**.

NOTA

- Actualmente solo se admite el modo de retención de conformidad. En este modo, ningún usuario puede eliminar versiones de objetos protegidos o cambiar su modo de retención durante el período de retención especificado.
- Durante el período de retención predeterminado especificado, OBS impide que se eliminen las versiones de objetos protegidas por WORM. Puede configurar un período de retención en días (de **1** a **36500**) o años (de **1** a **100**). El límite máximo es de 100 años.
- Al cargar un objeto en un bucket protegido por WORM, puede configurar el objeto para que herede la retención de WORM del bucket en la configuración avanzada. Si se aplica a un objeto una política de retención de WORM a nivel de bucket y a nivel de objeto, se utilizará la política de retención a nivel de objeto.

Figura 9-1 Configuración de una política de retención de WORM



Paso 6 Haga clic en **OK**.

----Fin

Omitir la configuración de retención de WORM

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

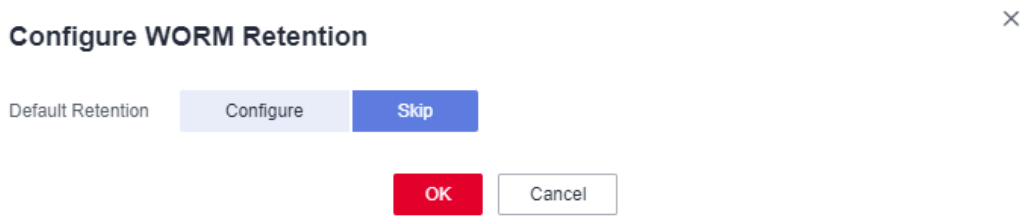
Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Overview**.

Paso 4 En el área **Basic Configurations**, haga clic en **WORM Retention**. Aparece el cuadro de diálogo **Configure WORM Retention**.

Paso 5 Elija **Skip**.

Figura 9-2 Omitir la configuración de retención de WORM



----Fin

Ampliación del período de retención

Después de configurar WORM para un objeto, puede ir a la página de detalles del objeto y ampliar el período de retención de una versión de objeto en la página **Versions**. Antes de la fecha especificada, OBS impide que se eliminen las versiones de objetos protegidos.

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

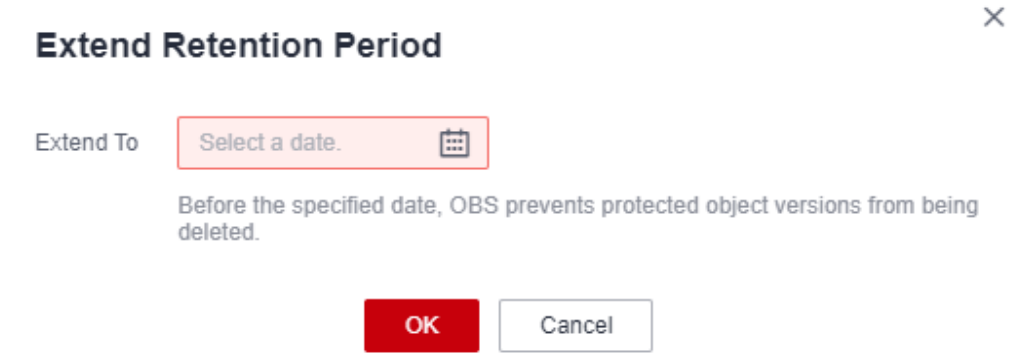
Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En la lista de objetos, haga clic en el objeto que desea ir a la página de detalles del objeto.

Paso 4 En la ficha **Versions**, vea todas las versiones del objeto.

Paso 5 Busque la versión de objeto para la que desea ampliar el período de retención, elija **More** > **Extend Retention Period** y seleccione una fecha.

Figura 9-3 Ampliación del período de retención



NOTA

Un período de retención solo se puede ampliar, pero no se puede acortar.

Supongamos que una versión de objeto se configuró para protegerse hasta el 30 de marzo de 2023. Si desea ampliar el período de retención el 1 de marzo de 2023, puede ampliarlo hasta el 31 de marzo de 2023 o una fecha posterior. Si extiende el período de retención el 1 de abril de 2023, puede extenderlo hasta el día actual (1 de abril de 2023) o una fecha posterior. Si se utiliza el día actual, la versión del objeto dejará de estar protegida por WORM después de las 24:00 de ese día.

----Fin

Operaciones relacionadas

Al cargar un objeto, configure una política de retención para el objeto. Para obtener más información, véase **Carga de un objeto**.

10 Metadatos de objeto

10.1 Object Metadata Overview

Object metadata is a set of name-value pairs that are part of object management.

Currently, only the metadata defined by the system is supported.

The metadata defined by the system is classified into the following types: system-controlled and user-controlled. For example, metadata such as **Last-Modified** is controlled by the system and cannot be modified. You can call the API to modify the metadata such as **ContentLanguage**. The metadata that can be modified is described as follows:

Tabla 10-1 OBS metadata

Name	Description
ContentDisposition	Provides a default file name for the object that is being requested. When an object is being downloaded or accessed, the file with the default file name is directly displayed in the browser or a download dialog box is displayed if the file is being accessed. For example, select **ContentDisposition** as the metadata name and enter **attachment;filename="testfile.xls"** as the metadata value for an object. If you access the object through a link, a dialog box is directly displayed for downloading objects, and the object name is changed to **testfile.xls**. For details, see the definition about ContentDisposition in HTTP.
ContentLanguage	Indicates the language or languages intended for the audience. Therefore, a user can differentiate according to the user's preferred language. For details, see the definition about ContentLanguage in HTTP.

Name	Description
WebsiteRedirectLocation	Redirects an object to another object or an external URL. The redirection function is implemented using static website hosting. For example, you can perform the following operations to implement object redirection: 1. Set metadata of object **testobject.html** in the root directory of bucket **testbucket**. Select **WebsiteRedirectLocation** for **Name** and enter **http://www.example.com** for **Value**. **NOTA** OBS only supports redirection for objects in the root directory of a bucket. Redirection for objects located in folders of a bucket is not supported. 2. Configure static website hosting for bucket **testbucket**, and set the object **testobject.html** in the bucket as the default home page of the hosted static website. 3. If you access object **testobject.html** through the URL link provided on the **Configure Static Website Hosting** page, the access request is redirected to **http://www.example.com**.
ContentEncoding	Content encoding format when an object is downloaded. The options are as follows: ● Standard: **compress**, **deflate**, **exi**, **identity**, **gzip**, and **pack200-gzip** ● Others: **br**, **bzip2**, **lzma**, **peerdist**, **sdch**, **xpress**, **xz**
CacheControl	Cache behavior of the web page when the specified object is downloaded. ● Cacheability: **public**, **private**, **no-cache**, and **only-if-cached** ● Expiration time: **max-age=<*seconds*>**, **s-maxage=<*seconds*>**, **max-stale[=<*seconds*>]**, **min-fresh=<*seconds*>**, **stale-while-revalidate=<*seconds*>**, **stale-if-error=<*seconds*>** ● Re-verification and reloading: **must-revalidate**, **proxy-revalidate**, **immutable** ● Others: **no-store**, **no-transform**
Expires	Cache expiration time (GMT)
ContentType	File type of an object. For details, see **About Object Metadata Content-Type**.

NOTA

- When versioning is enabled for a bucket, you can set metadata for objects which are **Latest Version**, but cannot set metadata for objects which are **Historical Version**.

10.2 About Object Metadata Content-Type

When an object is uploaded to OBS, the system automatically matches the value of **Content-Type** based on the file name extension of the object. When you access an object through a web browser, the system specifies an application to open the object according to the value of **Content-Type**. You can modify the **Content-Type** of an object based on its file name extension.

Tabla 10-2 Common Content-Type values

File Name Extension	Content-Type	File Name Extension	Content-Type
* (binary stream, which does not know the type of the file to be downloaded)	application/octet-stream	.tif	image/tiff
.001	application/x-001	.301	application/x-301
.323	text/h323	.906	application/x-906
.907	drawing/907	.a11	application/x-a11
.acp	audio/x-mei-aac	.ai	application/postscript
.aif	audio/aiff	.aifc	audio/aiff
.aiff	audio/aiff	.anv	application/x-anv
.asa	text/asa	.asf	video/x-ms-asf
.asp	text/asp	.asx	video/x-ms-asf
.au	audio/basic	.avi	video/avi
.awf	application/vnd.adobe.workflow	.biz	text/xml
.bmp	application/x-bmp	.bot	application/x-bot
.c4t	application/x-c4t	.c90	application/x-c90
.cal	application/x-cals	.cat	application/vnd.ms-pki.seccat
.cdf	application/x-netcdf	.cdr	application/x-cdr
.cel	application/x-cel	.cer	application/x-x509-ca-cert
.cg4	application/x-g4	.cgm	application/x-cgm
.cit	application/x-cit	.class	java/*

File Name Extension	Content-Type	File Name Extension	Content-Type
.cml	text/xml	.cmp	application/x-cmp
.cmx	application/x-cmx	.cot	application/x-cot
.crl	application/pkix-crl	.crt	application/x-x509-ca-cert
.csi	application/x-csi	.css	text/css
.cut	application/x-cut	.dbf	application/x-dbf
.dbm	application/x-dbm	.dbx	application/x-dbx
.dcd	text/xml	.dcx	application/x-dcx
.der	application/x-x509-ca-cert	.dgn	application/x-dgn
.dib	application/x-dib	.dll	application/x-msdownload
.doc	application/msword	.dot	application/msword
.drw	application/x-drw	.dtd	text/xml
.dwf	Model/vnd.dwf	.dwf	application/x-dwf
.dwg	application/x-dwg	.dxb	application/x-dxb
.dxf	application/x-dxf	.edn	application/vnd.adobe.edn
.emf	application/x-emf	.eml	message/rfc822
.ent	text/xml	.epi	application/x-epi
.eps	application/x-ps	.eps	application/postscript
.etd	application/x-ebx	.exe	application/x-msdownload
.fax	image/fax	.fdf	application/vnd.fdf
.fif	application/fractals	.fo	text/xml
.frm	application/x-frm	.g4	application/x-g4
.gbr	application/x-gbr	.	application/x-
.gif	image/gif	.gl2	application/x-gl2
.gp4	application/x-gp4	.hgl	application/x-hgl
.hmr	application/x-hmr	.hpg	application/x-hpgl

File Name Extension	Content-Type	File Name Extension	Content-Type
.hpl	application/x-hpl	.hqx	application/mac-binhex40
.hrf	application/x-hrf	.hta	application/hta
.htc	text/x-component	.htm	text/html
.html	text/html	.htt	text/webviewhtml
.htx	text/html	.icb	application/x-icb
.ico	image/x-icon	.ico	application/x-ico
.iff	application/x-iff	.ig4	application/x-g4
.igs	application/x-igs	.iii	application/x-iphone
.img	application/x-img	.ins	application/x-internet-signup
.isp	application/x-internet-signup	.IVF	video/x-ivf
.java	java/*	.jfif	image/jpeg
.jpe	image/jpeg	.jpe	application/x-jpe
.jpeg	image/jpeg	.jpg	image/jpeg
.jpg	application/x-jpg	.js	application/x-javascript
.jsp	text/html	.la1	audio/x-liquid-file
.lar	application/x-laplayer-reg	.latex	application/x-latex
.lavs	audio/x-liquid-secure	.lbm	application/x-lbm
.lmsff	audio/x-la-lms	.ls	application/x-javascript
.ltr	application/x-ltr	.m1v	video/x-mpeg
.m2v	video/x-mpeg	.m3u	audio/mpegurl
.m4e	video/mpeg4	.mac	application/x-mac
.man	application/x-troff-man	.math	text/xml
.mdb	application/msaccess	.mdb	application/x-mdb

File Name Extension	Content-Type	File Name Extension	Content-Type
.mfp	application/x-shockwave-flash	.mht	message/rfc822
.mhtml	message/rfc822	.mi	application/x-mi
.mid	audio/mid	.midi	audio/mid
.mil	application/x-mil	.mml	text/xml
.mnd	audio/x-musicnet-download	.mns	audio/x-musicnet-stream
.mocha	application/x-javascript	.movie	video/x-sgi-movie
.mp1	audio/mp1	.mp2	audio/mp2
.mp2v	video/mpeg	.mp3	audio/mp3
.mp4	video/mp4	.mpa	video/x-mpg
.mpd	application/vnd.ms-project	.mpe	video/x-mpeg
.mpeg	video/mpg	.mpg	video/mpg
.mpga	audio/rn-mpeg	.mpp	application/vnd.ms-project
.mps	video/x-mpeg	.mpt	application/vnd.ms-project
.mpv	video/mpg	.mpv2	video/mpeg
.mpw	application/vnd.ms-project	.mpx	application/vnd.ms-project
.mtx	text/xml	.mxp	application/x-mmxp
.net	image/pnetvue	.nrf	application/x-nrf
.nws	message/rfc822	.odc	text/x-ms-odc
.out	application/x-out	.p10	application/pkcs10
.p12	application/x-pkcs12	.p7b	application/x-pkcs7-certificates
.p7c	application/pkcs7-mime	.p7m	application/pkcs7-mime
.p7r	application/x-pkcs7-certreqresp	.p7s	application/pkcs7-signature
.pc5	application/x-pc5	.pci	application/x-pci

File Name Extension	Content-Type	File Name Extension	Content-Type
.pcl	application/x-pcl	.pcx	application/x-pcx
.pdf	application/pdf	.pdf	application/pdf
.pdx	application/vnd.adobe.pdx	.pfx	application/x-pkcs12
.pgl	application/x-pgl	.pic	application/x-pic
.pko	application/vnd.ms-pki.pko	.pl	application/x-perl
.plg	text/html	.pls	audio/scpls
.plt	application/x-plt	.png	image/png
.png	application/x-png	.pot	application/vnd.ms-powerpoint
.ppa	application/vnd.ms-powerpoint	.ppm	application/x-ppm
.pps	application/vnd.ms-powerpoint	.ppt	application/vnd.ms-powerpoint
.ppt	application/x-ppt	.pr	application/x-pr
.prf	application/pics-rules	.prn	application/x-prn
.prt	application/x-prt	.ps	application/x-ps
.ps	application/postscript	.ptn	application/x-ptn
.pwz	application/vnd.ms-powerpoint	.r3t	text/vnd.rn-realtext3d
.ra	audio/vnd.rn-realaudio	.ram	audio/x-pn-realaudio
.ras	application/x-ras	.rat	application/rat-file
.rdf	text/xml	.rec	application/vnd.rn-recording
.red	application/x-red	.rgb	application/x-rgb
.rjs	application/vnd.rn-realsystem-rjs	.rjt	application/vnd.rn-realsystem-rjt
.rlc	application/x-rlc	.rle	application/x-rle
.rm	application/vnd.rn-realmedia	.rmf	application/vnd.adobe.rmf

File Name Extension	Content-Type	File Name Extension	Content-Type
.rmi	audio/mid	.rmj	application/vnd.rn-realsystem-rmj
.rmm	audio/x-pn-realaudio	.rmp	application/vnd.rn-rn_music_package
.rms	application/vnd.rn-realmedia-secure	.rmvb	application/vnd.rn-realmedia-vbr
.rmx	application/vnd.rn-realsystem-rmx	.rnx	application/vnd.rn-realplayer
.rp	image/vnd.rn-realpix	.rpm	audio/x-pn-realaudio-plugin
.rsml	application/vnd.rn-rsml	.rt	text/vnd.rn-realtext
.rtf	application/msword	.rtf	application/x-rtf
.rv	video/vnd.rn-realvideo	.sam	application/x-sam
.sat	application/x-sat	.sdp	application/sdp
.sdw	application/x-sdw	.sit	application/x-stuffit
.slb	application/x-slb	.sld	application/x-sld
.slk	drawing/x-slk	.smi	application/smil
.smil	application/smil	.smk	application/x-smk
.snd	audio/basic	.sol	text/plain
.sor	text/plain	.spc	application/x-pkcs7-certificates
.spl	application/futuresplash	.spp	text/xml
.ssm	application/streamingmedia	.sst	application/vnd.ms-pki.certstore
.stl	application/vnd.ms-pki.stl	.stm	text/html
.sty	application/x-sty	.svg	text/xml
.swf	application/x-shockwave-flash	.tdf	application/x-tdf
.tg4	application/x-tg4	.tga	application/x-tga
.tif	image/tiff	.tif	application/x-tif

File Name Extension	Content-Type	File Name Extension	Content-Type
.tiff	image/tiff	.tld	text/xml
.top	drawing/x-top	.torrent	application/x-bittorrent
.tsd	text/xml	.txt	text/plain
.uin	application/x-icq	.uls	text/iuls
.vcf	text/x-vcard	.vda	application/x-vda
.vdx	application/vnd.visio	.vml	text/xml
.vpg	application/x-vpeg005	.vsd	application/vnd.visio
.vsd	application/x-vsd	.vss	application/vnd.visio
.vst	application/vnd.visio	.vst	application/x-vst
.vsw	application/vnd.visio	.vsx	application/vnd.visio
.vtx	application/vnd.visio	.vxml	text/xml
.wav	audio/wav	.wax	audio/x-ms-wax
.wb1	application/x-wb1	.wb2	application/x-wb2
.wb3	application/x-wb3	.wbmp	image/vnd.wap.wbmp
.wiz	application/msword	.wk3	application/x-wk3
.wk4	application/x-wk4	.wkq	application/x-wkq
.wks	application/x-wks	.wm	video/x-ms-wm
.wma	audio/x-ms-wma	.wmd	application/x-ms-wmd
.wmf	application/x-wmf	.wml	text/vnd.wap.wml
.wmv	video/x-ms-wmv	.wmx	video/x-ms-wmx
.wmz	application/x-ms-wmz	.wp6	application/x-wp6
.wpd	application/x-wpd	.wpg	application/x-wpg
.wpl	application/vnd.ms-wpl	.wq1	application/x-wq1
.wr1	application/x-wr1	.wri	application/x-wri
.wrk	application/x-wrk	.ws	application/x-ws
.ws2	application/x-ws	.wsc	text/scriptlet

File Name Extension	Content-Type	File Name Extension	Content-Type
.wsdl	text/xml	.wvx	video/x-ms-wvx
.xdp	application/vnd.adobe.xdp	.xdr	text/xml
.xfd	application/vnd.adobe.xfd	.xfdf	application/vnd.adobe.xfdf
.xhtml	text/html	.xls	application/vnd.ms-excel
.xls	application/x-xls	.xlw	application/x-xlw
.xml	text/xml	.xpl	audio/scpls
.xq	text/xml	.xql	text/xml
.xquery	text/xml	.xsd	text/xml
.xsl	text/xml	.xslt	text/xml
.xwd	application/x-xwd	.x_b	application/x-x_b
.sis	application/vnd.symbian.install	.sisx	application/vnd.symbian.install
.x_t	application/x-x_t	.ipa	application/vnd.iphone
.apk	application/vnd.android.package-archive	.xap	application/x-silverlight-app

10.3 Configuración de metadatos de objeto

Procedimiento

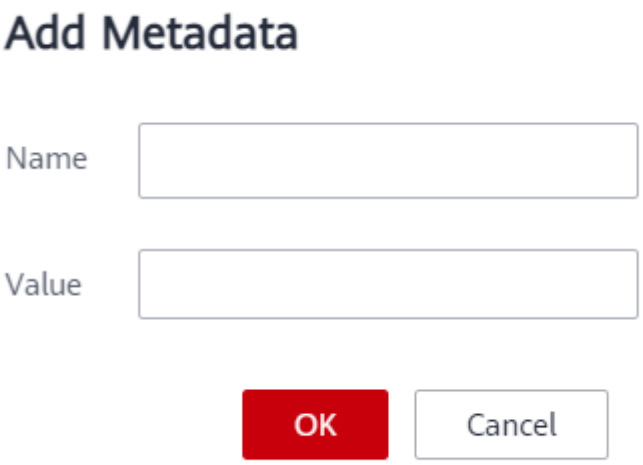
Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Haga clic en el objeto que desea operar y, a continuación, haga clic en la ficha **Metadata**.

Paso 4 Haga clic en **Add** y especifique la información de metadatos, tal y como se muestra en **Figura 10-1**.

Figura 10-1 Adición de metadatos



Paso 5 Haga clic en **OK**.

----Fin

11 Inventarios de bucket

11.1 Bucket Inventory Overview

The bucket inventory function periodically generate lists of metadata information of objects in a bucket. Inventories help you better understand object statuses in the bucket.

An inventory is a CSV file. Inventory files are automatically uploaded to the specified bucket.

You specify that inventories are generated for objects with the same object name prefix. You can also determine the inventory generation interval and whether to list all object versions in the inventory file. In addition, you can specify the object metadata to be included in the inventory, such as object size, modification time, storage class, encryption status, and replication status.

Limitations and Constraints

- A bucket can have a maximum of 10 inventory rules.
- The source bucket (for which a bucket inventory rule is configured) and the target bucket (where the generated inventory files are stored) must belong to the same account.
- The source bucket and the target bucket must be in the same region.
- Inventory files must be in the CSV format.
- OBS can generate inventory files for all objects in a bucket or a group of objects whose names begin with the same prefix.
- If a bucket has multiple inventory rules, overlaps between the inventory rules are not allowed.
  - If a bucket already has an inventory rule for the entire bucket, new inventory rules that filter objects by prefixes cannot be created. If you need an inventory rule that covers only a subset of objects in the bucket, delete the inventory rule configured for the entire bucket.
  - If an inventory rule that filters objects by a specified prefix already exists, you cannot create an inventory rule for the entire bucket. To create an inventory rule for the entire bucket, make sure that the bucket has no other inventory rules that filter objects by specified prefixes.
  - If a bucket already has an inventory rule that filters objects by the object name prefix **ab**, the filter of a new inventory rule cannot start with **a** or **ab**. Or, you can

delete the existing inventory rule and create a new one that filters objects according to your needs.

- Bucket inventory files can be encrypted only in the SSE-KMS mode.
- The bucket inventory function is offered for free, but inventory files are charged for the storage space they use.
- Default encryption cannot be enabled for the target bucket configured for storing inventory files.

11.2 Configuración de un inventario de bucket

Procedimiento

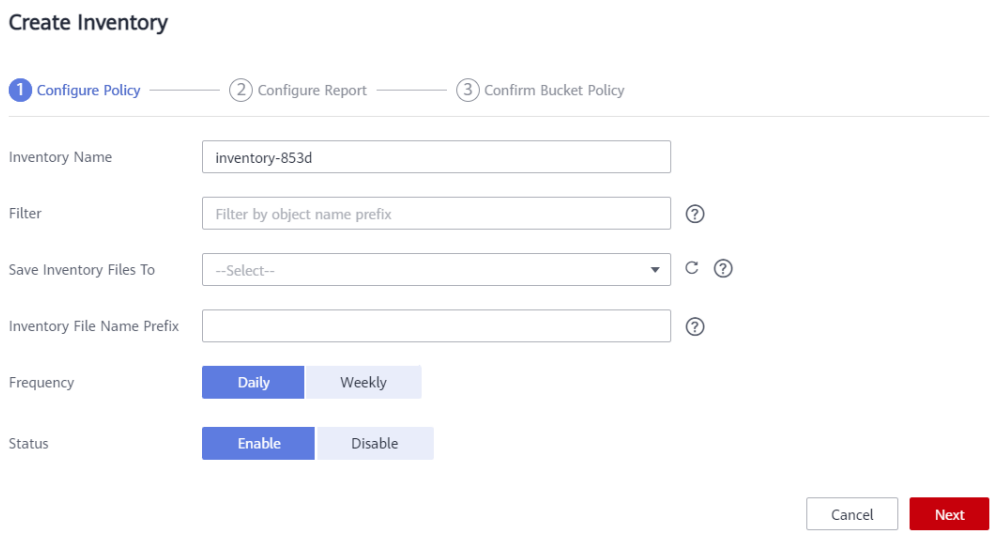
Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, haga clic en **Inventories**. Se muestra la lista de inventario.

Paso 4 Haga clic en **Create**. Aparece el cuadro de diálogo **Create Inventory**.

Figura 11-1 Configuración de inventario



Paso 5 Configure los parámetros necesarios.

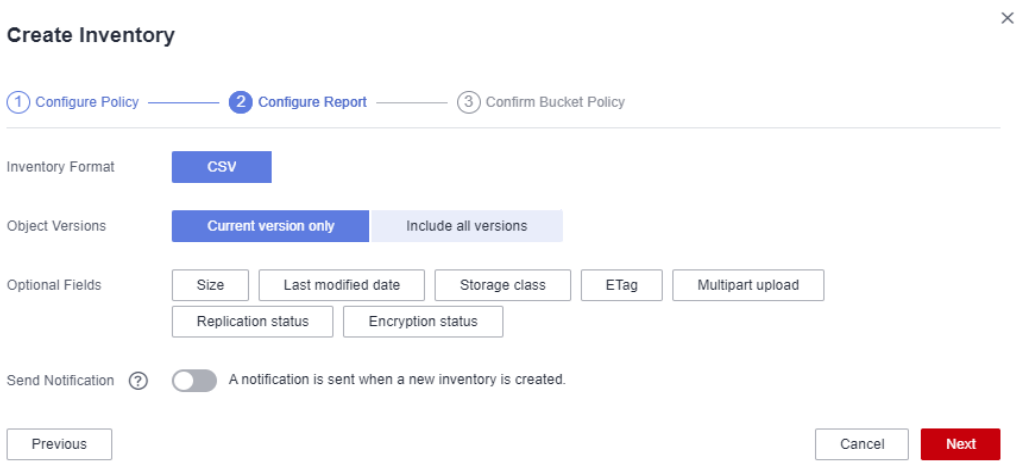
Tabla 11-1 Parámetros para configurar un inventario de bucket

Parámetro	Descripción
Inventory Name	Nombre de un inventario de bucket

Parámetro	Descripción
Filter	Condición de filtrado de un inventario. Puede introducir un prefijo de nombre de objeto, luego el inventario generado cubrirá los objetos cuyos nombres comiencen con el mismo prefijo. Un inventario solo puede filtrar objetos por un prefijo especificado. Si no se especifica el filtro, el inventario cubre todos los objetos del bucket. Si un bucket tiene varios inventarios, sus filtros no pueden solaparse entre sí.
Save Inventory Files To	Seleccione un bucket donde se almacenan los archivos de inventario generados. Este bucket y el bucket de origen deben estar en la misma región.
Inventory File Name Prefix	Prefijo de la ruta de almacenamiento de los archivos de inventario. Una vez que se genera un archivo de inventario, su ruta de guardado está en el siguiente formato: *Inventory file name prefix/Source bucket name/Inventory name/Date and time/files/* Si no se especifica este parámetro, el sistema agrega automáticamente el prefijo **BucketInventory** a un archivo de inventario.
Frequency	Con qué frecuencia se generan los archivos de inventario. Puede configurarse en **Daily** o **Weekly**.
Status	Estado del inventario configurado. Puede activarlo o desactivarlo para que la configuración sea efectiva o ineficaz.

Paso 6 Haga clic en **Next** para ir a la página **Configure Report**.

Figura 11-2 Configuración del informe



Paso 7 Configure el informe.

Tabla 11-2 Parámetros relacionados con el informe

Parámetro	Descripción
Inventory Format	Los archivos de inventario solo se pueden guardar en formato CSV.
Object Versions	Versiones de objetos que desea enumerar en un archivo de inventario. Puede configurarse en **Current version only** o **Include all versions**.
Optional Fields	Campos de información de objeto que pueden estar contenidos en un archivo de inventario, incluidos **Size**, **Last modified date**, **Storage class**, **ETag**, **Multipart upload**, **Encryption status**, y **Replication status**. Para obtener más información sobre los campos, consulte **Metadatos en un archivo de inventario**.

Paso 8 Haga clic en **Next** para confirmar la política de bucket.

Se crea una política de bucket en el bucket para que el bucket almacene archivos de inventario.

Paso 9 Haga clic en **OK**.

----Fin

12 Control de permisos

12.1 Overview

OBS supports the following permission control mechanisms:

- permisos de IAM: permisos de IAM define the actions that can be performed on your cloud resources. In other words, permisos de IAM specify what actions are allowed or denied.
- Bucket policies and object policies:

  A bucket policy applies to the configured bucket and objects in the bucket. A bucket owner can use a bucket policy to grant permissions of buckets and objects in the buckets to IAM users or other accounts.

  An object policy applies to specified objects in a bucket.
- Access control lists (ACLs): Control the read and write permissions for accounts. You can set ACLs for buckets and objects.

12.2 Mecanismos de control de permisos

12.2.1 IAM Permissions

You can create IAM users under a registered cloud service account, and then use IAM policies to control users' access permissions to cloud resources.

permisos de IAM define the actions that can be performed on your cloud resources. In other words, permisos de IAM specify what actions are allowed or denied.

permisos de IAM with OBS permissions take effect on all OBS buckets and objects. To grant an IAM user the permission to operate OBS resources, you need to assign one or more OBS permission sets to the user group to which the user belongs.

For details about OBS permissions controlled by IAM policies, see **Permissions Management**.

permisos de IAM Application Scenarios

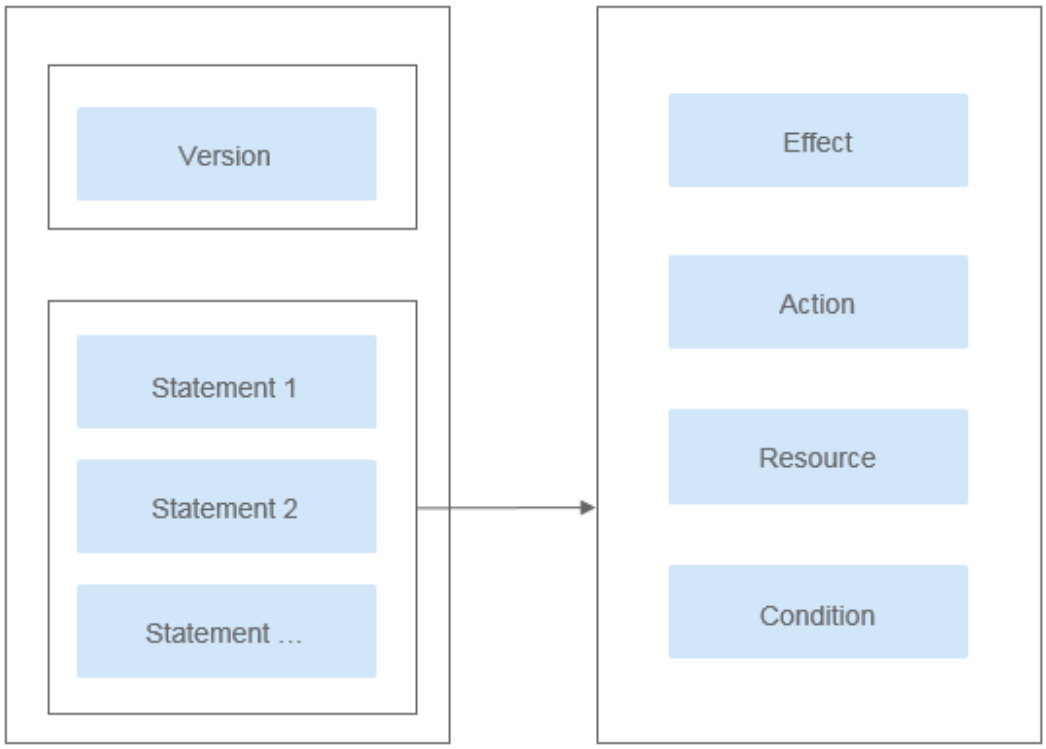
permisos de IAM are used to authorize IAM users under an account.

- Controlling permissions to cloud resources as a whole under an account
- Controlling permissions to all OBS buckets and objects under an account
- Controlling permissions to specified cloud resources under an account

Policy Structure and Syntax

A policy consists of a version and statements. Each policy can have multiple statements.

Figura 12-1 Policy structure



Policy syntax example:

```
{
    "Version": "1.1",
    "Statement": [
                {
            "Effect": "Allow",
            "Action": [
                "obs:bucket:HeadBucket",
                "obs:bucket:ListBucket",
                "obs:bucket:GetBucketLocation"
            ],
            "Resource": [
                "obs:*:*:bucket:*"
            ],
            "Condition": {
                "StringEndWithIfExsits": {
                    "g:UserName": ["specialCharacter"]
                },
                "Bool": {
                    "g:MFAPresent": ["true"]
```



```
                    }
                }
            }
        ]
}
```

Tabla 12-1 Policy syntax parameters

Parameter	Description
Version	The version number of a policy. ● **1.0**: RBAC policies. An RBAC policy consists of permissions for an entire service. Users in a group with such a policy assigned are granted all of the permissions required for that service. ● **1.1**: Fine-grained policies. A fine-grained policy consists of API-based permissions for operations on specific resource types. Fine-grained policies, as the name suggests, allow for more fine-grained control on specific operations and resources than RBAC policies. For example: You can restrict an IAM user to access only the objects in a specific directory of an OBS bucket.

Parameter	Description
Statement	Permissions defined by a policy, including **Effect**, **Action**, **Resource**, and **Condition**. **Condition** is optional. ● **Effect** The valid values for **Effect** are **Allow** and **Deny**. System policies contain only **Allow** statements. For custom policies containing both **Allow** and **Deny** statements, the **Deny** statements take precedence. ● **Action** Permissions of specific operations on resources in the format of *Service name*:*Resource type*:*Operation*. A policy can contain one or more permissions. The wildcard (*) is allowed to indicate all of the services, resource types, or operations depending on its location in the action. OBS has two resource types: bucket and object. For details about actions, see **Bucket-Related Actions** and **Object-Related Actions**. ● **Resource** Resources on which the policy takes effect in the format of *Service name*:*Region*:*Domain ID*:*Resource type*:*Resource path*. The wildcard (*) is allowed to indicate all of the services, regions, resource types, or resource paths depending on its location in the action. In the JSON view, if **Resource** is not specified, the policy takes effect for all resources. The value of **Resource** supports uppercase (A to Z), lowercase (a to z) letters, digits (0 to 9), and the following characters: -_*./\. If the value contains invalid characters, use the wildcard character (*). OBS is a global service. Therefore, set *Region* to *. *Domain ID* indicates the ID of the resource owner. Set it to * to indicate the ID of the account to whom the resources belong to. Examples: – **obs:*:*:bucket:***: all OBS buckets

Parameter	Description
	– **obs:*:*:object:my-bucket/my-object/***: all objects in the **my-object** directory of the **my-bucket** bucket ● **Condition** Conditions for the policy to take effect (Optional). Format: *Condition operator*: *{Condition key:[Value 1, Value 2]}* The condition includes the global service condition name and cloud service condition name. The condition names supported by OBS are the same as those in the bucket policy. When configuring in IAM, add **obs:**. For details, see **Conditions**. The value of **Condition** can contain only uppercase (A to Z), lowercase (a to z) letters, digits (0 to 9), and the following characters: -,./_@#$%&. If the value contains unsupported characters, consider using the condition operator for fuzzy match, such as StringLike and StringStartWith. Examples: – **StringEndWithIfExists": {"g:UserName": ["specialCharacter"]}**: The statement is valid for users whose names end with **specialCharacter**. – **"StringLike":{"obs:prefix": ["private/"]}**: When listing objects in a bucket, you need to set prefix to **private/** or include **private/**.

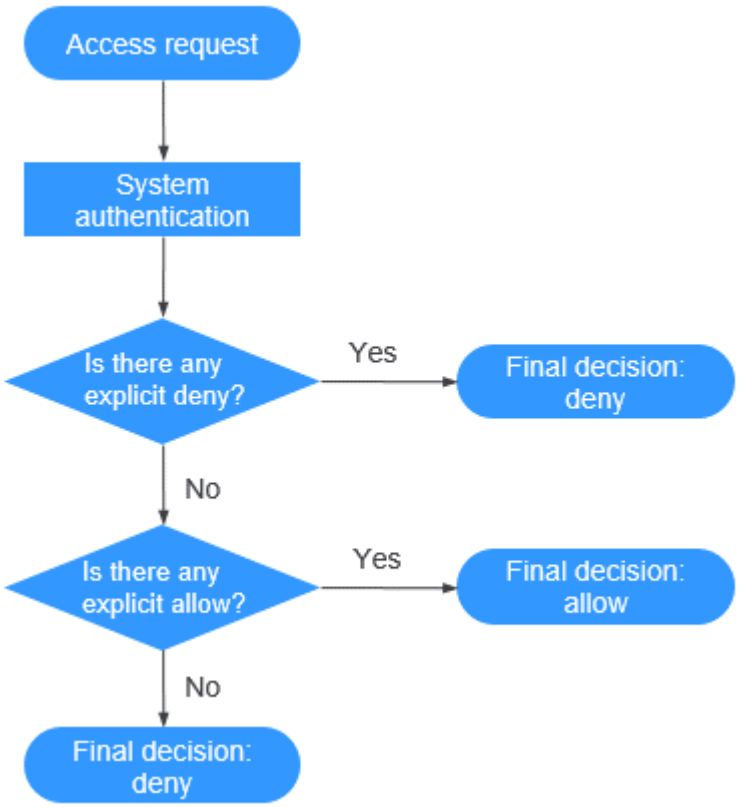
NOTA

- Fine-grained permission control at the **Resource** level will be deployed in regions one after another. Before using this feature, ensure that the region where your bucket resides supports the feature.
- To use the fine-grained permission control at the **Resource** level, **submit a service ticket** to OBS.

Authentication of permisos de IAM

The authentication of permisos de IAM starts from the Deny statements. The following figure shows the authentication logic for resource access.

Figura 12-2 Authentication logic



NOTA

The actions in each policy are in the OR relationship.

1. A user accesses the system and makes an operation request.
2. The system evaluates all the permission policies assigned to the user.
3. In these policies, the system looks for explicit deny permissions. If the system finds an explicit deny that applies, it returns a decision of Deny, and the authentication ends.
4. If no explicit deny is found, the system looks for allow permissions that would apply to the request. If the system finds an explicit allow permission that applies, it returns a decision of Allow, and the authentication ends.
5. If no explicit allow permission is found, IAM returns a decision of Deny, and the authentication ends.

12.2.2 Bucket Policies and Object Policies

Bucket Owner and Object Owner

The owner of a bucket is the account that created the bucket. If the bucket is created by an IAM user under the account, the bucket owner is the account instead of the IAM user.

The owner of an object is the account that uploads the object, who may not be the owner of the bucket to which the object belongs. For example, account **B** is granted the permission to access a bucket of account **A**, and account **B** uploads a file to the bucket. In that case, instead of the bucket owner account **A**, account **B** is the owner of the object.

Bucket Policies

A bucket policy is attached to a bucket and objects in the bucket. By leveraging bucket policies, the owner of a bucket can grant IAM users or other accounts the permissions to operate the bucket and objects in the bucket.

NOTA

Creating buckets and obtaining the bucket list are service level operations that should be configured by **granting IAM permissions**.

Application Scenarios

- If no permisos de IAM are used for access control and you want to grant other accounts the permissions to access your OBS resources, you can use bucket policies.
- You can configure bucket policies to grant IAM users different access permissions on buckets.
- You can also use bucket policies to grant other accounts the permissions to access your buckets.

Bucket Policy Templates

OBS Console provides bucket policy templates for six typical scenarios. You can use the templates to quickly configure bucket policies.

When using a template to create a bucket policy, you need to specify principals (authorized users) and resources, or you can modify the template settings, including principal, resources, actions, and conditions.

Tabla 12-2 Bucket policy templates

Template Name	Principal	Resource	Template Action
Bucket read-only	To be specified	The bucket and all objects in the bucket	**Allows specified users to perform the following actions on the current bucket and all objects in it:** Get* (all GET actions) List* (all LIST actions) HeadBucket (to check whether the bucket exists)
Bucket read and write	To be specified	The bucket and all objects in the bucket	**Allows specified users to perform all actions excluding the following ones on the current bucket and all objects in it:** DeleteBucket (to delete the bucket) PutBucketPolicy (to configure a bucket policy) PutBucketAcl (to configure the bucket ACL)

Template Name	Principal	Resource	Template Action
Directory read-only	To be specified	To be specified (You need to specify an object name prefix.)	**Allows specified users to perform the following actions on the current bucket and specified objects in it:** ListBucket (to list objects in the bucket and obtain the bucket metadata) HeadBucket (to check whether the bucket exists) GetBucketLocation (to get the bucket location) ListBucketVersions (to list object versions in the bucket) GetObject (to obtain object content and metadata) RestoreObject (to restore objects from Archive storage) GetObjectAcl (to obtain the object ACL) GetObjectVersion (to obtain the content and metadata of a specified object version) GetObjectVersionAcl (to obtain the ACL of a specified object version)

Template Name	Principal	Resource	Template Action
Directory read and write	To be specified	To be specified (You need to specify an object name prefix.)	**Allows specified users to perform the following actions on the current bucket and specified objects in it:** ListBucket (to list objects in the bucket and obtain the bucket metadata) HeadBucket (to check whether the bucket exists) GetBucketLocation (to get the bucket location) ListBucketVersions (to list object versions in the bucket) ListBucketMultipartUploads (to list multipart uploads) GetObject (to obtain object content and metadata) PutObject (to upload objects using PUT and POST, upload parts, initiate multipart uploads, and assemble parts) RestoreObject (to restore objects from Archive storage) GetObjectAcl (to obtain the object ACL) PutObjectAcl (to configure the object ACL) GetObjectVersion (to obtain the content and metadata of a specified object version) GetObjectVersionAcl (to obtain the ACL of a specified object version) AbortMultipartUpload (to abort multipart uploads) ListMultipartUploadParts (to list uploaded parts) ModifyObjectMetaData (to modify object metadata)

Template Name	Principal	Resource	Template Action
Public read	Anonymous user (all Internet users)	The bucket and all objects in the bucket	**Allows anonymous users to perform the following actions on the current bucket and all objects in it:** HeadBucket (to check whether the bucket exists) GetBucketLocation (to get the bucket location) ListBucketVersions (to list object versions in the bucket) GetObject (to obtain object content and metadata) RestoreObject (to restore objects from Archive storage) GetObjectVersion (to obtain the content and metadata of a specified object version)

Template Name	Principal	Resource	Template Action
Public read and write	Anonymous user (all Internet users)	The bucket and all objects in the bucket	**Allows anonymous users to perform the following actions on the current bucket and all objects in it:** ListBucket (to list objects in the bucket and obtain the bucket metadata) HeadBucket (to check whether the bucket exists) GetBucketLocation (to get the bucket location) ListBucketVersions (to list object versions in the bucket) ListBucketMultipartUploads (to list multipart uploads) GetObject (to obtain object content and metadata) PutObject (to upload objects using PUT and POST, upload parts, initiate multipart uploads, and assemble parts) RestoreObject (to restore objects from Archive storage) GetObjectAcl (to obtain the object ACL) PutObjectAcl (to configure the object ACL) GetObjectVersion (to obtain the content and metadata of a specified object version) GetObjectVersionAcl (to obtain the ACL of a specified object version) AbortMultipartUpload (to abort multipart uploads) ListMultipartUploadParts (to list uploaded parts) ModifyObjectMetaData (to modify object metadata)

Custom Bucket Policies

You can also customize bucket policies based on your needs. A custom bucket policy consists of five basic elements: effect, principals, resources, actions, and conditions. For details, see **Bucket Policy Parameters**.

Object Policies

Object policies apply to objects in a bucket. A bucket policy is applicable to a set of objects (with the same object name prefix) or to all objects (specified by an asterisk *) in the bucket.

To configure an object policy, select an object, and then configure the policy directly for the object.

Object Policy Templates

OBS Console provides object policy templates for four typical scenarios. You can use the templates to quickly configure object policies.

When using a template to create an object policy, you need to specify principals (authorized users), or you can modify the template settings, including the principal, actions, and conditions. The resource is the object for which the policy needs to be configured. This resource is automatically specified by the system and does not need to be modified.

Tabla 12-3 Object policy templates

Template Name	Principal	Resource	Template Action
Read-only	To be specified	The selected object, which is automatically specified by the system and does not need to be modified.	**Allows specified users to perform the following actions on the current object:** GetObject (to obtain object content and metadata) GetObjectVersion (to obtain the content and metadata of a specified object version) GetObjectVersionAcl (to obtain the ACL of a specified object version) GetObjectAcl (to obtain the object ACL) RestoreObject (to restore objects from Archive storage)

Template Name	Principal	Resource	Template Action
Read and write	To be specified	The selected object, which is automatically specified by the system and does not need to be modified.	**Allows specified users to perform the following actions on the current object:** PutObject (to upload objects using PUT and POST, upload parts, initiate multipart uploads, and assemble parts) GetObject (to obtain object content and metadata) GetObjectVersion (to obtain the content and metadata of a specified object version) ModifyObjectMetaData (to modify object metadata) ListMultipartUploadParts (to list uploaded parts) AbortMultipartUpload (to abort multipart uploads) GetObjectVersionAcl (to obtain the ACL of a specified object version) GetObjectAcl (to obtain the object ACL) PutObjectAcl (to configure the object ACL) RestoreObject (to restore objects from Archive storage)
Public read	Anonymous user (all Internet users)	The selected object, which is automatically specified by the system and does not need to be modified.	**Allows anonymous users to perform the following actions on the current object:** GetObject (to obtain object content and metadata) RestoreObject (to restore objects from Archive storage) GetObjectVersion (to obtain the content and metadata of a specified object version)

Template Name	Principal	Resource	Template Action
Public Read and Write	Anonymous user (all Internet users)	The selected object, which is automatically specified by the system and does not need to be modified.	**Allows anonymous users to perform the following actions on the current object:** PutObject (to upload objects using PUT and POST, upload parts, initiate multipart uploads, and assemble parts) GetObject (to obtain object content and metadata) ModifyObjectMetaData (to modify object metadata) ListMultipartUploadParts (to list uploaded parts) AbortMultipartUpload (to abort multipart uploads) RestoreObject (to restore objects from Archive storage) GetObjectVersion (to obtain the content and metadata of a specified object version) PutObjectAcl (to configure the object ACL) GetObjectVersionAcl (to obtain the ACL of a specified object version) GetObjectAcl (to obtain the object ACL)

Custom Object Policies

You can also customize an object policy based on your service requirements. A custom object policy consists of five basic elements: effect, principal, resources, actions, and conditions, similar to a bucket policy. For details, see **Bucket Policy Parameters**. The resource is the selected object and is automatically configured by the system.

12.2.3 Bucket ACLs and Object ACLs

Access control lists (ACLs) enable you to manage access to buckets and objects, and define grantees and their granted access permissions. Each bucket and object has its own ACL that defines which accounts or groups are granted access and the type of access. When a request is received against a resource, OBS checks the ACL of the resource to verify whether the requester has necessary access permissions.

When you create a bucket or an object, OBS creates a default ACL that grants the resource owner full control (FULL_CONTROL) over the bucket or object.

An ACL supports up to 100 grants.

Who Is a Principal?

A principal can be an account or one of the predefined OBS groups. For details, see **Tabla 12-4**.

Tabla 12-4 Users supported by OBS

Principal	Description
Specific User	You can grant accounts access permissions to a bucket or an object using ACLs. Once a specific account is granted the access permissions, all IAM users who have OBS resource permissions under this account can have the same access permissions to operate the bucket or object. If you need to grant different access permissions to different IAM users, configure bucket policies. For details, see **Granting an IAM User Permissions to Operate a Specific Bucket**.
Owner	The owner of a bucket is the account that created the bucket. By default, the bucket owner can read and write the bucket and the bucket ACL, but cannot read objects. A bucket owner has the bucket ACL read and write permissions that are permanent and cannot be modified. The owner of an object is the account that uploaded the object, who may not be the owner of the bucket to which the object belongs. The object owner has the read access to the object, as well as the read and write access to the object ACL, and such access permissions cannot be modified. **AVISO** Do not modify the bucket owner's read and write access permissions for the bucket.
Anonymous User	Unregistered common users group of cloud services. If anonymous users are granted access to a bucket or an object, anyone can access the object or bucket without identity authentication.
Log Delivery User **NOTA** Only the bucket ACL supports authorizing permissions to the log delivery user.	A log delivery user only delivers access logs of buckets and objects to the specified target bucket. OBS does not create or upload any file to a bucket automatically. Therefore, if you want to record bucket access logs, you need to grant the permission to the log delivery user who will deliver the access logs to your specified target bucket. The user only delivers logs within the service scope of OBS. **AVISO** After logging is enabled, the log delivery user group will be automatically granted the permission to read the bucket ACL and write the bucket where logs are saved. If you manually disable such permissions, bucket logging fails.

What Permissions Can I Grant Using an ACL?

Tabla 12-5 lists the permissions you can grant using a bucket ACL.

Tabla 12-5 Access permissions controlled by a bucket ACL

Permission	Option	Description
Access to Bucket	READ	Allows a grantee to obtain the list of objects, multipart tasks, metadata, versioning settings, and list of object versions in a bucket.
	Object READ	Allows a grantee to obtain the content and metadata of an object.
	WRITE	Allows a grantee to upload, overwrite, and delete any object in a bucket.
Access to ACL	READ_ACP	Allows a grantee to obtain the ACL of a bucket. The bucket owner has this permission permanently by default.
	WRITE_ACP	Allows a grantee to update the ACL of a bucket. The bucket owner has this permission permanently by default.

Tabla 12-6 lists the permissions you can grant using an object ACL.

Tabla 12-6 Access permissions controlled by an object ACL

Permission	Option	Description
Access to Object	READ	Allows a grantee to obtain the content and metadata of an object.
Access to ACL	READ_ACP	Allows a grantee to obtain the ACL of an object. The object owner has this permission permanently by default.
	WRITE_ACP	Allows a grantee to update the ACL of an object. The object owner has this permission permanently by default.

NOTA

Every time you change the bucket or object access permission setting in an ACL, it overwrites the existing setting instead of adding a new access permission to the bucket or object.

You can also set an ACL through a header when invoking the API for creating a bucket or uploading an object. Six types of predefined permissions can be set. Even with the predefined permissions configured, the bucket or object owner still has the full control over the resource. Tabla 12-7 lists the predefined permissions.

Tabla 12-7 Predefined access permissions in OBS

Predefined Access Permission	Description
private	Indicates that the owner of a bucket or an object has the full control over the resource. Any other users cannot access the bucket or object. This is the default access control policy.
public-read	If this permission is granted on a bucket, anyone can obtain the object list, multipart tasks, metadata, and object versions in the bucket. If it is granted on an object, anyone can obtain the content and metadata of the object.
public-read-write	If this permission is granted on a bucket, anyone can obtain the object list, multipart tasks, metadata, and object versions in the bucket, and can upload or delete objects, initialize multipart upload tasks, upload parts, merge parts, copy parts, and cancel multipart upload tasks. If it is granted on an object, anyone can obtain the content and metadata of the object.
public-read-delivered	If this permission is granted on a bucket, anyone can obtain the object list, multipart tasks, metadata, and object versions, and obtain the object content and metadata in the bucket. It does not apply to objects.
public-read-write-delivered	If this permission is granted on a bucket, anyone can obtain the object list, multipart tasks, metadata, and object versions in the bucket, and can upload or delete objects, initialize multipart upload tasks, upload parts, merge parts, copy parts, and cancel multipart upload tasks. You can also obtain object content and metadata in the bucket. It does not apply to objects.
bucket-owner-full-control	If this permission is granted on a bucket, the bucket can be accessed only by its owner. If it is granted on an object, only the bucket or object owner has the full control over the object.

Bucket ACL Application Scenarios

ACLs control the read and write permissions for accounts and groups. ACL permission granularity is not as fine as bucket policies and permisos de IAM. Generally, it is recommended that you use permisos de IAM and bucket policies for access control.

It is recommended that you use bucket ACLs in the following scenarios:

- Grant an account with the read and write access to a bucket, so that data in the bucket can be shared or the bucket can be mounted. For example, if account **A** grants the bucket read and write permissions to account **B**, then account **B** can access the bucket by using the API and SDK, and can add an external bucket through OBS Browser+.

Object ACL Application Scenarios

ACLs control the read and write permissions for accounts and groups. ACL permission granularity is not as fine as bucket policies and permisos de IAM. Generally, it is recommended that you use permisos de IAM and bucket policies for access control.

It is recommended that you use object ACLs in the following scenarios:

- Object-level access control is required. A bucket policy can control access permissions for an object or a set of objects. If you want to further specify an access permission for an object in the set of objects for which a bucket policy has been configured, then the object ACL is recommended for easier access control over single objects.
- An object is accessed through a URL. Generally, if you want to grant anonymous users the permission to read an object through a URL, use the object ACL.

12.2.4 Relationship Between a Bucket ACL and a Bucket Policy

Mapping Between Bucket ACLs and Bucket Policies

Bucket ACLs are used to control basic read and write access to buckets. Custom settings of bucket policies support more actions that can be performed on buckets. Bucket policies supplement bucket ACLs. In most cases (granting permissions to log delivery user groups excluded), you can use bucket policies to manage access to buckets. **Tabla 12-8** shows the mapping between bucket ACL access permissions and bucket policy actions.

Tabla 12-8 Mapping relationship between bucket ACLs and bucket policies

ACL Permission	Option	Mapped Action in a Custom Bucket Policy
Access to bucket	Read	• HeadBucket • ListBucket • ListBucketVersions • ListBucketMultipartUploads
	Object read	• GetObject
	Write	• PutObject • DeleteObject • DeleteObjectVersion
Access to ACL	Read	GetBucketAcl
	Write	PutBucketAcl

Mapping Relationship Between Object ACLs and Bucket Policies

Object ACLs are used to control basic read and write access permissions for objects. The custom settings of bucket policies support more actions that can be performed on objects. **Tabla 12-9** describes the mapping relationship between object ACL access permissions and bucket policy actions.

Tabla 12-9 Mapping relationship between object ACLs and bucket policies

Object ACL	Option	Mapped Action in a Custom Bucket Policy
Access to Object	Read	• GetObject • GetObjectVersion
Access to ACL	Read	• GetObjectAcl • GetObjectVersionAcl
	Write	• PutObjectAcl • PutObjectVersionAcl

12.2.5 How Does Authorization Work When Multiple Access Control Mechanisms Co-Exist?

Based on the least-privilege principle, decisions default to deny, and an explicit deny statement always takes precedence over an allow statement. For example, permisos de IAM grant a user the access to an object, a bucket policy denies the user's access to that object, and there is no ACL. Then access will be denied.

If no method specifies an allow statement, then the request will be denied by default. Only if no method specifies a deny statement and one or more methods specify an allow statement, will the request be allowed. For example, if a bucket has multiple bucket policies with allow statements, the adding of a new bucket policy with an allow statement will simply add the allowed permissions to the bucket, but the adding of a new bucket policy with a deny statement will result in a re-arrangement of the permissions. The deny statement will take precedence over allowed statements, even the denied permissions are allowed in other bucket policies.

Figura 12-3 Authorization process

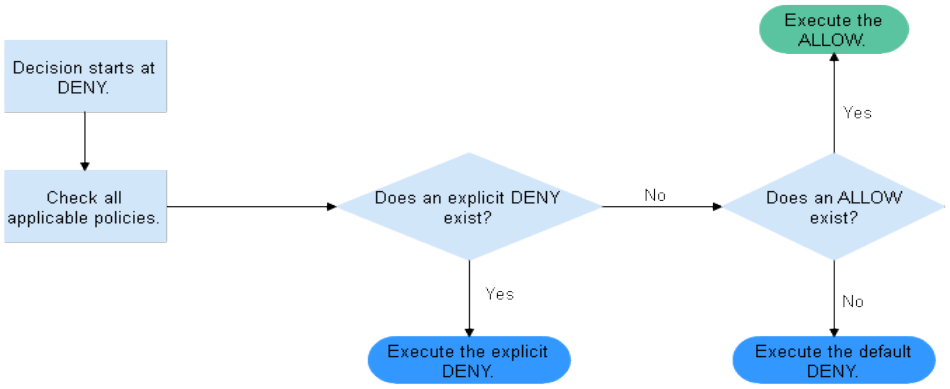


Figura 12-4 is a matrix of the permisos de IAM, bucket policies, and ACLs (allow and deny effects).

Figura 12-4 Matrix of the permisos de IAM, bucket policies, and ACLs (allow and deny effects)

<table>
<tr><td rowspan="2">Bucket Policy</td><td colspan="3">IAM Policy</td><td rowspan="2">ACL</td></tr>
<tr><td>Deny</td><td>Allow</td><td>Default Deny</td></tr>
<tr><td rowspan="2">Deny</td><td colspan="3" rowspan="2">Deny</td><td>Allow</td></tr>
<tr><td>Default Deny</td></tr>
<tr><td rowspan="2">Allow</td><td rowspan="4">Deny</td><td colspan="2" rowspan="2">Allow</td><td>Allow</td></tr>
<tr><td>Default Deny</td></tr>
<tr><td rowspan="2">Default Deny</td><td>Allow</td><td>Deny</td><td>Allow</td></tr>
<tr><td>Deny</td><td>Deny</td><td>Default Deny</td></tr>
</table>

12.3 Bucket Policy Parameters

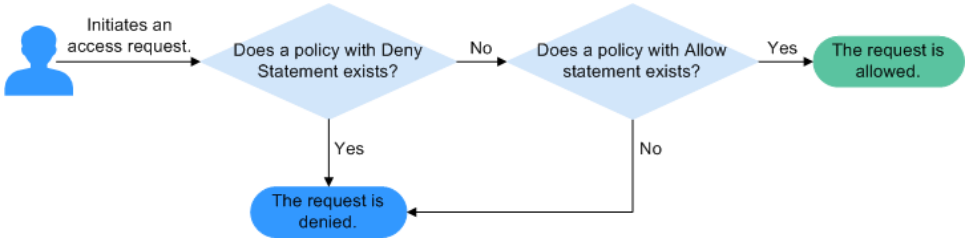
12.3.1 Effect

A bucket policy can either allow or deny requests.

- **Allow**: The policy allows the matched requests.
- **Deny**: The policy denies the matched requests.

When a bucket policy contains both the allow and deny effects, the deny effect prevails. The following figure shows the judgment process.

Figura 12-5 Determining a bucket policy when the allow and deny statements conflict



1. A user initiates an access request.
2. OBS preferentially searches for bucket policies that have the deny (explicit deny) effect. If a deny statement is found, OBS directly rejects the access. The access request ends.
3. If there is no deny statement, OBS searches for allow statements.
   - If an allow statement is found, OBS allows the access.
   - If no allow statement is found, OBS rejects the access. The access request ends.
4. If an error occurs during the judgment, an error message is generated and returned to the user who initiates the access request.

12.3.2 Principals

The principals indicate the users which the bucket policies apply to. These users can be accounts and IAM users. Target users can be specified in either of the following ways:

- **Include**: The policy takes effect on specified users.
- **Exclude**: The policy takes effect on all users except the specified ones.

12.3.3 Resources

You can apply a bucket policy to the following resources: the current bucket, and all objects in a bucket.

Resources can be specified in either of the following ways:

- **Include**: The policy takes effect on the specified OBS resources.
- **Exclude**: The policy takes effect on all OBS resources except the specified ones.

Applying a Bucket Policy to a Bucket

To specify the current bucket as the resource, select **Current bucket**. When configuring actions for the policy, select bucket related actions.

Applying a Bucket Policy to Specified Objects

To apply the bucket policy to specified objects in a bucket, object-related actions must be configured in the policy. The configuration format is as follows:

- For an object, enter the object name (including its folder name if any). For example, if the specified resource is the **example.jpg** file in the **imgs-folder** folder in the bucket, enter the following content in the resource text box:

  imgs-folder/example.jpg
- For an object set, the wildcard asterisk (*) should be used. The asterisk * indicates an empty string or any combination of multiple characters. The format rules are as follows:
  - Use only one asterisk (*) to indicate all objects in a bucket.
  - Use *Object name prefix** to indicate objects starting with this prefix in a bucket. For example,

    imgs*
  - Use **Object name suffix* to indicate objects ending with this suffix in a bucket. For example,

    *.jpg

12.3.4 Actions

Actions are related to resources. When the resource is the current bucket, bucket-related actions should be configured in a bucket policy. When objects are specified as resources, object-related actions should be configured in a bucket policy.

Actions can be specified in either of the following ways:

- **Include**: The policy takes effect on specified actions.

- **Exclude**: The policy takes effect on all actions except the specified ones.

Actions Related to Buckets

Tabla 12-10 Actions related to buckets

Type	Value	Description
General	*	The value supports a wildcard character (*) that indicates all operations can be performed.
	Get*	The value supports a wildcard character (*) that indicates all GET operations can be performed.
	Put*	The value supports a wildcard character (*) that indicates all PUT operations can be performed.
	List*	The value supports a wildcard character (*) that indicates all LIST operations can be performed.
Bucket	HeadBucket	Checks whether a bucket exists.
	DeleteBucket	Deletes a bucket.
	GetBucketStorage	Obtains bucket storage information.
	ListBucket	Lists objects in a bucket, and obtains the bucket metadata.
	ListBucketVersions	Lists versioned objects in a bucket.
	ListBucketMultipartUp-loads	Lists multipart uploads.
	GetBucketAcl	Obtains the bucket ACL information.
	PutBucketAcl	Configures a bucket ACL.
	GetBucketCORS	Obtains the CORS configuration of the bucket.
	PutBucketCORS	Configures CORS for a bucket.
	GetBucketVersioning	Obtains the bucket versioning information.
	PutBucketVersioning	Configures versioning for a bucket.
	ListBucketVersions	Lists versioned objects in a bucket.
	GetBucketLocation	Obtains the bucket location.
	GetBucketLogging	Obtains the bucket logging information.
	PutBucketLogging	Configures logging for a bucket.
	GetBucketWebsite	Obtains the static website configuration of the bucket.
	PutBucketWebsite	Configures the static website hosting for the bucket.

Type	Value	Description
	DeleteBucketWebsite	Deletes the static website hosting configuration of the bucket.
	GetLifecycleConfiguration	Obtains the lifecycle rules of the bucket.
	PutLifecycleConfiguration	Configures a lifecycle rule for a bucket.
	GetBucketInventoryConfiguration	Obtains the inventory configuration of a bucket.
	PutBucketInventoryConfiguration	Configures inventories for a bucket.
	DeleteBucketInventoryConfiguration	Deletes the inventory configuration of a bucket.
	PutBucketPolicy	Configures a bucket policy.
	GetBucketPolicy	Obtains a bucket policy.
	DeleteBucketPolicy	Deletes a bucket policy.
	PutBucketNotification	Configures event notifications for a bucket.
	GetBucketNotification	Obtains the event notification configuration of a bucket.
	PutBucketStoragePolicy	Configures the default storage class for a bucket.
	GetBucketStoragePolicy	Obtains the default storage class of a bucket.
	PutReplicationConfiguration	Configures cross-region replication for a bucket.
	GetReplicationConfiguration	Obtains the cross-region replication configuration of a bucket.
	DeleteReplicationConfiguration	Deletes the cross-region replication configuration of a bucket.
	PutBucketTagging	Configures tags for a bucket.
	GetBucketTagging	Obtains bucket tags.
	DeleteBucketTagging	Deletes bucket tags.
	PutBucketQuota	Configures bucket storage quota.
	GetBucketQuota	Queries bucket storage quota.
	PutBucketCustomDomainConfiguration	Binds a user-defined domain name to a bucket.

Type	Value	Description
	GetBucketCustomDomainConfiguration	Obtains the user-defined domain name bound to a bucket.
	DeleteBucketCustomDomainConfiguration	Unbinds a user-defined domain name from a bucket.
	PutDirectColdAccessConfiguration	Configures direct reading for a bucket.
	GetDirectColdAccessConfiguration	Obtains the direct reading configuration of a bucket.
	DeleteDirectColdAccessConfiguration	Deletes the direct reading configuration of a bucket.
	GetEncryptionConfiguration	Obtains the encryption configuration of a bucket.
	PutEncryptionConfiguration	Configures default encryption for a bucket.
	GetBucketObiectLockConfiquration	Obtains the default retention settings of a bucket.
	PutBucketObiectLockConfiquration	Configures a default retention policy for a bucket.

Actions Related to Objects

Tabla 12-11 Actions related to objects

Type	Value	Description
General	*	The value supports a wildcard character (*) that indicates all operations can be performed.
	Get*	The value supports a wildcard character (*) that indicates all GET operations can be performed.
	Put*	The value supports a wildcard character (*) that indicates all PUT operations can be performed.
	List*	The value supports a wildcard character (*) that indicates all LIST operations can be performed.
Object	GetObject	Obtains an object and its metadata.
	GetObjectVersion	Obtains the object of a specified version and its metadata.
	PutObject	Performs PUT upload, POST upload, multipart upload, initialization of uploaded parts, and merging of parts.

Type	Value	Description
	GetObjectAcl	Obtains the object ACL information.
	GetObjectVersionAcl	Obtains the ACL information of a specified object version.
	PutObjectAcl	Configures an object ACL.
	PutObjectVersionAcl	Configures the ACL for a specified object version.
	DeleteObject	Deletes an object.
	DeleteObjectVersion	Deletes a specified object version.
	ListMultipartUploadParts	Lists uploaded parts.
	AbortMultipartUpload	Cancels a multipart upload task.
	ModifyObjectMetadata	Modifies object metadata
	RestoreObject	Restores Archive objects.
	PutObjectRetention	Configures a retention policy for an object.

12.3.5 Conditions

In addition to effect, principals, resources, and actions, you can specify conditions for a bucket policy. A bucket policy takes effect only when its condition expressions match values contained in the request. **Conditions** is an optional parameter. You can determine whether to use this parameter based on service requirements.

For example, if account **A** needs to be granted with full control permissions for an object uploaded by account **B** in bucket **example**, you can specify that the upload request must contain the **acl** key and set the policy effect to **Allow** for account **A**. The complete condition expression is as follows:

Condition Operator	Key	Value
StringEquals	acl	bucket-owner-full-control

A condition consists of three parts: condition operator, key, and value. Condition operators and keys are associated with each other. For example:

- If a string type condition operator is selected, such as **StringEquals**, the key can only be of the string type, such as **UserAgent**.
- If a date type key is selected, such as **CurrentTime**, the condition operator can only be of the date type, such as **DateEquals**.

Tabla 12-12 describes the predefined condition operators provided by OBS.

Tabla 12-12 Condition operators

Type	Key	Description
String	StringEquals	Strict matching. Short version: streq
	StringNotEquals	Strict negated matching. Short version: strneq
	StringEqualsIgnoreCase	Strict matching, ignoring case. Short version: streqi
	StringNotEqualsIgnoreCase	Strict negated matching, ignoring case. Short version: strneqi
	StringLike	Loose case-sensitive matching. The values can include a multi-character match wildcard (*) or a single-character match wildcard (?) anywhere in the string. Short version: strl
	StringNotLike	Negated loose case-sensitive matching. The values can include a multi-character match wildcard (*) or a single-character match wildcard (?) anywhere in the string. Short version: strnl
Numeric	NumericEquals	Strict matching. Short version: numeq
	NumericNotEquals	Strict negated matching. Short version: numneq
	NumericLessThan	"Less than" matching. Short version: numlt
	NumericLessThanEquals	"Less than or equals" matching. Short version: numlteq
	NumericGreaterThan	"Greater than" matching. Short version: numgt
	NumericGreaterThanEquals	"Greater than or equals" matching. Short version: numgteq
Date	DateEquals	Strict matching. Short version: dateeq
	DateNotEquals	Strict negated matching. Short version: dateneq
	DateLessThan	Indicates that the date is earlier than a specific date. Short version: datelt
	DateLessThanEquals	Indicates that the date is earlier than or equal to a specific date. Short version: datelteq
	DateGreaterThan	Indicates that the date is later than a specific date. Short version: dategt

Type	Key	Description
	DateGreaterThanEquals	Indicates that the date is later than or equal to a specific date. Short version: dategteq
Boolean	Bool	Strict Boolean matching
IP address	IpAddress	Takes effect only on a specified IP address or IP address range. Example: **x.x.x.x/24**
	NotIpAddress	Takes effect only on all except the specified IP address or IP address range. Example: **x.x.x.x/24**

A condition can contain any of the three types of keys: general keys, keys related to bucket actions, and keys related to object actions.

Tabla 12-13 General keys

Key	Type	Description
CurrentTime	Date	Indicates the date when the request is received by the server. The date format must comply with ISO 8601.
EpochTime	Numeric	Indicates the time when the request is received by the server, which is expressed as seconds since 1970.01.01 00:00:00 UTC, regardless of the leap seconds.
SecureTransport	Bool	Requests whether to use SSL.
SourceIp	IP address	Source IP address from which the request is sent
UserAgent	String	Requested client software agent
Referer	String	Indicates the link from which the request is sent.

Tabla 12-14 Keys related to bucket actions

Action	Optional Key	Description	Description
ListBucket	prefix	Type: String. Lists objects that begin with the specified prefix.	If **prefix**, **delimiter**, and **max-keys** are configured, the key-value pair meeting the conditions must be specified in the List operation for the bucket policy to take effect. For example, if a bucket policy (with the conditional operator set to **NumericEquals**, the key to **max-keys**, and the value to **100**) that allows anonymous users to read data is configured for a bucket, the anonymous users must add **?max-keys=100** to the end of the bucket domain name for listing objects. The listed objects are the first 100 objects in alphabetic order.
	max-keys	Type: Numeric. Sets the maximum number of objects. Returned objects are listed in alphabetic order.	
ListBucketVersions	prefix	Type: String. Lists multi-version objects whose name starts with the specified prefix.	
	max-keys	Type: Numeric. Sets the maximum number of objects. Returned objects are listed in alphabetic order.	
PutBucketAcl	acl	Type: String. Configures the bucket ACL. When modifying a bucket ACL, you can use the request that contains a canned ACL setting in its header. Value options of a canned ACL setting: **private|public-read|public-read-write|authenticated-read|bucket-owner-read|bucket-owner-full-control|log-delivery-write**	None

Tabla 12-15 Keys related to object actions

Action	Optional Key	Description
PutObject	acl	Type: String. Configures the object ACL. When uploading an object, you can use the request that contains a canned ACL setting in its header. Value options of a canned ACL setting: **private|public-read|public-read-write|authenticated-read|bucketowner-read|bucket-owner-full-control|log-delivery-write**.
	copysource	Type: String. Specifies names of the source bucket and the source object. Format: /**bucketname/keyname**
	metadata-directive	Type: String. Specifies whether to copy the metadata from the source object or replace with the metadata in the request. Values: **COPY|REPLACE**
PutObjectAcl	acl	Type: String. Configures the object ACL. When uploading an object, you can use the request that contains a canned ACL setting in its header. Value options of a canned ACL setting: **private|public-read|public-read-write|authenticated-read|bucketowner-read|bucket-owner-full-control|log-delivery-write**.
GetObjectVersion	VersionId	Type: String. Obtains the object with the specified version ID.
GetObjectVersionAcl	VersionId	Type: String. Obtains the ACL of the object with specified version ID.
PutObjectVersionAcl	VersionId	Type: String. Specifies a version ID.
	acl	Type: String. Configures the ACL of the object with the specified version ID. When uploading an object, you can use the request that contains a canned ACL setting in its header. Value options of a canned ACL setting: **private|public-read|public-read-write|authenticated-read|bucketowner-read|bucket-owner-full-control|log-delivery-write**.
DeleteObjectVersion	VersionId	Type: String. Deletes the object with the specified version ID.

12.4 Configuración de permisos de IAM

12.4.1 Creación de un usuario de IAM y concesión de permisos de OBS

En este capítulo se describe cómo utilizar **IAM** para el control de permisos detallado para los recursos de OBS. Con IAM, usted puede:

- Crear usuarios de IAM para empleados en función de la estructura organizativa de su empresa. Cada usuario de IAM tiene sus propias credenciales de seguridad, lo que proporciona acceso a los recursos de OBS.
- Gestionar los permisos según el principio de permisos mínimos (PoLP).
- Confiar una cuenta de Huawei Cloud o un servicio en la nube para realizar operaciones eficientes en sus recursos de OBS.

Si su cuenta de Huawei Cloud no requiere usuarios individuales de IAM, omita este capítulo.

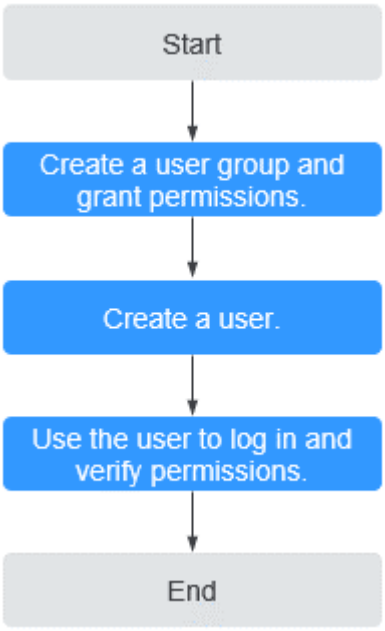
En esta sección se describe el procedimiento para conceder permisos (consulte **Figura 12-6**).

Requisitos previos

Obtenga información sobre los permisos (consulte **Gestión de permisos**) admitidos por OBS y elija políticas o roles de acuerdo con sus requisitos.

Proceso

Figura 12-6 Proceso de concesión de permisos de OBS a un usuario de IAM



El siguiente ejemplo describe cómo conceder a un usuario de IAM el permiso **Tenant Guest** en OBS.

1. **Crear un grupo de usuarios y asignar permisos**.

   Cree un grupo de usuarios en la consola de IAM y asigne al grupo el permiso **Tenant Guest**.

2. **Crear un usuario de IAM y agregarlo al grupo de usuario**.

   Cree un usuario en la consola de IAM y agregue el usuario al grupo creado en **1**.

3. **Iniciar sesión** y verificar el permiso otorgado.

   Inicie sesión en OBS Console con el usuario recién creado y compruebe que el permiso asignado haya tenido efecto:

   – Elija **Object Storage Service** en la lista de servicios para ir a la página de inicio de OBS. Si se muestra la lista de bucket y se puede ver la información básica sobre cualquier bucket, pero no se puede crear o eliminar bucket ni realizar ninguna otra operación, el permiso **Tenant Guest** concedido ya tiene efecto.

   – Vaya a un bucket de OBS. Si se muestra la lista de objetos y se pueden descargar objetos, pero no se pueden cargar o eliminar objetos ni realizar ninguna otra operación, el permiso **Tenant Guest** concedido ya ha surtido efecto.

12.4.2 Políticas personalizadas de OBS

Se pueden crear políticas personalizadas para complementar las políticas definidas por el sistema de OBS. Para ver las acciones admitidas para las políticas personalizadas, consulte **Acciones relacionadas con buckets** y **Acciones relacionadas con objetos**.

Puede crear políticas personalizadas de cualquiera de las dos formas siguientes:

- Visual editor: Seleccione los servicios en la nube, acciones, recursos y condiciones de solicitud sin la necesidad de conocer la sintaxis de la política.
- JSON: Edite las políticas de JSON desde cero o basándose en una política existente.

Para obtener más información, consulte **Creación de una política personalizada**. A continuación se proporcionan ejemplos de políticas personalizadas de OBS comunes.

Ejemplo de las políticas personalizadas

- Ejemplo 1: Concede todos los permisos de OBS a los usuarios.

  Esta política permite a los usuarios realizar cualquier operación en OBS.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:*:*"
            ]
        }
    ]
}
```

- Ejemplo 2: Concede todos los permisos de OBS Console a los usuarios.

  Esta política permite a los usuarios realizar todas las operaciones en OBS Console.

  Cuando un usuario inicia sesión en OBS Console, el usuario puede acceder a recursos de otros servicios, como información de auditoría en CTS, nombres de dominio de aceleración en CDN y claves en KMS. Por lo tanto, además de los permisos de OBS del ejemplo 1, también debe configurar los permisos de acceso a otros servicios. CDN es un servicio global, mientras que CTS y KMS son regionales. Debe configurar el permiso de **Tenant Guest** para el proyecto global y los proyectos regionales en función de los servicios y regiones que utilice.

```
{
    "Version": "1.1",
    "Statement": [
```



```
        {
            "Effect": "Allow",
            "Action": [
                "obs:*:*"
            ]
        }
    ]
}
```

- Ejemplo 3: Otorgar el permiso de solo lectura en un bucket a los usuarios (cualquier directorio).

  Este política permite a los usuarios listar y descargar todos los objetos de bucket **obs-example**.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:GetObject",
                "obs:bucket:ListBucket"
            ],
            "Resource": [
                "obs:*:*:object:obs-example/*",
                "obs:*:*:bucket:obs-example"
            ]
        }
    ]
}
```

- Ejemplo 4: Otorgar el permiso de solo lectura en un bucket a los usuarios (directorio especificado).

  Este política permite a los usuarios descargar objetos solo en el directorio **my-project/** de bucket **obs-example**. Los objetos de otros directorios se pueden enumerar, pero no se pueden descargar.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:GetObject",
                "obs:bucket:ListBucket"
            ],
            "Resource": [
                "obs:*:*:object:obs-example/my-project/*",
                "obs:*:*:bucket:obs-example"
            ]
        }
    ]
}
```

- Ejemplo 5: Otorgar los permisos de lectura y escritura en un bucket a los usuarios (directorio especificado).

  Este política permite a los usuarios listar, descargar, cargar y eliminar objetos en el directorio **my-project** de bucket **obs-example**.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:GetObject",
                "obs:object:ListMultipartUploadParts",
                "obs:bucket:ListBucket",
                "obs:object:DeleteObject",
```



```
                "obs:object:PutObject"
            ],
            "Resource": [
                "obs:*:*:object:obs-example/my-project/*",
                "obs:*:*:bucket:obs-example"
            ]
        }
    ]
}
```

- Ejemplo 6: Otorgar todos los permisos de un bucket a los usuarios.

  Este política permite a los usuarios realizar cualquier operación en bucket **obs-example**.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:*:*"
            ],
            "Resource": [
                "obs:*:*:bucket:obs-example",
                "obs:*:*:object:obs-example/*"
            ]
        }
    ]
}
```

- Ejemplo 7: Denegar permisos a los usuarios para cargar objetos.

  Una política de denegación debe usarse junto con otras políticas. Si los permisos asignados a un usuario contienen tanto "Allow" como "Deny", los permisos "Deny" tienen prioridad sobre los permisos "Allow".

  Si concede la directiva de sistema OBS OperateAccess a un usuario pero no desea que el usuario tenga el permiso de carga de objetos (que también es un permiso permitido por OBS OperateAccess), puede crear una directiva personalizada además de la política de OBS OperateAccess para denegar el permiso de carga del usuario. De acuerdo con el principio de autorización, la política con la declaración de denegación tiene prioridad, de modo que el usuario puede realizar todas las operaciones permitidas por OBS OperateAccess, excepto cargar objetos. A continuación se muestra un ejemplo de una política de denegación:

```
{
         "Version": "1.1",
         "Statement": [
                 {
                         "Effect": "Deny",
                         "Action": [
                                 "obs:object:PutObject"
                         ],
                 }
         ]
 }
```

12.4.3 Recursos de OBS

Un recurso es un objeto que existe dentro de un servicio. Los recursos de OBS incluyen buckets y objetos. Puede seleccionar estos recursos especificando sus rutas.

Tabla 12-16 Recursos de OBS y sus caminos

Tipo de recurso	Nombre del recurso	Ruta
bucket	bucket	[Format] obs:*:*:bucket:*bucket name* [Notes] Para los recursos del bucket, IAM genera automáticamente el prefijo de la ruta del recurso: **obs:*:*:bucket:** Para la ruta de un bucket específico, agregue el *bucket name* al final. También puede utilizar un asterisco * para indicar cualquier bucket. Ejemplo: **obs:*:*:bucket:***
object	object	[Format] obs:*:*:object:*bucket name/object name* [Notes] Para los recursos de objeto, IAM genera automáticamente el prefijo de la ruta del recurso: **obs:*:*:object:** Para la ruta de un objeto específico, agregue el *bucket name/object name* al final. También puede utilizar un asterisco * para cualquier objeto de un bucket. Ejemplo: **obs:*:*:object:my-bucket/my-object/*** indica cualquier objeto en el directorio **my-object** del bucket **my-bucket**.

12.4.4 Condiciones de solicitud de OBS

Las condiciones de solicitud son útiles para determinar cuándo entra en vigor una política personalizada. Una condición de solicitud consiste en una clave de condición y un operador. Las claves de condición son globales o de nivel de servicio y se utilizan en los elementos de condición de una instrucción de política. **Las claves de condición globales** (comenzando con **g:**) están disponibles para las operaciones de todos los servicios, mientras que las claves de condición de nivel de servicio (comenzando con un acrónimo de nombre de servicio como **obs:**) solo están disponibles para las operaciones de un servicio específico. Un operador se utiliza junto con una clave de condición para formar una declaración de condición completa.

OBS has a group of predefined condition keys that can be used in IAM. For example, to define an allow permission, you can use the condition key **obs:SourceIp** to filter matching requesters by IP address.

Las claves de condición y los operadores admitidos por OBS son los mismos que los de la política de bucket. Cuando configure las claves de condición en IAM, inícielas con **obs:**. Para obtener más información, consulte **Formato de política**.

12.5 Configuración de la política de bucket

12.5.1 Creación de una política de bucket con una plantilla

OBS Console proporciona plantillas de políticas de bucket para seis escenarios típicos. Puede utilizar estas plantillas para configurar rápidamente las políticas de bucket.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

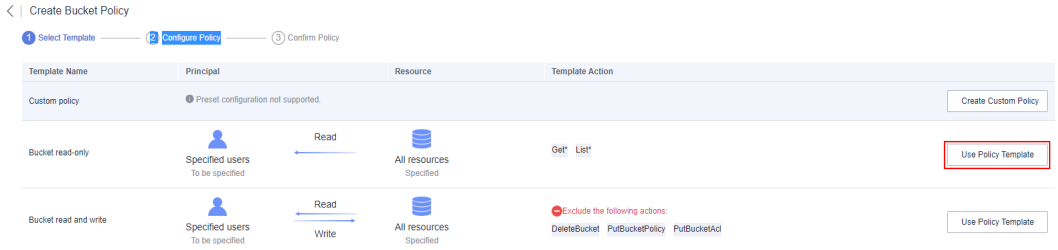
Paso 3 En el panel de navegación, elija **Permissions** > **Bucket Policy**.

Paso 4 Haga clic en **Create**.

Paso 5 En la lista de plantillas, seleccione una plantilla y haga clic en **Use Policy Template** a la derecha.

Para obtener más información sobre cada plantilla, consulte **Política de bucket**.

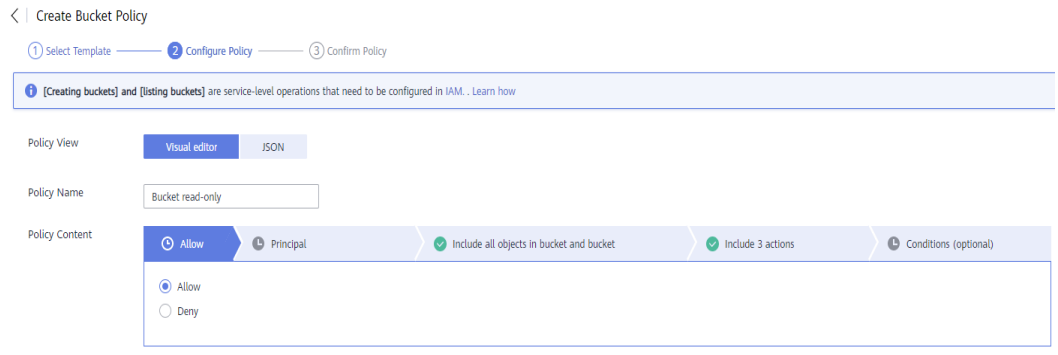
Figura 12-7 Creación de una política de bucket con una plantilla



Paso 6 Ingrese la información requerida.

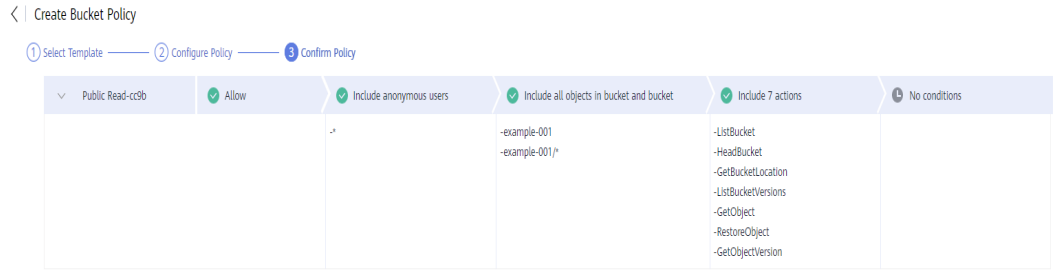
Para algunas plantillas de política de bucket, debe configurar el principal y los recursos como se le indique. También puede cambiar la configuración de una plantilla predefinida, incluidos el nombre de la política, el principal, los recursos, las acciones y las condiciones. Para obtener más información, consulte **Parámetros de política de bucket**.

Figura 12-8 Configuración de la política de bucket



Paso 7 Haga clic en **Next** para confirmar la configuración de la política.

Figura 12-9 Confirmación de una configuración de política de bucket



Paso 8 Haga clic en **Create** en la esquina inferior derecha de la página para crear la política de bucket.

----Fin

12.5.2 Creación de una política de bucket personalizada (Visual Editor)

También puede personalizar las políticas de bucket en función de sus necesidades de servicio. Una política de bucket personalizada consta de cinco elementos básicos: efecto, principales, recursos, acciones y condiciones. Para obtener más detalles, consulte **Parámetros de política de bucket**.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

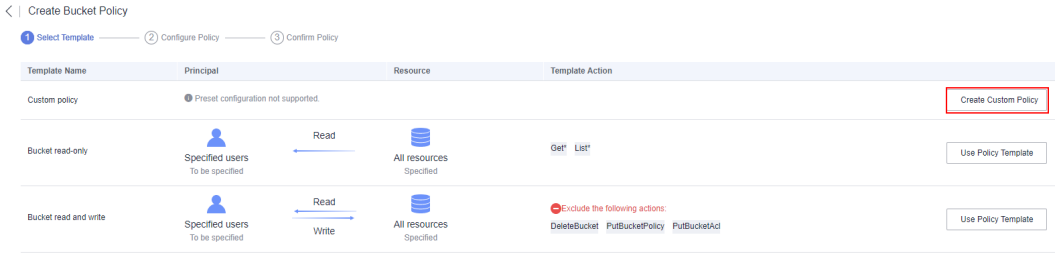
Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Permissions** > **Bucket Policy**.

Paso 4 Haga clic en **Create**.

Paso 5 En la primera fila de la lista de plantillas, haga clic en **Create Custom Policy** a la derecha.

Figura 12-10 Creación de una política personalizada



Paso 6 Configure una política de bucket.

Figura 12-11 Configuración de la política de bucket

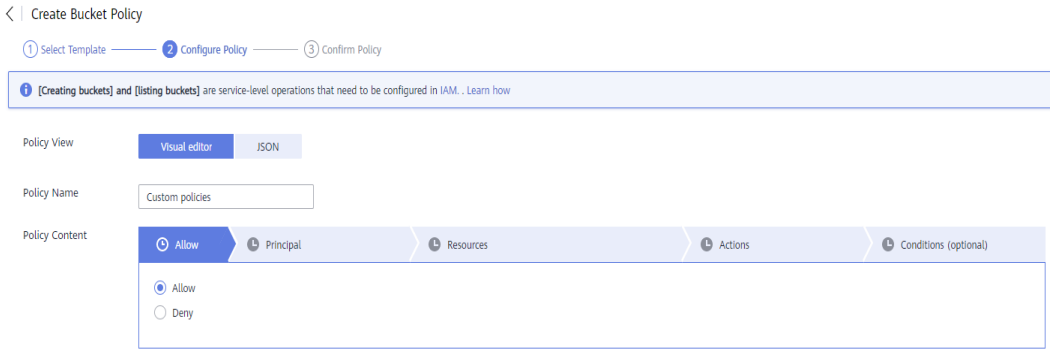


Tabla 12-17 Parámetros para configurar una política de bucket personalizada

Parámetro		Descripción
Policy View		Visual editor o JSON. El editor visual se utiliza aquí. Para obtener más información sobre las configuraciones en la vista de JSON, consulte **Creación de una política de bucket personalizada (vista JSON)**.
Policy Name		Ingrese un nombre de política de bucket.
Policy Content	Effect	● **Allow**: La política permite las solicitudes coincidentes. ● **Deny**: La política deniega las solicitudes coincidentes.
	Principal	● Configure usuarios autorizados: – **Current account**: Seleccione uno o más usuarios de IAM en la cuenta actual. – **Other account**: Especifique uno o más ID de cuenta. Si desea aplicar la política de bucket a los usuarios de IAM en esa cuenta, introduzca sus ID de usuario de IAM. – **Anonymous user**: Conceda la política del bucket a cualquiera. ● Seleccione una política de usuario. – **Include specified users**: La política de bucket entra en vigor en los usuarios especificados. – **Exclude specified users**: La política de bucket tiene efecto en usuarios distintos de los especificados.

Parámetro		Descripción
	Resources	● Seleccionar ámbito de recurso: – **Current bucket**: la política de bucket se aplica a todo el bucket. Puede configurar acciones relacionadas con el bucket. – **Objects in bucket**: la política de bucket se aplica a los objetos del bucket. Puede configurar acciones relacionadas con el objeto. Puede especificar un objeto o un conjunto de objetos en los siguientes formatos: Objeto: *Object name* Conjunto de objetos: *Object name prefix**, **Object name suffix* o * ● Seleccione una política de recursos. – **Include specified resources**: la política de bucket entra en vigor en los recursos especificados. – **Exclude specified resources**: La política de bucket tiene efecto en recursos distintos de los especificados.
	Actions	● Seleccione las acciones que desea conceder. Para obtener más información sobre las acciones, consulte **Parámetros de política de bucket**. – Si solo se selecciona **Current bucket** para **Resource**, puede configurar acciones comunes y acciones de bucket. – Si solo se selecciona **Objects in bucket** para **Resource** puede configurar acciones comunes y acciones de objetos. – Si selecciona **Current bucket** y **Objects in bucket** para **Resource**, puede configurar acciones comunes, acciones de bucket y acciones de objetos. ● Seleccione una estrategia de operación para las acciones seleccionadas: – **Include selected**: la política de bucket tiene efecto en las acciones seleccionadas. – **Exclude selected**: la política de bucket tiene efecto en todas las acciones excepto en las seleccionadas.
	Conditions (optional)	● **Conditional Operator**: Consulte **Parámetros de política de bucket**. ● **Key**: Consulte **Parámetros de política de bucket**. ● **Value**: el valor introducido está asociado con la clave.

Paso 7 Haga clic en **Next** para confirmar la configuración de la política.

Paso 8 Haga clic en **Create** en la esquina inferior derecha de la página para crear la política de bucket.

----Fin

12.5.3 Creación de una política de bucket personalizada (vista JSON)

Si está familiarizado con la sintaxis de JSON y las políticas de bucket de OBS, puede codificar una política de bucket en la vista JSON. No hay límite en el número de políticas de bucket (declaraciones) para un bucket, pero el tamaño total de script de JSON de todas las políticas de bucket en un bucket no puede superar los 20 KB.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Permissions** > **Bucket Policy**.

Paso 4 En la esquina superior derecha de la página, seleccione **JSON** y haga clic en **Edit**.

Paso 5 El siguiente es un ejemplo de política editado en JSON:

```
{
   "Statement":[
       {
           "Action":[
               "CreateBucket",
               "DeleteBucket"
           ],
           "Effect":"Allow",
           "Principal":{
               "ID":[
                   "domain/account ID",
                   "domain/account ID:user/User ID"
               ]
           },
           "Condition":{
               "NumericNotEquals":{
                   "Referer":"sdf"
               },
               "StringNotLike":{
                   "Delimiter":"ouio"
               }
           },
           "Resource":"000-02/key01"
       }
   ]
}
```

Tabla 12-18 Descripción del parámetro

Parámetro	Descripción
Action	Acciones a las que se aplica la política de bucket. Para obtener más información, consulte **Parámetros de política de bucket**.

Parámetro	Descripción
Effect	Efecto de la política de bucket. Para obtener más información, consulte **Parámetros de política de bucket**.
Principal	Usuarios autorizados sobre los que entra en vigor la política de bucket. Puede obtener el ID de usuario en la página **My Credential** iniciando sesión en la consola como usuario autorizado. Formato principal: ● "dominio/*account ID*" (cuando el principal es una cuenta) ● Dominio/*account ID*:usuario/*User ID* (cuando el principal es un usuario bajo una cuenta)
Condition	Condiciones bajo las cuales la política de bucket entra en vigor. Para obtener más información, consulte **Parámetros de política de bucket**.
Resource	Recursos en los que entra en vigor la política de bucket. Para obtener más información, consulte **Parámetros de política de bucket**.

Paso 6 Haga clic en **Save**.

----Fin

12.5.4 Replicación de políticas de bucket

Escenarios

OBS le permite replicar las políticas de bucket existentes en un bucket nuevo. Al replicar políticas, OBS reemplaza automáticamente el nombre del bucket en las políticas del bucket de origen por el nombre del bucket de destino, para que las políticas se apliquen al bucket de destino.

Limitaciones y restricciones

- Las políticas replicadas desde un bucket de origen no sobrescribirán las políticas existentes en el bucket de destino.
- Las políticas de origen con el mismo nombre que las del bucket de destino no se replicarán.
- La versión de los bucket de origen y destino debe ser 3.0.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

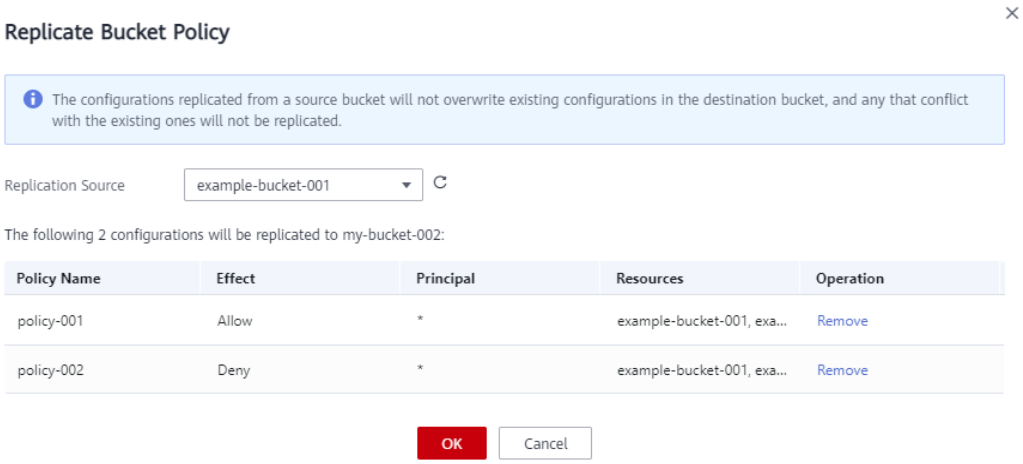
Paso 3 En el panel de navegación, elija **Permissions** > **Bucket Policy**.

Paso 4 Haga clic en **Replicate**.

Paso 5 Seleccione un origen de replicación, es decir, el bucket de origen para el que se configuraron las políticas de bucket.

Después de seleccionar un origen de replicación, se muestran todas las políticas de bucket con un nombre diferente a las del bucket de destino. Puede quitar cualquiera que no sea necesario.

Figura 12-12 Replicación de políticas de bucket



Paso 6 Haga clic en **OK** para replicar las políticas de bucket en el bucket de destino.

----Fin

12.6 Configuración de una política de objeto

Las políticas de objeto se aplican a los objetos de un bucket. Con una política de objetos, puede configurar condiciones y acciones para los objetos en un bucket.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En la fila que contiene el objeto para el que desea configurar una directiva, elija **More** > **Configure Object Policy** en la columna **Operation**. Se muestra la página **Configure Object Policy**.

Puede personalizar una política o utilizar una plantilla preestablecida para configurar una según sea necesario.

- **Using a preset template**: El sistema preajusta plantillas de política de objetos para cuatro escenarios típicos. Puede utilizar las plantillas para configurar rápidamente las

políticas de objetos. Para obtener más información sobre cada plantilla, consulte la sección **Parámetros de política de bucket**.

- **Customizing a policy**: También puede personalizar una política de objetos en función de sus necesidades. Una política de objeto personalizada consta de cinco elementos básicos: efecto, principios, recursos, acciones y condiciones, similares a una política de bucket. Para obtener más información, consulte **Parámetros de política de bucket**. El recurso es el objeto seleccionado y el sistema lo configura automáticamente. Para obtener más información acerca de cómo personalizar una política de objeto, vea **Creación de una política de bucket personalizada (Visual Editor)**. A diferencia de personalizar una política de bucket, para personalizar una política de objeto:

  a. No es necesario especificar el recurso.

  b. Solo puede configurar las acciones relacionadas con objetos.

----Fin

12.7 Configuración de la ACL de bucket

Requisitos previos

Usted es el propietario del bucket o tiene permiso para escribir la ACL de bucket.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

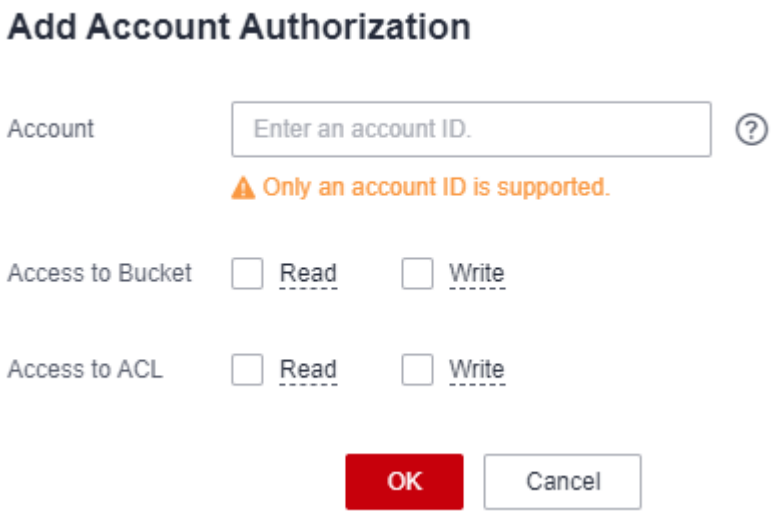
Paso 3 En el panel de navegación, elija **Permissions** > **Bucket ACLs**.

Paso 4 En **Bucket ACLs**, haga clic en **Edit** para conceder al propietario, al usuario anónimo y al usuario de entrega de registros los permisos necesarios para el bucket.

Paso 5 Haga clic en **Add** para aplicar los permisos de ACL específicos a una cuenta, como se muestra en **Figura 12-13**.

Introduzca un ID de cuenta y especifique los permisos de ACL para la cuenta. Puede obtener el ID de cuenta en la página **My Credentials**.

Figura 12-13 Adición de permisos



Paso 6 Haga clic en **OK**.

----Fin

Procedimiento de seguimiento

Después de conceder a una cuenta específica los permisos ACL para un bucket, el usuario autorizado puede usar las AK y SK para acceder a ese bucket agregando el bucket a OBS Browser+.

Después de conceder ciertos permisos a un usuario anónimo, el usuario anónimo puede acceder al bucket sin ninguna autenticación. Un usuario anónimo registrado puede utilizar cualquiera de los métodos anteriores para acceder a bucket. Un usuario anónimo no registrado puede acceder al bucket de cualquiera de las siguientes maneras:

- Acceda al nombre de dominio del bucket en un explorador para ver los objetos del bucket.
- Configure el nombre de dominio del bucket en un sistema de terceros para conectarse directamente al bucket.

12.8 Configuración de una ACL de objeto

Requisitos previos

Usted es el propietario del objeto o tiene el permiso para escribir la ACL del objeto.

Un propietario de objeto es la cuenta que carga el objeto, pero puede no ser el propietario del bucket que almacena el objeto. Por ejemplo, la cuenta **B** tiene permiso para acceder a un bucket dela cuenta **A**y la cuenta **B** carga un archivo al bucket. En ese caso, la cuenta **B**, en lugar de la cuenta de propietario del bucket **A**, es el propietario del objeto. De forma predeterminada, la cuenta A no tiene permitido acceder a este objeto y no puede leer ni modificar la ACL del objeto.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 Haga clic en el objeto que desea operar.

Paso 4 En la página de ficha **Object ACL**, haga clic en **Edit** para conceder al propietario y al usuario anónimo los permisos de ACL para el objeto.

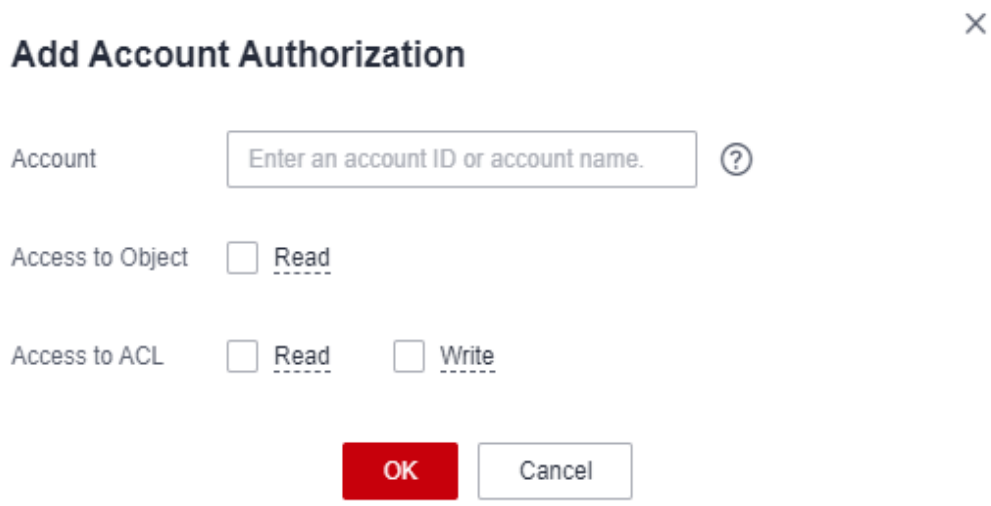
NOTA

Los permisos de ACL para objetos cifrados no se pueden conceder a usuarios registrados o usuarios anónimos.

Paso 5 Haga clic en **Add** para aplicar los permisos de ACL específicos a una cuenta, como se muestra en **Figura 12-14**.

Ingrese un ID de cuenta o nombre de cuenta y establezca permisos de ACL para la cuenta. Puede obtener el ID de cuenta o el nombre de cuenta en la página **My Credentials**.

Figura 12-14 Adición de permisos de ACL para un objeto



Paso 6 Haga clic en **OK**.

----Fin

12.9 Application Cases

12.9.1 Granting an IAM User Permissions to Operate a Specific Bucket

Create an IAM user under in an account. The IAM user has no permission to any resource before it is added to any user group. The bucket owner (root account) or other accounts and

IAM users, who have the permission to set bucket policies, can configure bucket policies to grant the bucket operation permissions to IAM users.

The following is an example about how to grant an IAM user the bucket access and object upload permissions.

Notes

In this example, the authorized IAM user can access the authorized bucket and upload objects to the bucket using OBS Browser+, APIs, or SDKs, but cannot access the bucket on OBS Console. To allow the access through OBS Console, you need to **create a custom policy** to add the IAM user to the user group that has the **obs:bucket:ListAllMyBuckets** permission for all OBS resources. In this way, the IAM user can view the authorized bucket on OBS Console.

Procedure

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 In the navigation pane, choose **Permissions** > **Bucket Policy**.

Paso 4 Click **Create**.

Paso 5 In the first row of the template list, click **Create Custom Policy** on the right.

Paso 6 Configure parameters listed in the table below to grant an IAM user the permissions to access the bucket (to list objects in the bucket) and to upload objects.

Tabla 12-19 Parameters for granting bucket access and object upload permissions

Parameter		Description
Policy View		Visual editor
Policy Name		Enter a custom name.
Policy Content	Effect	Allow
	Principal	● Current account ● Sub-user: Specify IAM users under the current account. ● User Policy: Include specified users.
	Resources	● Select the **Current bucket** and **Object in bucket**, and then select **All objects**. ● Resource Policy: Include specified resources.

Parameter		Description
	Actions	● Select **ListBucket** and **PutObject** actions. ● Operation Strategy: Include selected actions. **NOTA** In this example, only the upload action among object actions is selected. You can also select other object actions to grant corresponding permissions if needed. The asterisk (*) indicates all actions. For details about the supported actions, see **Actions**.

Paso 7 Click **Next** in the lower right corner to confirm the policy configuration.

Paso 8 Click **Create** in the lower right corner.

----Fin

Verification

Verify the preceding permissions on OBS Browser+.

Paso 1 Create an **access key (AK/SK)** of the authorized user on OBS Console.

Paso 2 Open OBS Browser+, enter the obtained AK and SK, and set the **Access Path** to the name of the authorized bucket.

Paso 3 Access requests from unauthorized users are denied.

Paso 4 After being granted the permission to access the bucket, the user can access the bucket on OBS Browser+, with objects in the bucket properly displayed.

Paso 5 Upload an object to the bucket. The upload fails.

Paso 6 After being granted the permission to upload objects, the user can upload objects to the bucket on OBS Browser+, with the uploaded objects properly displayed in the object list.

----Fin

12.9.2 Granting Other Huawei Cloud Accounts Permissions to Operate a Specific Bucket

The bucket owner (root account) or other accounts and IAM users, who have the permission to set bucket policies, can configure bucket policies to grant the bucket operation permissions to other accounts or IAM users under other accounts.

The following is an example about how to grant other accounts bucket access and object upload permissions.

NOTA

To grant permissions to IAM users under other accounts, you need to configure both bucket policies and permisos de IAM.

1. Configure a bucket policy to allow IAM users to access the bucket.
2. Configure permisos de IAM for the account where authorized IAM users belong, to allow the IAM users to access the bucket.

Only permissions that are allowed by both the bucket policy and permisos de IAM can take effect.

Procedure

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 In the navigation pane, choose **Permissions** > **Bucket Policy**.

Paso 4 Click **Create**.

Paso 5 In the first row of the template list, click **Create Custom Policy** on the right.

Paso 6 Configure parameters listed in the table below to grant other accounts the permissions to access the bucket (to list objects in the bucket) and to upload objects.

Tabla 12-20 Parameters for granting bucket access and object upload permissions

Parameter		Description
Policy View		Visual editor
Policy Name		Enter a custom name.
Policy Content	Effect	Allow
	Principal	● Other account ● Enter the account ID and IAM user ID. **NOTA** The account ID and IAM user ID can be obtained on the **My Credentials** page of the account or user to be authorized. The following describes different authorization scenarios: – **Granting permissions to all the other accounts and their IAM users**: Set the account ID and IAM user ID to *. – **Granting permissions to an account**: Enter the desired account ID and IAM user ID. – **Granting permissions to an account and its IAM users**: Enter the desired account ID, and set the IAM user ID to * (indicating all IAM users under the account). – **Granting permissions to certain IAM users**: Enter the desired account ID and one or more IAM users IDs. ● User Policy: Include specified users.

Parameter		Description
	Resources	● Select the **Current bucket** and **Object in bucket**, and then select **All objects**. ● Resource Policy: Include specified resources.
	Actions	● Select **ListBucket** and **PutObject** actions. ● Operation Strategy: Include selected actions. **NOTA** In this example, only the upload action among object actions is selected. You can also select other object actions to grant corresponding permissions if needed. The asterisk (*) indicates all actions. For details about the supported actions, see **Actions**.

Paso 7 Click **Next** in the lower right corner to confirm the policy configuration.

Paso 8 Click **Create** in the lower right corner.

----Fin

Verification

Verify the preceding permissions on OBS Browser+.

Paso 1 Create an **access key (AK/SK)** of the authorized user on OBS Console.

Paso 2 Open OBS Browser+, enter the obtained AK and SK, and set the **Access Path** to the name of the authorized bucket.

Paso 3 Access requests from unauthorized users are denied.

Paso 4 After being granted the permission to access the bucket, the user can access the bucket on OBS Browser+, with objects in the bucket properly displayed.

Paso 5 Upload an object to the bucket. The upload fails.

Paso 6 After being granted the permission to upload objects, the user can upload objects to the bucket on OBS Browser+, with the uploaded objects properly displayed in the object list.

----Fin

12.9.3 Restricting Access to a Bucket to Specific Addresses

You can configure a bucket policy to restrict access to a bucket to specified addresses. This example describes how to deny access from clients whose IP address is in the range of **114.115.1.0/24** to a bucket.

Procedure

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 In the navigation pane, choose **Permissions** > **Bucket Policy**.

Paso 4 Click **Create**.

Paso 5 In the first row of the template list, click **Create Custom Policy** on the right.

Paso 6 Configure parameters listed in the table below.

Tabla 12-21 Restricting access to a bucket to specified addresses

Parameter		Description
Policy View		Visual editor
Policy Name		Enter a custom name.
Policy Content	Effect	Deny
	Principal	● Anonymous user ● User Policy: Include specified users.
	Resources	● Select the **Current bucket** and **Object in bucket**, and then select **All objects**. ● Resource Policy: Include specified resources.
	Actions	● Select ***** (indicating all actions). ● Operation Strategy: Include selected actions.
	Conditions	● **Conditional Operator**: **IpAddress** ● **Key**: **SourceIP** ● **Value**: **114.115.1.0/24**

Paso 7 Click **Next** in the lower right corner to confirm the policy configuration.

Paso 8 Click **Create** in the lower right corner.

----Fin

Verification

Initiate an access request from an IP address in the range of **114.115.1.0/24**. The access is denied. Initiate an access request from an IP address beyond the range of **114.115.1.0/24**. The access is allowed.

Scenario

To allow only a specified IP address to access the OBS bucket, set **Condition Operator** to **NotIpAddress** and specify the allowed IP address as the **Value**.

12.9.4 Limiting the Time When Objects in a Bucket Are Accessible

You can configure the bucket policy to limit the time when objects in a bucket are accessible. In the following example, the access time window is from 2019-03-26T12:00:00Z to 2019-03-26T15:00:00Z.

Procedure

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 In the navigation pane, choose **Permissions** > **Bucket Policy**.

Paso 4 Click **Create**.

Paso 5 In the first row of the template list, click **Create Custom Policy** on the right.

Paso 6 Configure parameters listed in the table below.

Tabla 12-22 Limiting the time when objects in a bucket are accessible

Parameter		Description
Policy View		Visual editor
Policy Name		Enter a custom name.
Policy Content	Effect	Allow
	Principal	● Anonymous user ● User Policy: Include specified users.
	Resources	● Resource scope: Object in bucket. Select **All objects**. ● Resource Policy: Include specified resources. **NOTA** This example only grants permissions for resources in the bucket. If you also want to grant permission for the bucket (for example, the permission to list objects in the bucket), create another custom bucket policy.
	Actions	● Select * (indicating all actions). ● Operation Strategy: Include selected actions. **NOTA** Selecting * may cause resources to be deleted. To avoid this risk, select **Get*** that indicates all read permissions.

Parameter		Description
	Conditions	● Condition 1: – Condition Operator: DateGreaterThan – Key: CurrentTime – Value: 2019-03-26T12:00:00Z (UTC format) ● Condition 2: – Condition Operator: DateLessThan – Key: CurrentTime – Value: 2019-03-26T15:00:00Z (UTC format)

Paso 7 Click **Next** in the lower right corner to confirm the policy configuration.

Paso 8 Click **Create** in the lower right corner.

----Fin

Verification

During the specified time period, any user can access the specified resources in the bucket. Outside the specified time period, only the bucket owner can access the bucket.

12.9.5 Granting Anonymous Users Permission to Access Objects

An enterprise stores a large volume of map data in OBS, and offers the data for public query. This enterprise sets a read permission for anonymous users, and provides the data URLs on the Internet. Then all users can read or download the data through the URLs.

Procedure

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

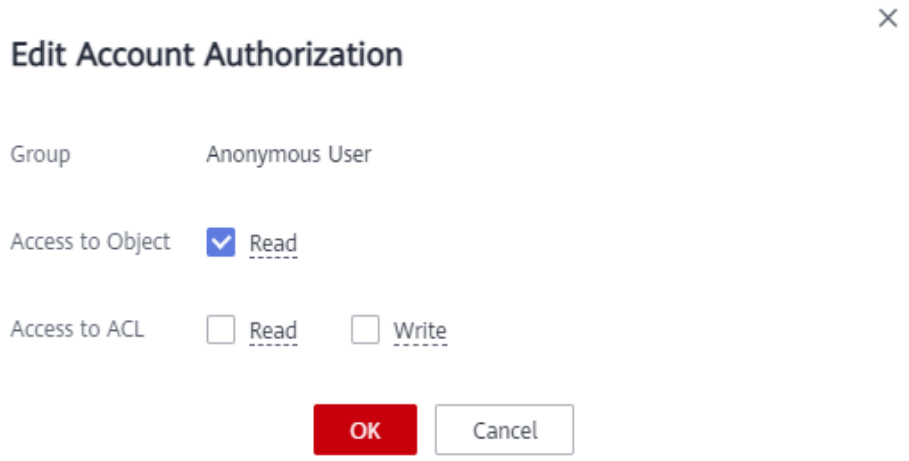
Paso 2 In the upper right corner of the page, click **Create Bucket** to create a bucket.

Paso 3 In the bucket list, click the name of the newly created bucket. On the displayed object management page, upload the map data to the new bucket. The map data is stored as an object.

Paso 4 Click the object name. The object details page is displayed.

Paso 5 Under **Object ACL** > **Public Permissions**, click **Edit** to grant the object read permission for anonymous users, as shown in **Figura 12-15**.

Figura 12-15 Setting an object read permission for anonymous users



Paso 6 Click **OK**.

----Fin

Verification

Paso 1 Click the object. Its URL is displayed under **Link**. Share the URL over the Internet, so that all users can access or download the object through the Internet.

Paso 2 An anonymous user can view the object by copying the URL of the object to the web browser.

----Fin

12.9.6 Granting Anonymous Users Permission to Access Folders

If all objects in a folder need to be accessible to anonymous users, you can configure a bucket policy or an object policy to grant anonymous users the permission to access the folder. In this example, a bucket policy is used. If you want to use an object policy to grant permission, select the target folder and configure an object policy. Parameters in both types of policies are the same.

Procedure

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 In the navigation pane, choose **Permissions** > **Bucket Policy**.

Paso 4 Click **Create**.

Paso 5 In the first row of the template list, click **Create Custom Policy** on the right.

Paso 6 Configure parameters listed in the table below.

Tabla 12-23 Authorizing folder access permissions to anonymous users

Parameter		Description
Policy View		Visual editor
Policy Name		Enter a custom name.
Policy Content	Effect	Allow
	Principal	● Anonymous user ● User Policy: Include specified users.
	Resources	● Resource scope: Object in bucket. Specify objects. ● Resource path: If the folder name is **folder-001**, enter **folder-001/***, indicating all objects in the folder. ● Resource Policy: Include specified resources.
	Actions	● GetObject ● Operation Strategy: Include selected actions.

Paso 7 Click **Next** in the lower right corner to confirm the policy configuration.

Paso 8 Click **Create** in the lower right corner.

----Fin

Verification

Paso 1 After the permission is successfully configured, select an object in the folder and click the object name to view its details. The object link (URL) is displayed on the details page. Share the URL over the Internet, so that all users can access or download the object through the Internet.

Paso 2 An anonymous user can use the URL to access the object in a browser.

----Fin

13 Configuración de lectura directa

Con la lectura directa habilitada para un bucket, puede acceder a los objetos de la clase de almacenamiento Archive sin restaurarlos primero. La descarga o copia de un objeto de Archive incurrirá en tarifas de tráfico por leer directamente el objeto. Para obtener información detallada, consulte **Detalles de los precios de productos**.

Puede habilitar la lectura directa de un bucket durante su creación. Para obtener más información, véase **Creación de un bucket**. Alternativamente, puede habilitar la lectura directa de un bucket creado haciendo lo siguiente:

NOTA

La lectura directa ya está disponible en las siguientes regiones: CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN Southwest-Guiyang1 y AF-Johannesburg.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

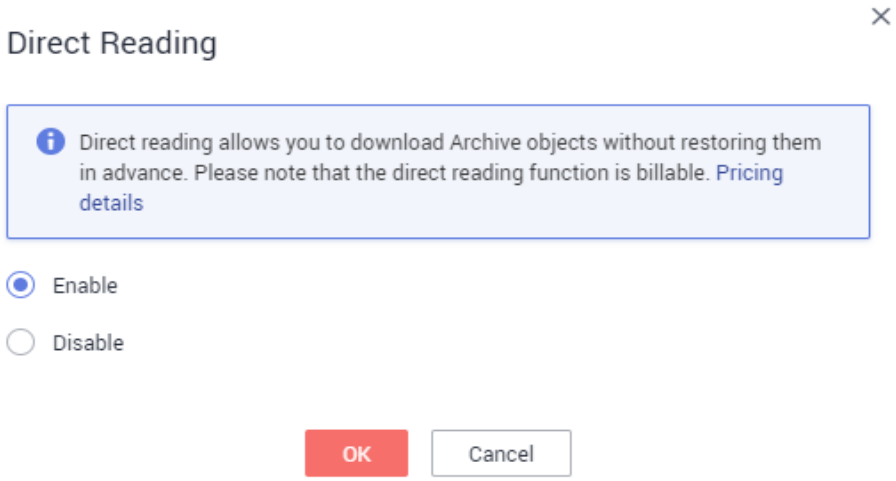
Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Overview**.

Paso 4 En el área **Basic Configurations**, haga clic en **Direct Reading**. Aparece el cuadro de diálogo **Direct Reading**.

Paso 5 Seleccione **Enable**.

Figura 13-1 Habilitar la lectura directa.



Paso 6 Haga clic en **OK**.

----Fin

14 Control de versiones

14.1 Versioning Overview

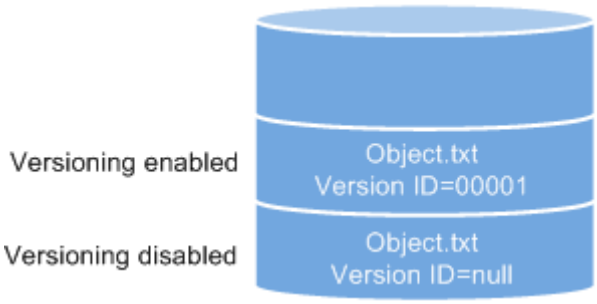
OBS can store multiple versions of an object. You can quickly search for and restore different versions or restore data in the event of accidental deletions or application faults.

By default, the versioning function is disabled for new buckets on OBS. Therefore, if you upload an object to a bucket where an object with the same name exists, the new object will overwrite the existing one.

Enabling Versioning

- Enabling versioning does not change the versions and contents of existing objects in the bucket. The version ID of an object is **null** before versioning is enabled. If a namesake object is uploaded after versioning is enabled, a version ID will be assigned to the object. For details, see **Figura 14-1**.

  Figura 14-1 Versioning (with existing objects)

- OBS automatically allocates a unique version ID to a newly uploaded object. Objects with the same name are stored in OBS with different version IDs.

Figura 14-2 Versioning (for new objects)

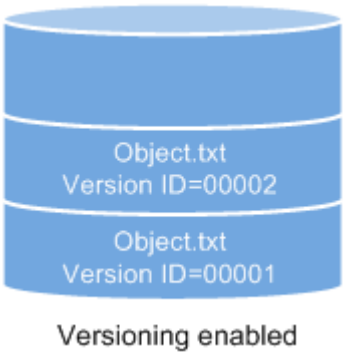
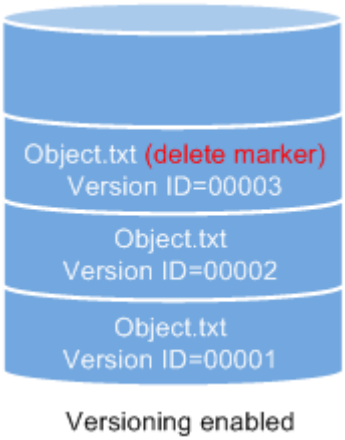


Tabla 14-1 Version description

Version	Description
Latest version	After versioning is enabled, each operation on an object will result in saving of the object with a new version ID. The version ID generated upon the latest operation is called the latest version.
Historical version	After versioning is enabled, each operation on an object will result in saving of the object with a new version ID. Version IDs generated upon operations other than the latest operation are called historical versions.

- The latest objects in a bucket are returned by default after a GET Object request.
- Objects can be downloaded by version IDs. By default, the latest object is downloaded if the version ID is not specified. For details, see **Operaciones relacionadas** in **Configuración del control de versiones**.
- You can select an object and click **Delete** on the right to delete the object. After the object is deleted, OBS generates a **Delete Marker** with a unique version ID for the deleted object, and the deleted object is displayed in the **Deleted Objects** list. For details, see **Eliminación de un objeto o una carpeta**. The 404 error will be returned if attempts are made to access this deleted object.

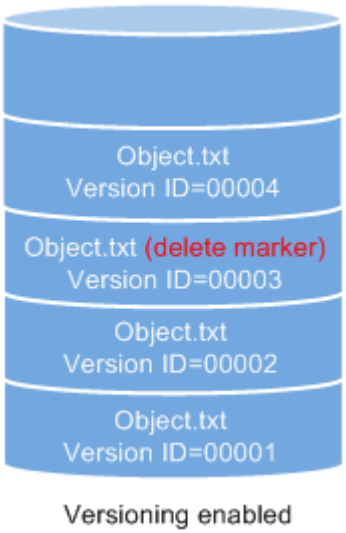
Figura 14-3 Object with a delete marker



- You can recover a deleted object by deleting the delete marker. For details, see **Operaciones relacionadas** in **Recuperación de un objeto**.
- After an object is deleted, you can specify the version number in **Deleted Objects** to permanently delete the object of the specified version. For details, see **Operaciones relacionadas** in **Eliminación de un objeto o una carpeta**.
- An object is displayed either in the object list or the list of deleted objects. It will never be displayed in both the lists at the same time.

  For example, after object **A** is uploaded and deleted, it will be displayed in the **Deleted Objects** list. If you upload an object named **A** again, the object **A** will be displayed in the **Objects** list, and the previously deleted object **A** will no longer be displayed in the **Deleted Objects** list. For details, see **Figura 14-4**.

Figura 14-4 Uploading a namesake object after the original one is deleted

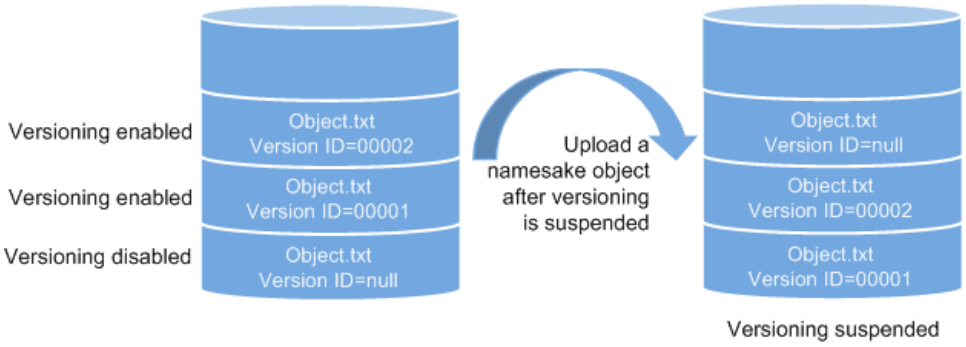


- All object versions except those with **Delete Marker** stored in OBS are charged.

Suspending Versioning

Once the versioning function is enabled, it can be suspended but cannot be disabled. Once versioning is suspended, version IDs will no longer be allocated to newly uploaded objects. If an object with the same name already exists and does not have a version ID, the object will be overwritten.

Figura 14-5 Object versions in the scenario when versioning is suspended



If versions of objects in a bucket do not need to be controlled, you can suspend the versioning function.

- Historical versions will be retained in OBS. If you do not need these historical versions, manually delete them.
- Objects can be downloaded by version IDs. By default, the latest object is downloaded if the version ID is not specified.
- All historical object versions except those with **Delete Marker** stored in OBS are charged.

Differences Between Scenarios When Versioning Is Suspended and Disabled

If you delete an object when versioning is suspended, a **null** version with the **Delete Marker** is generated regardless of whether the object has historical versions. But, if versioning is disabled, the same operation will not generate a version with the **Delete Marker**.

14.2 Configuración del control de versiones

Procedimiento

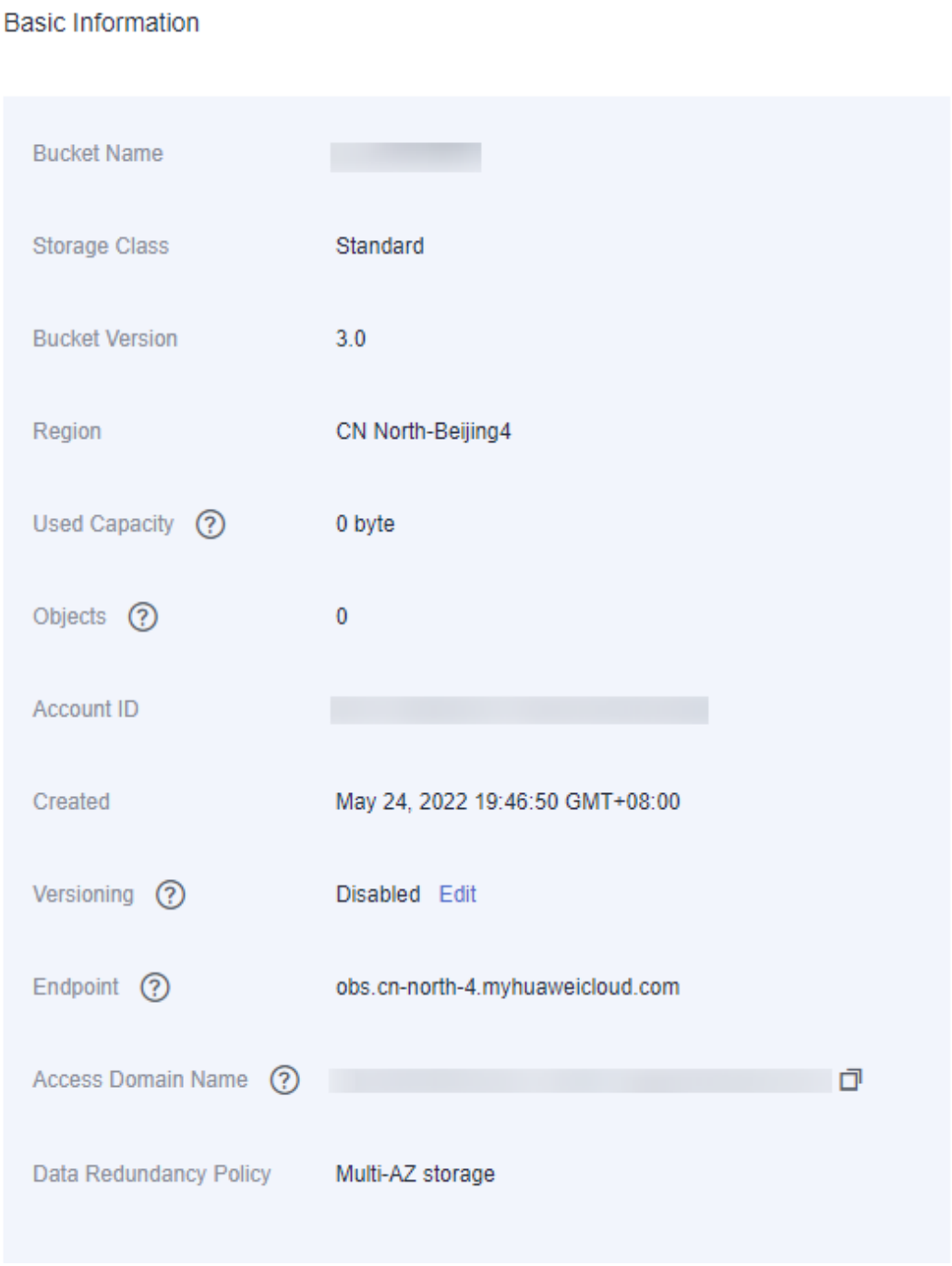
Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Overview**.

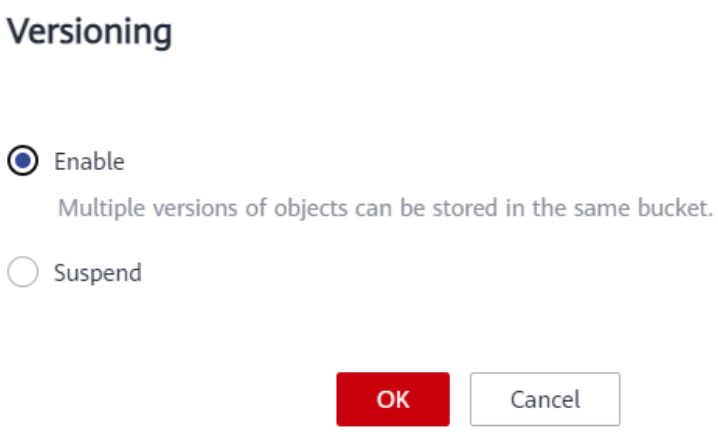
Paso 4 En el área **Basic Information**, busque **Versioning** y haga clic en **Edit**. Aparece el cuadro de diálogo **Versioning**.

Figura 14-6 Edición del estado de control de versiones



Paso 5 Seleccione **Enable**. Para obtener más información, véase **Figura 14-7**.

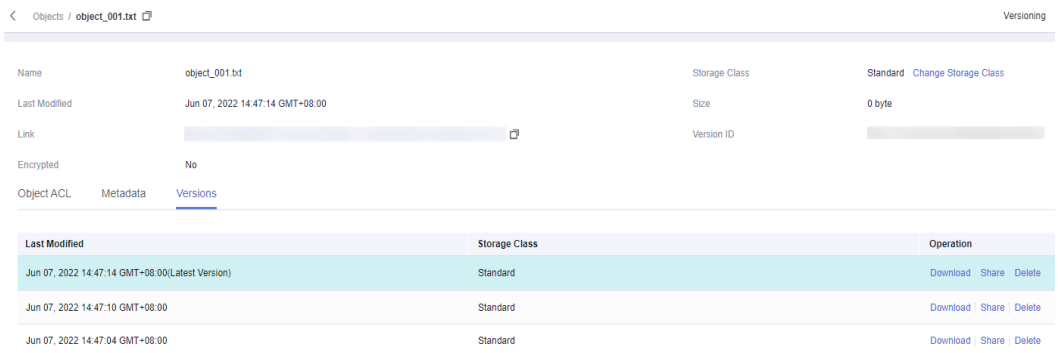
Figura 14-7 Configuración del control de versiones



Paso 6 Haga clic en **OK** para habilitar el control de versiones para el bucket.

Paso 7 Haga clic en un objeto para ir a la página de detalles del objeto. En la ficha **Versions**, vea todas las versiones del objeto.

Figura 14-8 Consulta de versiones de objetos



----Fin

Operaciones relacionadas

Después de habilitar el control de versiones, en la página de detalles del objeto que se muestra, haga clic en **Versions** y, a continuación, puede eliminar y descargar versiones del objeto.

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En la lista de objetos, haga clic en el objeto que desea ir a la página de detalles del objeto.

Paso 4 En la ficha **Versions**, vea todas las versiones del objeto.

Paso 5 Realice las siguientes operaciones en las versiones de objetos:

1. Descargue la versión deseada del objeto haciendo clic en **Download** en la columna **Operation**.

   NOTA

   Si la versión que desea descargar está en la clase de almacenamiento Archive, restáurela primero.

2. Comparta una versión del objeto haciendo clic en **Share** en la columna **Operation**.
3. Para eliminar una versión del objeto, haga clic en **Delete** o **More** > **Delete** en la columna **Operation**. Si elimina la versión más reciente, la versión más reciente se convierte en la versión más reciente.

   NOTA

   Las versiones de objetos con políticas de retención de WORM configuradas no se pueden eliminar de forma permanente durante el período de retención. Si una versión de objeto no tiene ninguna política de retención de WORM configurada, puede eliminarla en la ficha **Versions** de la página de detalles del objeto.

----Fin

15 Registro

15.1 Logging Overview

You can enable logging to facilitate analysis or audit as required. Access logs enable a bucket owner to analyze the property, type, or trend of requests to the bucket in depth. When the logging function of a bucket is enabled, OBS will log access requests for the bucket automatically, and write the generated log files to the specified bucket (target bucket).

AVISO

Uploading bucket logs to the target bucket incurs billable PUT requests. For details about the pricing, see **Requests**.

OBS can record bucket access requests in logs for request analysis and log audit.

Logs occupy some OBS storage space rented by users, causing extra fees. For this reason, OBS does not collect bucket access logs by default.

The log files are generated and uploaded by OBS to the bucket where the logs are stored. Therefore, OBS requires the authorization to upload the generated log files. Therefore, before configuring logging for a bucket, you need to create an IAM agency for OBS and add this agency when configuring logging for the bucket. By default, when configuring permissions for an agency, you only need to grant the agency the permission to upload log files (PutObject) to the bucket for storing log files. In the following example, **mybucketlogs** is the bucket. If the default encryption function is enabled for the log storing bucket, the IAM agency also requires the KMS Administrator permissions in the region where the log storing bucket resides.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "obs:object:PutObject"
            ],
            "Resource": [
                "OBS:*:*:object:mybucketlogs/*"
            ],
            "Effect": "Allow"
```



```
        }
    ]
}
```

After logging is configured, you can view operation logs in the bucket that stores the logs in approximately fifteen minutes.

The following shows an example access log of the target bucket:

```
787f2f92b20943998a4fe2ab75eb09b8 bucket [13/Aug/2015:01:43:42 +0000] xx.xx.xx.xx
787f2f92b20943998a4fe2ab75eb09b8 281599BACAD9376ECE141B842B94535B
REST.GET.BUCKET.LOCATION
- "GET /bucket?location HTTP/1.1" 200 - 211 - 6 6 "-"  "HttpClient" - -
```

The access log of each bucket contains the following information.

Tabla 15-1 Bucket log format

Parameter	Value Example	Description
BucketOwner	787f2f92b20943998a4fe2ab75eb09b8	Account ID of the bucket owner
Bucket	bucket	Name of the bucket
Time	[13/Aug/2015:01:43:42 +0000]	Timestamp of the request (UTC)
Remote IP	xx.xx.xx.xx	IP address from where the request is initiated
Requester	787f2f92b20943998a4fe2ab75eb09b8	Requester ID ● When an account initiates a request, this is the account ID. When an IAM user initiates a request, this is the ID of the account to which the IAM user belongs. ● When a request is initiated by an anonymous user, the value of this parameter is **Anonymous**.
RequestID	281599BACAD9376ECE141B842B94535B	Request ID
Operation	REST.GET.BUCKET.LOCATION	Name of the operation
Key	-	Object name
Request-URI	GET /bucket?location HTTP/1.1	URI of the request

Parameter	Value Example	Description
HTTPStatus	200	Return code
ErrorCode	-	Error code
BytesSent	211	Size of the HTTP response, expressed in bytes
ObjectSize	-	Object size (bytes)
TotalTime	6	Processing time on the server (ms)
Turn-AroundTime	6	Total time for processing the request (ms)
Referer	-	Header field **Referer** of the request
User-Agent	HttpClient	User-Agent header of the request
VersionID	-	Version ID carried in the request
STSLogUrn	-	Federated authentication and agency information
StorageClass	STANDARD_IA	Current storage class of the object
TargetStorageClass	GLACIER	Storage class that the object will be transited to

15.2 Configuración del registro de acceso para un bucket

Una vez que el registro está habilitado para un bucket, OBS convierte automáticamente los registros de bucket en objetos siguiendo las reglas de nomenclatura y escribe los objetos en un bucket de destino.

La carga de registros de bucket en el bucket de destino conlleva solicitudes de PUT facturables. Para obtener más información sobre los precios, consulte **Solicitudes**.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

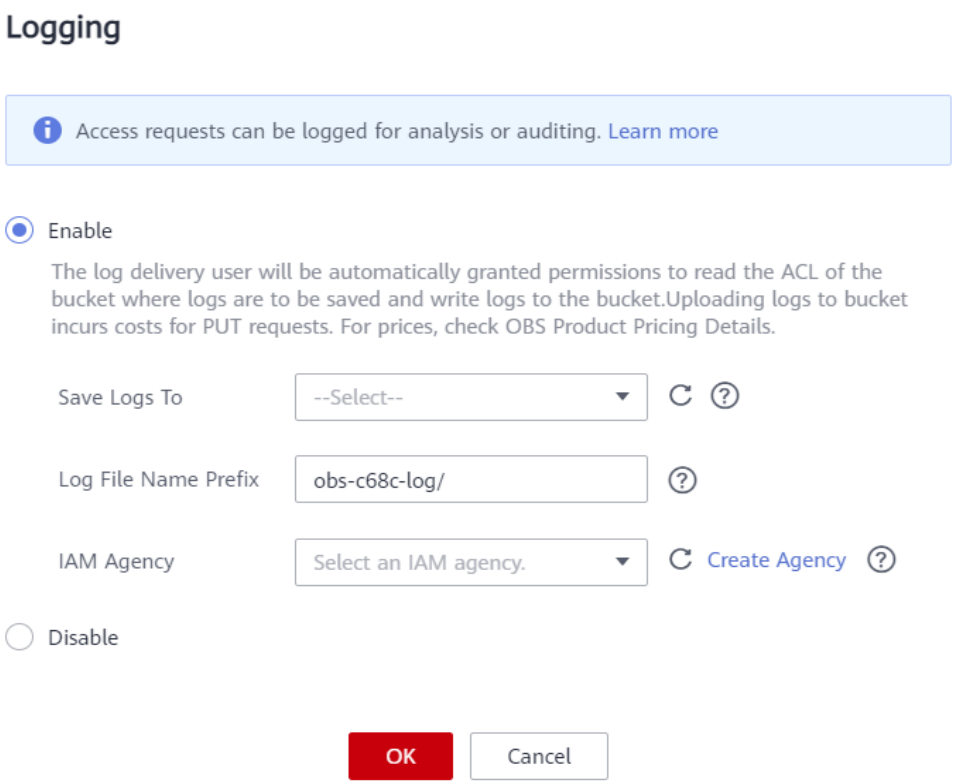
Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Overview**.

Paso 4 En el área **Basic Configurations**, haga clic en **Logging**. Aparece el cuadro de diálogo **Logging**.

Paso 5 Seleccione **Enable**. Para obtener más información, véase **Figura 15-1**.

Figura 15-1 Registro



Paso 6 Seleccione un bucket existente en el que desea almacenar los archivos de registro.

Paso 7 Introduzca un prefijo para el **Log File Name Prefix**.

Después de habilitar el registro, los registros generados se nombran con el siguiente formato:

<*Log File Name Prefix*>YYYY-mm-DD-HH-MM-SS-<*UniqueString*>

- <*Log File Name Prefix*> es el prefijo compartido de los nombres de los archivos de registro.
- **YYYY-mm-DD-HH-MM-SS** indica cuándo se genera el registro.
- <*UniqueString*> indica una string de caracteres generada por OBS.

En OBS Console, si el <*Log File Name Prefix*> configurado termina con una barra diagonal (/), los registros generados en el bucket se almacenan en la carpeta <*Log File Name Prefix*> del bucket, lo que facilita la gestión de los archivos de registro.

Ejemplo:

- Si el bucket denominado **bucket** se utiliza para guardar archivos de registro y el prefijo de nombre de archivo de registro se establece en **bucket-log/**, todos los archivos de

registro entregados a este bucket se guardan en la carpeta **bucket-log**. Un archivo de registro se denomina **2015-06-29-12-22-07-N7MXLAF1BDG7MPDV** de la siguiente manera.

- Si el bucket llamado **bucket** se utiliza para guardar archivos de registro, y el prefijo de nombre de archivo de registro se establece en **bucket-log**, todos los archivos de registro se guardan en el directorio raíz del bucket. Un archivo de registro se denomina **bucket-log2015-06-29-12-22-07-N7MXLAF1BDG7MPDV** de la siguiente manera.

Paso 8 Seleccione una delegación de IAM para conceder a OBS el permiso para cargar archivos de registro en el bucket especificado.

De forma predeterminada, al configurar permisos para una delegación, solo tiene que conceder a la agencia el permiso para cargar archivos de registro (PutObject) en el bucket para almacenar archivos de registro. En el siguiente ejemplo, **mybucketlogs** es el bucket. Si la encriptación predeterminada está habilitada para el bucket de almacenamiento de registro, la delegación de IAM también requiere los permisos de administrador de KMS en la región donde reside el bucket de almacenamiento de registro.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "obs:object:PutObject"
            ],
            "Resource": [
                "OBS:*:*:object:mybucketlogs/*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Puede elegir una delegación de IAM existente en la lista desplegable o hacer clic en **Create Agency** para crear una. Para obtener más información sobre cómo crear una delegación, consulte **Creación de una delegación de IAM**.

Paso 9 Haga clic en **OK**.

Después de configurar el registro, puede ver los registros de operaciones en el bucket que almacena los registros en aproximadamente quince minutos.

----Fin

Operaciones relacionadas

Si no necesita grabar registros, haga clic en **Disable** en el cuadro de diálogo **Logging** y, a continuación, haga clic en **OK**. Después de deshabilitar el registro, los registros no se registran, pero los registros existentes en el depósito de destino se conservarán.

16 Etiquetas

16.1 Descripción general de la etiqueta

Las etiquetas se utilizan para identificar y clasificar los bucket de OBS.

Si agrega etiquetas a un bucket, los registros de detalles de servicio (SDR) generados para él se etiquetarán con estas etiquetas. Puede clasificar los SDR por etiqueta para el análisis de costos. Por ejemplo, si tiene una aplicación que carga sus datos en ejecución en un bucket, puede etiquetar el bucket con el nombre de la aplicación. De esta manera, los costes de la aplicación pueden analizarse usando etiquetas en SDR.

Una etiqueta se describe mediante un par clave-valor. Un bucket puede tener un máximo de 10 etiquetas. Cada etiqueta tiene solo una clave y un valor.

La clave y el valor pueden existir en cualquier orden en una etiqueta. Cada clave es única entre todas las etiquetas de un bucket, mientras que los valores pueden ser repetidos o estar vacíos.

16.2 Configuración de etiquetas para un bucket

Puede agregar etiquetas a un bucket al crear el bucket. Para obtener más información, véase **Creación de un bucket**. También puede agregar etiquetas a un bucket después de que se haya creado. En este tema se describe cómo agregar etiquetas a un bucket una vez creado.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

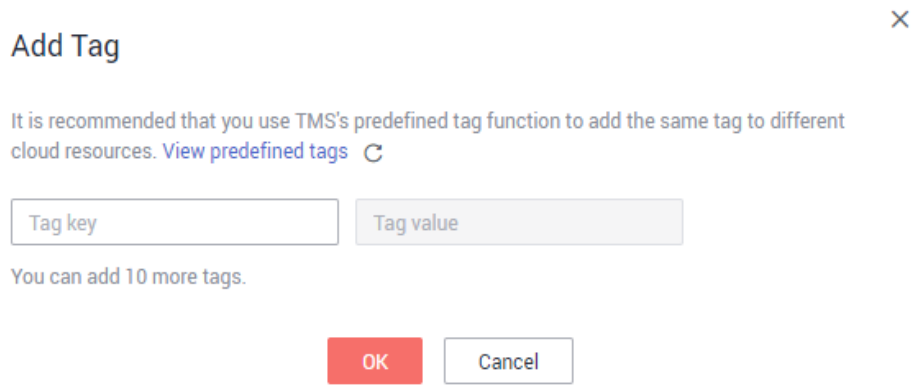
Paso 3 En el panel de navegación, elija **Overview**.

Paso 4 En el área **Basic Configurations**, haga clic en **Tags**.

Alternativamente, puede elegir **Basic Configurations** > **Tagging** en el panel de navegación.

Paso 5 Haga clic en **Add Tag**. Aparece el cuadro de diálogo **Add Tag**. Vea **Figura 16-1** para más detalles.

Figura 16-1 Agregar etiqueta



Paso 6 Establezca la clave y el valor en función de **Tabla 16-1**.

Tabla 16-1 Descripción del parámetro

Parámetro	Descripción
Key	Clave de una etiqueta. Las claves de etiqueta para el mismo bucket deben ser únicas. Puede personalizar las etiquetas o seleccionar las predefinidas en TMS. Una clave de etiqueta: ● Debe contener de 1 a 36 caracteres y distinguir entre mayúsculas y minúsculas. ● No se puede comenzar o terminar con un espacio o contener los siguientes caracteres: =*<>\,|/
Value	Valor de una etiqueta. Un valor de etiqueta puede ser repetitivo o dejarse en blanco. Un valor de etiqueta: ● Puede contener de 0 a 43 caracteres y debe distinguir entre mayúsculas y minúsculas. ● No puede contener los siguientes caracteres:=*<>\,|/

Paso 7 Haga clic en **OK**.

Se tarda aproximadamente 3 minutos para que la etiqueta surta efecto.

----Fin

Operaciones relacionadas

En la lista de etiquetas, haga clic en **Edit** para cambiar el valor de la etiqueta o haga clic en **Delete** para quitar la etiqueta.

17 Configuración de notificaciones de eventos

17.1 SMN-Enabled Event Notifications

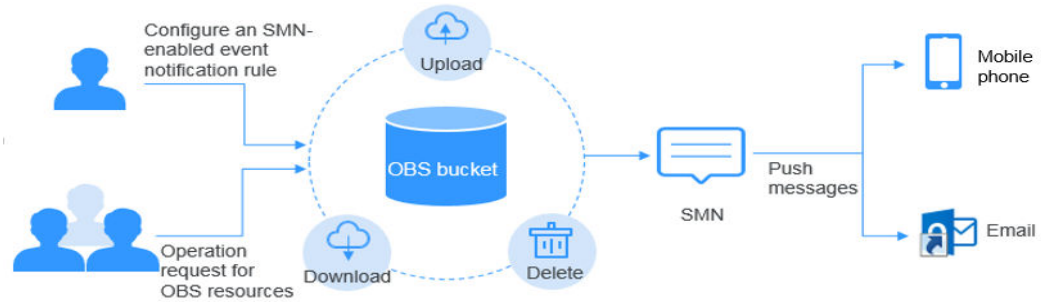
Simple Message Notification (SMN) is a reliable and extensible message notification service that can handle a huge number of messages. It significantly simplifies system coupling and can automatically push messages to endpoints via email or text message.

OBS leverages SMN to provide event notifications. In OBS, you can use SMN to send event notifications to specified subscribers, so that you will be informed of any critical operations (such as upload and deletion) that occur on specified buckets in real time. For example, you can configure an event notification rule to send messages through SMN to the specified email address whenever an upload operation occurs on the specified bucket.

You can configure the event notification rule to filter objects by the object name prefix or suffix. For example, you can add an event notification rule to send notifications whenever an object with the **.jpg** suffix is uploaded to the specified bucket. You can also add an event notification rule to send notifications whenever an object with the **images/** prefix is uploaded to the specified bucket.

For details about events supported by SMN and how to configure an SMN-enabled event notification rule, see **Configuración de la notificación de eventos habilitados para SMN**.

Figura 17-1 SMN-enabled event notification



17.2 Configuración de la notificación de eventos habilitados para SMN

En este tema se describe cómo configurar una regla de notificación de eventos habilitada para SMN en la consola de OBS.

Puede crear reglas de notificación de SMN o replicar reglas de notificación de SMN existentes de un bucket a otro en la misma región.

Información de antecedentes

Para obtener más información, consulte notificaciones de eventos.

Creación de una regla de notificación de SMN

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

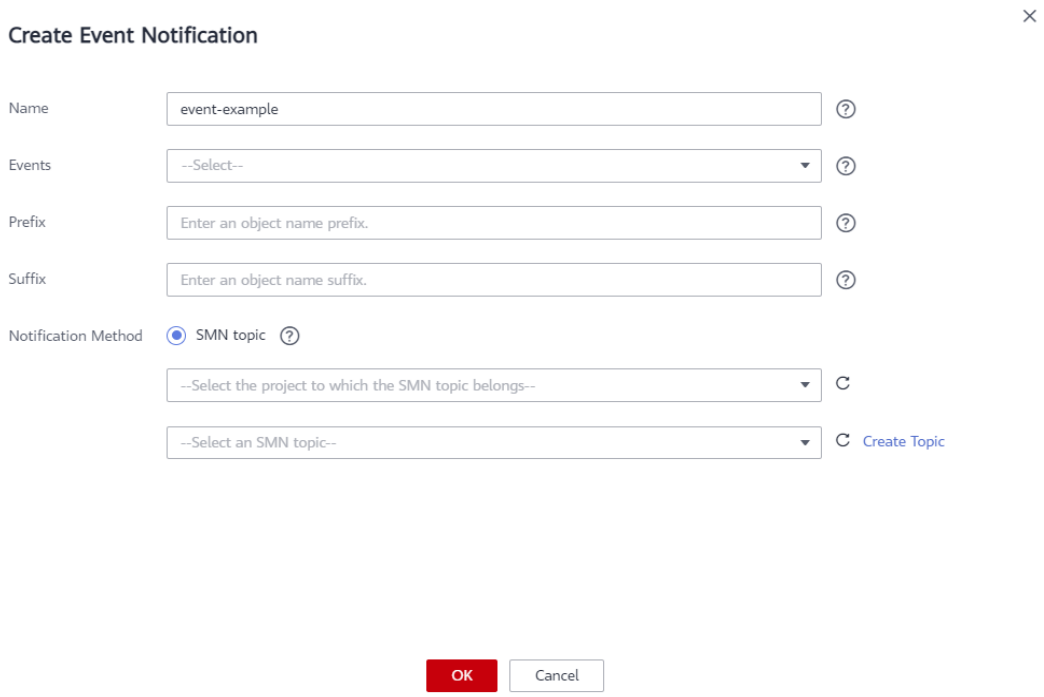
Paso 3 En el panel de navegación, elija **Overview**.

Paso 4 En el área **Basic Configurations**, haga clic en **Event Notification**. Se muestra la página **Event Notification**.

Alternativamente, puede elegir **Basic Configurations** > **Event Notification** en el panel de navegación.

Paso 5 Haga clic en **Create**. Aparece el cuadro de diálogo **Create Event Notification**. Vea **Figura 17-2** para más detalles.

Figura 17-2 Creación de una regla de notificación de evento



Paso 6 Configure los parámetros de notificación de eventos, como se describe en **Tabla 17-1**.

Tabla 17-1 Parámetros de notificación de eventos

Parámetro	Descripción
Name	Nombre del evento. Si el nombre del evento se deja en blanco, el sistema asignará automáticamente un ID único globalmente.
Events	Varios tipos de eventos. Actualmente, OBS admite la notificación de eventos para los siguientes tipos de eventos: ● **ObjectCreated**: Indica todo tipo de operaciones de creación de objetos, incluidos PUT, POST y COPY de objetos, así como la fusión de partes. – **Put**: Crea o sobrescribe un objeto mediante el método PUT. – **Post**: Crea o sobrescribe un objeto utilizando el método POST (subida basada en navegador). – **Copy**: Crea o sobrescribe un objeto mediante el método COPY. – **CompleteMultipartUpload**: Combina partes de una carga de varias partes. ● **ObjectRemoved**: Borra un objeto. – **Delete**: Elimina un objeto con un ID de versión especificado. – **DeleteMarkerCreated**: Elimina un objeto sin especificar un ID de versión. Se pueden aplicar varios tipos de eventos al mismo objeto. Por ejemplo, si ha seleccionado **Put**, **Copy** y **Delete** en la misma regla de notificación de evento, se le enviará una notificación cuando el objeto especificado se cargue, se copia o se elimine del bucket. **ObjectCreated** contiene **Put**, **Post**, **Copy** y **CompleteMultipartUpload**. Si selecciona **ObjectCreated**, los eventos que contiene **ObjectCreated** se seleccionan automáticamente. Del mismo modo, si selecciona **ObjectRemoved**, **Delete** y **DeleteMarkerCreated** se seleccionan automáticamente.
Prefix	Prefijo de nombre de objeto para el que se activarán las notificaciones. **NOTA** Si no se configura ni **Prefix** ni **Suffix**, la regla de notificación de eventos se aplica a todos los objetos del bucket.

Parámetro	Descripción
Suffix	Sufijo de nombre de objeto para el que se activarán las notificaciones. **NOTA** ● Una ruta de carpeta termina con una barra diagonal (/). Por lo tanto, si desea configurar la notificación de evento para las operaciones en carpetas y necesita filtrar las carpetas por sufijo, el sufijo también debe terminar con una barra diagonal (/). ● Si no se configura ni **Prefix** ni **Suffix**, la regla de notificación de eventos se aplica a todos los objetos del bucket.
SMN Topic	Proyecto: El proyecto que contiene el tema SMN que desea seleccionar. Los proyectos se utilizan para gestionar y clasificar recursos en la nube, incluidos los temas de SMN. Cada proyecto contiene diferentes temas de SMN. Seleccione primero un proyecto y, a continuación, un tema.
	Tema: especifica el tema SMN que autoriza a OBS a publicar mensajes. Puede crear estos temas en la consola de gestión de SMN. **NOTA** ● Una vez que se seleccionan los temas de SMN para enviar notificaciones de eventos de OBS, no los elimine ni cancele sus autorizaciones a OBS. ● Si se eliminan los temas o se cancelan sus autorizaciones a OBS, pueden producirse las siguientes condiciones: a. El suscriptor del tema no puede recibir mensajes. b. Las notificaciones de eventos asociadas a temas no disponibles se borran automáticamente. ● Para obtener más información sobre cómo usar SMN, consulte **Creación de un tema** , **Adición de una suscripción** y **Configuración de políticas de tema** en la *Guía de usuario de Simple Message Notification*.

Paso 7 Haga clic en **OK**.

----Fin

Replicating SMN Notification Rules

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Overview**.

Paso 4 In the **Basic Configurations** area, click **Event Notification**. The **Event Notification** page is displayed.

Alternatively, you can choose **Basic Configurations** > **Event Notification** in the navigation pane.

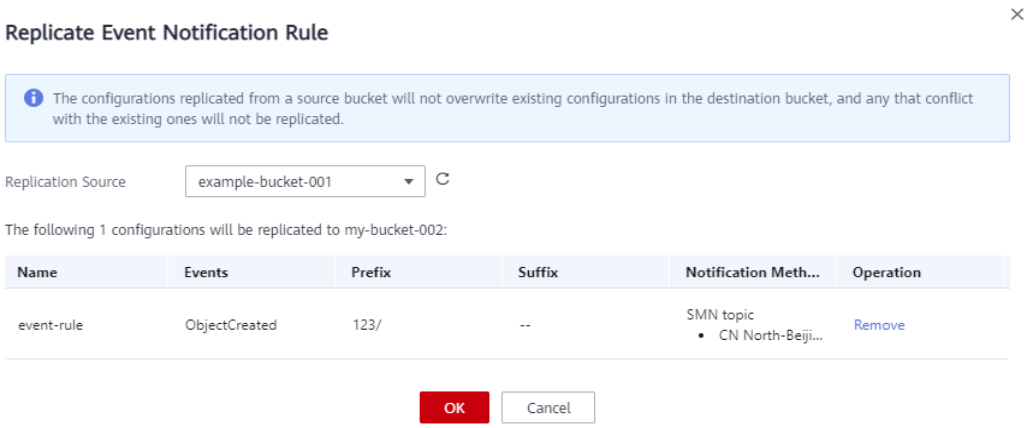
Paso 5 Click **Replicate**.

Paso 6 Select a replication source, that is, the source bucket for which the SMN notification rules were configured.

NOTA

- The notification rules replicated from a source bucket will not overwrite existing rules in the destination bucket, and any that conflict with the existing ones will not be replicated.
- The version of both the source and destination buckets must be 3.0.
- The source and destination buckets must be in the same region.
- You can remove the rules that you do not want to replicate.

Figura 17-3 Replicating SMN notification rules



Paso 7 Click **OK** to replicate the rules to the destination bucket.

----Fin

Operaciones relacionadas

Puede hacer clic en **Edit** en la columna **Operation** de una regla de notificación de evento, para editar la regla de notificación o hacer clic en **Delete** para eliminar la regla.

Si desea eliminar por lotes las reglas de notificación de eventos, selecciónelas y haga clic en **Delete** encima de la lista.

17.3 Application Example: Configuring SMN-Enabled Event Notification

Background Information

An enterprise has a large number of files to archive but it does not want to cost much on storage resources. Therefore, the enterprise subscribes to OBS for storing daily files and expects that an employee can be informed of every operation performed on OBS via email.

Procedure

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

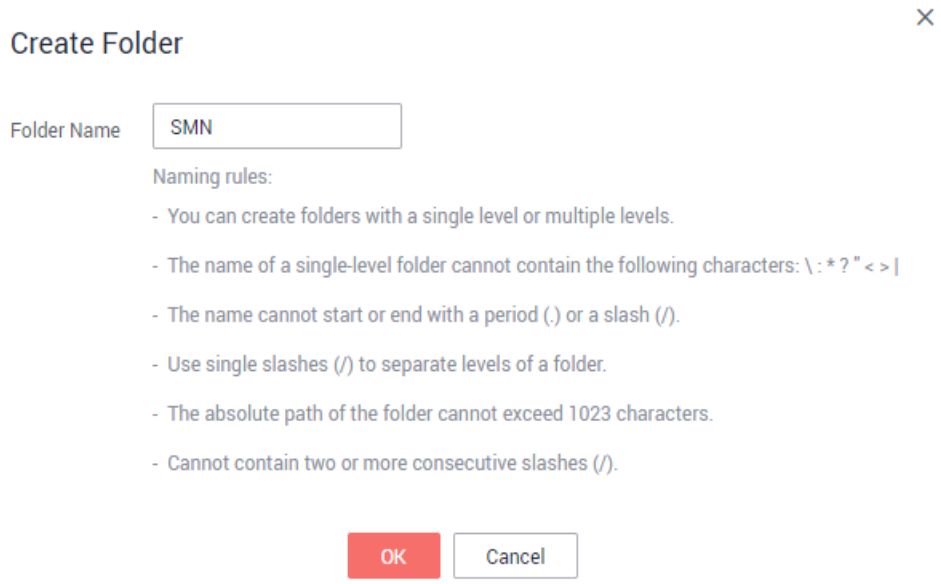
Paso 2 Create a bucket.

Click **Create Bucket** in the upper right corner of the page. On the page, select a region and storage class, and specify a bucket name and other parameters. Then, click **Create Now**.

Paso 3 Create a folder.

Click the bucket created in **Step 2** to go to the **Overview** page. Choose **Objects** > **Create Folder**, enter a folder name, and click **OK**, as shown in **Figura 17-4**. In the following example, **SMN** is the folder name.

Figura 17-4 Creating a folder



Paso 4 In the upper left corner of the page, click ☰ and choose **Simple Message Notification**. On the displayed SMN page, create a topic.

In the following example, **TestTopic** is the SMN topic and the notifications are sent via email.

Use SMN to create a notification topic for OBS as follows:

1. Create an SMN topic.
2. Add a subscription.
3. Modify the topic policy. On the **Configure Topic Policy** page, select **OBS** under **Services that can publish messages to this topic**.

Paso 5 Go back to OBS Console.

Paso 6 Configure an event notification rule.

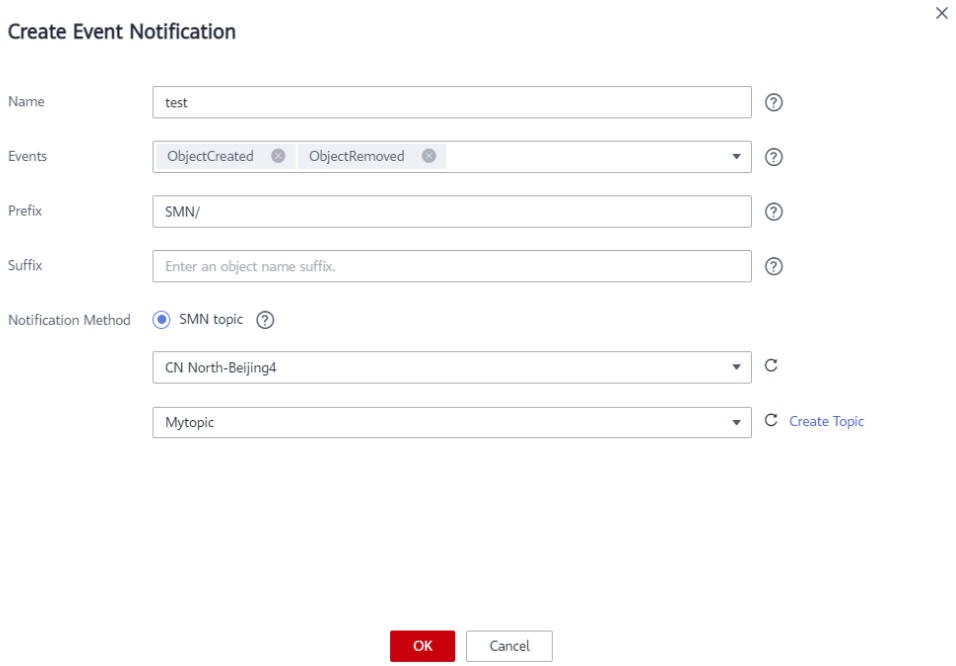
1. In the bucket list, click the bucket that you have created in **Paso 2**.
2. In the navigation pane, choose **Basic Configurations** > **Event Notification**. The **Event Notification** page is displayed.
3. Click **Create**. The **Create Event Notification** dialog box is displayed.

4. Configure event notification parameters, as shown in **Figura 17-5**. After the notification is configured, an employee will be informed of all specified operations on the **SMN** folder in bucket **testbucket**. For details about the parameters, see **Tabla 17-1**.

   NOTA

   – Una ruta de carpeta termina con una barra diagonal (/). Por lo tanto, si desea configurar la notificación de evento para las operaciones en carpetas y necesita filtrar las carpetas por sufijo, el sufijo también debe terminar con una barra diagonal (/).
   – Si no se configura ni **Prefix** ni **Suffix**, la regla de notificación de eventos se aplica a todos los objetos del bucket.

Figura 17-5 Adding an event notification rule



----Fin

Verification

Paso 1 Log in to OBS Console as an enterprise user.

Paso 2 Upload the **test.txt** file to the folder created in **Step 3**.

After the file is uploaded, an employee receives an email. Keyword **ObjectCreated:Post** in the email indicates that the object is successfully uploaded.

Paso 3 Delete the **test.txt** file uploaded in **Step 2**.

After the file is successfully deleted, an employee will receive an email. Keyword **ObjectRemoved:Delete** in the email indicates that the object is successfully deleted.

----Fin

18 Replicación entre regiones

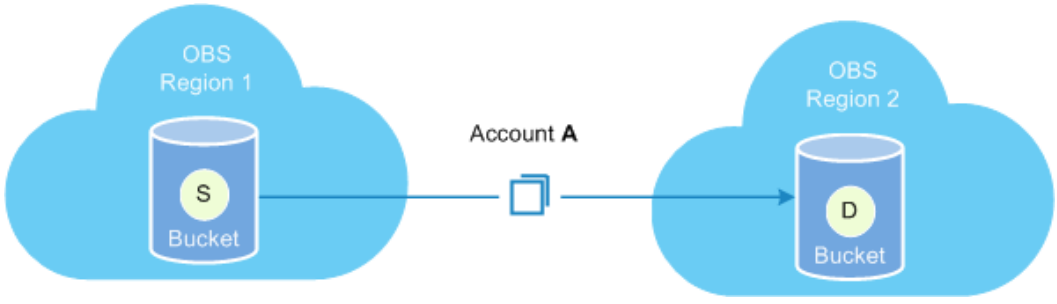
18.1 Cross-Region Replication Overview

OBS offers disaster recovery across regions, catering to your needs for remote backup.

Cross-region replication refers to the process of automatically and asynchronously replicating data from a source bucket in one region to a destination bucket in another region based on the created replication rule. Source and destination buckets must belong to the same account. Replication across accounts is currently not supported.

You can configure a rule to replicate only objects with a specified prefix or replicate all objects in a bucket. Replicated objects in the destination bucket are copies of those in the source bucket. Objects in both buckets have the same name and metadata (including the content, size, last modification time, creator, version ID, custom metadata, and ACL). By default, the storage class of the replicated object is the same as that of the source object. You can also specify a storage class for the replicated object.

Figura 18-1 Cross-region replication



Contents Replicated

After the cross-region replication rule is enabled, objects that meet the following conditions are copied to the destination bucket:

- Newly uploaded objects (excluding objects in the Archive storage class)
- Updated objects, for example, objects whose content or ACL information is updated
- Historical objects in a bucket (The function of synchronizing existing objects must be enabled.)

Application Scenarios

- The same OBS resources need to be accessed in different locations. To minimize the access latency, you can use cross-region replication to create object copies in the nearest region.
- Due to business reasons, you need to migrate OBS data to the data center in another region.
- To ensure data security and availability, you need to create explicit backups for all data written to OBS in the data center of another region. Therefore, secure backup data is available if the source data is damaged irrevocably.

Limitations and Constraints

Cross-region replication has the following limitations and constraints:

- Currently, only buckets of version 3.0 support cross-region replication. To check the bucket version, go to the **Overview** page of the bucket on OBS Console. Then you can view the bucket version in the **Basic Information** area.
- By default, objects uploaded before cross-region replication is enabled are not replicated to the destination bucket unless the function for synchronizing existing objects is enabled.
- The source bucket and the destination bucket must belong to different regions separately. Data cannot be copied between buckets in the same region.
- Objects cannot be copied from the source bucket to the destination bucket if they are in the Archive storage class.
- If the region where the destination bucket resides does not support the storage classes, object copies will be stored in the standard storage class.
- The versioning status of the source bucket must be the same as that of the destination bucket.
- Objects in a source bucket can be copied to only one destination bucket, and cannot be copied again from the destination bucket to another bucket. For example, bucket A and bucket B are in two different regions. You can copy data from bucket A to bucket B or the other way round. However, data copies in either bucket A or bucket B cannot be replicated anymore.
- Object deletion actions made on the source bucket are usually not synchronized to the destination bucket. The object deletion synchronization will happen only when both the source and destination buckets have versioning enabled and you delete an object from the source bucket without specifying a version.
- If you change the versioning status of the destination bucket when cross-region replication is enabled, the replication of objects will fail. If you want to change the versioning status of the source bucket, disable the cross-region replication first, and then make the change.
- Ensure that owners of the source and destination buckets have the read and write permissions to the two buckets. Otherwise, data cannot be synchronized. If the system does not have the permissions to read the source bucket or write the destination bucket due to read/write permission errors, objects cannot be copied successfully, and such replication will not be resumed even if the permission error is rectified.
- For a source bucket, you can create only one cross-region replication rule that applies to the whole bucket for replication of all objects in the bucket. However, you can create a maximum of 100 cross-region replication rules based on object prefixes for the replication of objects that match the prefixes.

- OBS currently only supports the replication between one source bucket and one destination bucket. Replication from one source bucket to multiple destination buckets is not supported. The destination bucket can be modified. However, modifying the destination bucket will change the destination bucket of all existing rules.
- If you delete the OBS agency when the cross-region replication is enabled, the replication will be in the FAILED status.
- Do not delete, overwrite object replicas in the destination bucket, or modify their ACLs, which may cause inconsistency of latest object versions or permission control settings between the destination bucket and the source bucket.
- If the function for synchronizing existing objects is enabled, modifying the cross-region replication configuration may cause failures in synchronizing existing objects. Therefore, do not modify the cross-region replication configuration before the synchronization finishes.
- If cross-region replication is enabled, data cannot be added to the end of objects in the source bucket.
- After a replication with **Synchronize Existing Objects** enabled is complete, if the replication policy keeps unchanged, any ACL changes of source objects will be synchronized to object copies. However, ACL changes of source historical objects will not be synchronized to the copies of historical objects.

18.2 Configuración de la replicación entre regiones

Actualmente, OBS permite configurar una regla de replicación entre regiones para copiar todos los objetos de un bucket de origen a un bucket de destino o varias reglas de replicación entre regiones que coincidan con prefijos.

NOTA

Una regla de replicación entre regiones puede no surtir efecto inmediatamente después de su configuración. Por consiguiente, los objetos a los que se aplica esta regla pueden no replicarse inmediatamente después de configurar la regla.

Los buckets con WORM habilitado no admiten la replicación entre regiones.

Requisitos previos

La versión del bucket de origen es 3.0 o posterior, y la replicación entre regiones está disponible en la región del bucket de origen. Para obtener detalles acerca de la compatibilidad con la replicación entre regiones en cada región, busque "cross-region replication" (replicación entre regiones) en la página **Descripción de funciones**.

Procedimiento

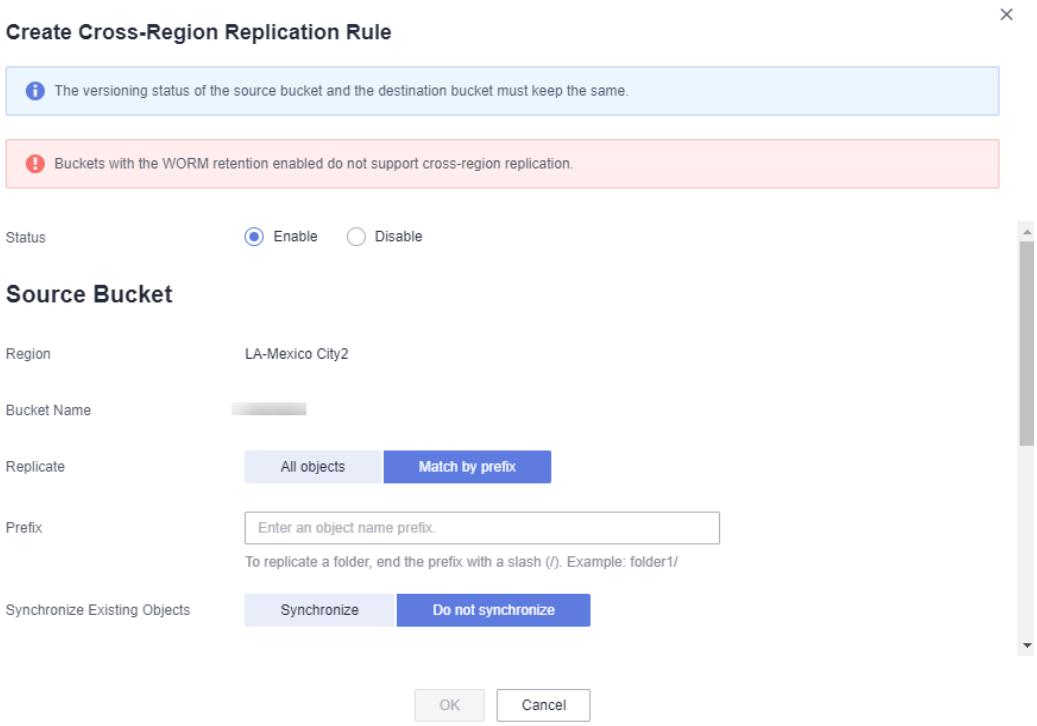
Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, haga clic en **Cross-Region Replication**.

Paso 4 Haga clic en **Create Rule**. Aparece el cuadro de diálogo **Create Cross-Region Replication Rule**. Véase **Figura 18-2**.

Figura 18-2 Creación de una regla de replicación entre regiones



NOTA

- El estado de control de versiones del bucket de origen debe ser el mismo que el del bucket de destino.
- Para un bucket de origen, solo se puede configurar un bucket de destino y una delegación de IAM para la replicación entre regiones. El bucket de destino y la IAM Agency creados en una regla posterior sobrescribirán los de la regla anterior.

Paso 5 Configure una regla de replicación entre regiones según sus necesidades de servicio. Para obtener más información sobre los parámetros, consulte **Tabla 18-1**.

Tabla 18-1 Parámetros de replicación entre regiones

Parámetro		Descripción
Status		Indica si se debe habilitar o deshabilitar la regla de replicación. El estado de control de versiones del bucket de origen debe ser el mismo que el del bucket de destino.
Source bucket	Replicate	Indica los objetos en los que la regla tiene efecto. ● **All objects**: La regla se aplica a todos los objetos del bucket. ● **Match by prefix**: La regla solo se aplica a los objetos con el prefijo preestablecido.

Parámetro		Descripción
	Prefix	● Si desea aplicar la regla a los objetos por prefijo, debe establecer un valor no superior a 1024 caracteres para **Prefix**. ● Cuando se selecciona **Match by prefix** y el prefijo especificado se superpone con el prefijo de una regla existente, OBS considera las dos reglas como una y la nueva no se puede configurar correctamente. Por ejemplo, si existe una regla con el prefijo **abc** en el sistema, no se puede configurar otra regla cuyo prefijo comience por **abc**. ● Para copiar una carpeta, termine el prefijo con una barra diagonal (/), por ejemplo, **imgs/**.
	Synchronize Existing Objects	Indica si se deben sincronizar los objetos que ya estaban en el bucket antes de la configuración de la regla con el bucket de destino. De forma predeterminada, estos objetos no están sincronizados.
	Replicate KMS encrypted objects	OBS intentará copiar los objetos cifrados de KMS sin importar si esta opción está seleccionada o no. ● Si esta opción está seleccionada, sólo las delegaciones de IAM que tienen los permisos **KMS Administrator** en los extremos de origen y destino se muestran en la lista desplegable de **IAM Agency** en este cuadro de diálogo. ● Si esta opción no está seleccionada, sólo las delegaciones de IAM que no tienen el permiso **KMS Administrator** en el extremo de origen o destino se muestran en la lista desplegable de **IAM Agency** en este cuadro de diálogo. Si KMS no está disponible en la región de destino o la delegación no tiene los permisos **KMS Administrator** en las regiones de origen y destino, los objetos cifrados de KMS en el bucket de origen no se replicarán en el bucket de destino y el estado de replicación de objetos será FAILED. Después de que un objeto cifrado en KMS en el bucket de origen se replica en el bucket de destino, la clave para cifrar la copia de objeto cambia a la clave predeterminada **obs/default** de la región donde se encuentra el bucket de destino.
Destination bucket	Region	Indica la región del bucket de destino. Los bucket de destino y de origen deben estar en diferentes regiones.
	Bucket	Indica el bucket de destino.

Parámetro		Descripción
	Change storage class for replicated objects	De forma predeterminada, esta opción no está seleccionada, lo que indica que la clase de almacenamiento de las copias de objetos es la misma que la de los objetos del bucket de origen. Si necesita cambiar la clase de almacenamiento de copias de objetos, seleccione este parámetro y, a continuación, puede especificar una clase de almacenamiento.
Permissions	IAM Agency	Delega a OBS para que opere sus recursos, de modo que OBS pueda utilizar esta delegación para implementar la replicación entre regiones. Se requiere una delegación de IAM para utilizar la función de replicación entre regiones. Cree uno si no tiene ninguna delegación de IAM. Si ya ha creado delegaciones de IAM, seleccione una de la lista desplegable. **NOTA** Requerimientos: La delegación de IAM debe ser de OBS. El proyecto de OBS debe tener los permisos de **Tenant Administrator**. Si se selecciona **Replicate KMS encrypted objects**, también necesitará los permisos de **KMS Administrator** en las regiones donde se encuentran los bucket de origen y de destino.

Paso 6 (Opcional) Cree una IAM Agency. Para obtener más información, véase **Creación de una delegación de IAM**.

Paso 7 Haga clic en **OK**. Se crea la regla de replicación entre regiones.

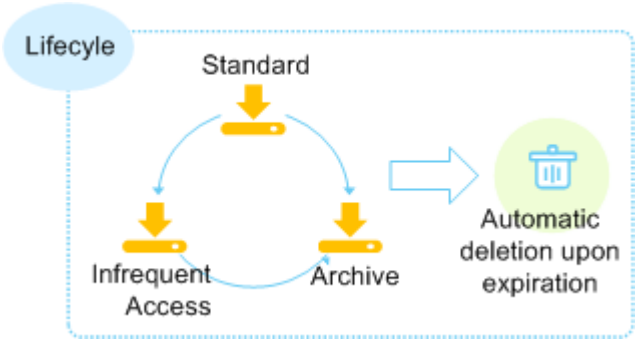
----Fin

19 Gestión del ciclo de vida

19.1 Lifecycle Management Overview

Lifecycle management means periodically deleting objects in a bucket or transitioning between object storage classes by configuring rules.

Figura 19-1 Lifecycle management



You may configure lifecycle rules to:

- Periodically delete logs that are only meant to be retained for a specific period of time (a week or a month).
- Transition documents that are seldom accessed to the Infrequent Access or Archive storage class or delete them.

You can define lifecycle rules for identifying objects and manage lifecycles of the objects based on the rules.

Objects that are no longer frequently accessed can be transitioned to **Infrequent Access** or **Archive**, saving your costs. In short, transition basically means that the object storage class is altered without copying the object. You can also manually change the storage class of an object on the **Objects** page. For details, see **Carga de un objeto**.

Lifecycle rules have two key elements:

- Configuration policy:

You can also specify the prefix of object names so that objects whose names have this prefix are restricted by the rules. You can configure a lifecycle rule for a bucket so that all objects in the bucket can be restricted by the lifecycle rule.

- Time: You can specify the number of days after which objects that have been last updated and meet specified conditions are automatically transitioned to **Infrequent Access**, **Archive**, or expire and are then automatically deleted.
  - **Transition to Infrequent Access**: You can specify the number of days after which objects that have been last updated and meet specified conditions are automatically transitioned to **Infrequent Access**.
  - **Transition to Archive**: You can specify the number of days after which objects that have been last updated and meet specified conditions are automatically transitioned to **Archive**.
  - Expiration time: You can specify the number of days after which objects are automatically deleted or the day after which an object that matches with a rule is deleted.

19.2 Configuración de una regla de ciclo de vida

Una regla de ciclo de vida se puede aplicar a un bucket o a un conjunto de objetos. Puede definir una regla de ciclo de vida para pasar objetos de una clase de almacenamiento a otra:

- De Standard a Infrequent Access o a Archive
- De Infrequent Access a Archive

Los objetos de Archive no se pueden pasar a otras clases de almacenamiento mediante una regla de ciclo de vida.

También puede configurar los objetos para que se eliminen automáticamente después de que caduquen.

Además de crear nuevas reglas de ciclo de vida, puede replicar las reglas de ciclo de vida existentes desde otro bucket.

NOTA

Una regla de ciclo de vida puede cambiar la clase de almacenamiento de una versión de objeto protegida por WORM, pero no puede eliminar la versión de objeto.

Creación de una regla de ciclo de vida

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

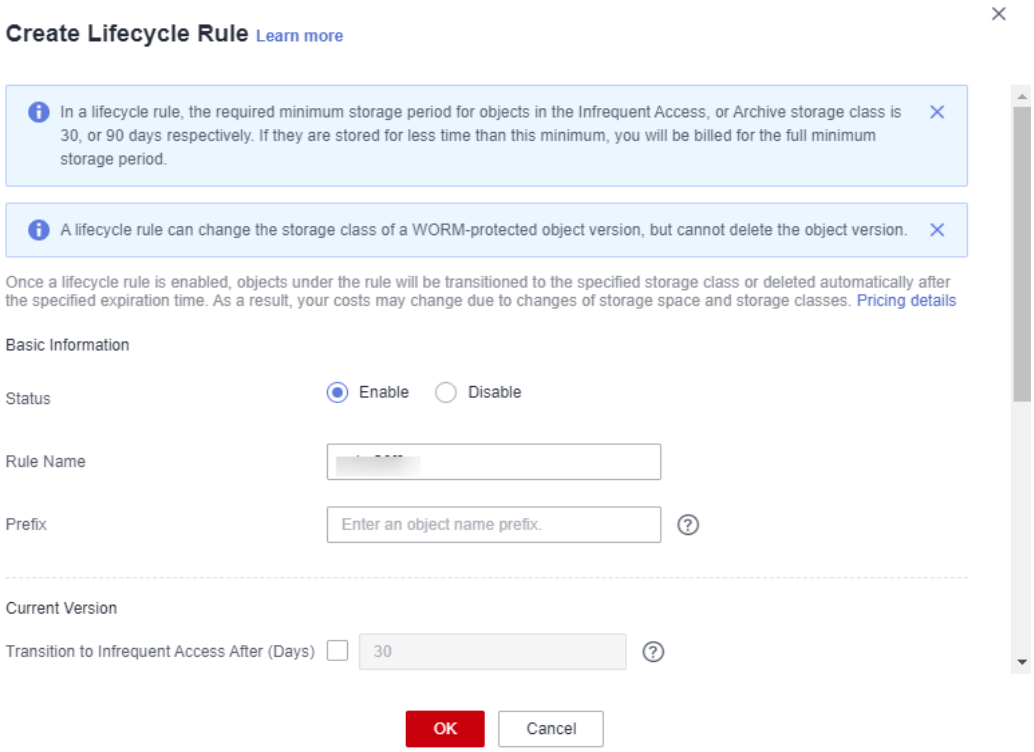
Paso 3 En el panel de navegación, elija **Overview**.

Paso 4 En el área **Basic Configurations**, haga clic en **Lifecycle Rules**. Se muestra la página **Lifecycle Rules**.

También puede elegir **Basic Configurations** > **Lifecycle Rules** en el panel de navegación.

Paso 5 Haga clic en **Create**. Se muestra un cuadro de diálogo que se muestra en **Figura 19-2**.

Figura 19-2 Creación de una regla de ciclo de vida



Paso 6 Configure una regla de ciclo de vida.

Información básica:

- **Status**:

  Seleccione **Enable** para activar la regla del ciclo de vida.

- **Rule Name**:

  Identifique las reglas del ciclo de vida. El **Rule Name** contiene un máximo de 255 caracteres.

- **Prefix**: Es opcional.
  - Si este campo está configurado, los objetos con el prefijo especificado serán gestionados por la regla de ciclo de vida. El prefijo no puede comenzar con una barra (/) o contener dos barras diagonales consecutivas (//), y no puede contener el siguiente characters especiales: **\:*?"<>|**
  - Si este campo no está configurado, todos los objetos del bucket serán gestionados por la regla del ciclo de vida.

NOTA

- Cuando se selecciona **Object name prefix** y el prefijo especificado y el prefijo de una regla de ciclo de vida existente se superponen, OBS considera las dos reglas como una y deshabilita la que se va a configurar. Por ejemplo, si existe una regla con el prefijo **abc** en el sistema, no se puede configurar otra regla cuyo prefijo comience por **abc**.
- Si se ha configurado una regla de ciclo de vida cuyo **Applies To** está establecido en **Object name prefix**, no se puede configurar una regla de ciclo de vida cuyo **Applies To** está establecido en **Bucket**.

Current Version o **Historical Version**:

NOTA

- **Versión actual** y **Versión histórica** son dos conceptos para **Control de versiones**. Si **Versioning** está habilitado, cargar objetos con el mismo nombre en la misma ruta genera diferentes versiones. El objeto cargado por última vez se llama **Versión actual** y el objeto cargado anteriormente se llama **Versión histórica**. Para obtener más información, consulte **Control de versiones**.
- Puede configurar la **Versión actual** o la **Versión histórica** o ambas.

- **Transition to Infrequent Access After (Days)**: Después de este número de días desde la última actualización, los objetos que cumplan determinadas condiciones pasarán a Infrequent Access. Este número debe ser al menos 30.
- **Transition to Archive After (Days)**: Después de este número de días desde la última actualización, los objetos que cumplan determinadas condiciones se pasarán a Archive. Si configura la transición de objetos primero a Infrequent Access y después Archive, los objetos deben permanecer en Infrequent Access al menos 30 días antes de poder pasar a Archive. Si sólo se utiliza la transición a Archive, pero la transición a Infrequent Access no, no hay límite en el número de días para la transición.
- **Delete Objects After (Days)**: Después de este número de días desde la última actualización, los objetos que cumplan determinadas condiciones caducarán y, a continuación, se eliminarán. El número establecido aquí debe ser mayor que el especificado para cualquiera de las operaciones de transición.

Por ejemplo, el 7 de enero de 2015, guardó los siguientes archivos en OBS:

- log/test1.log
- log/test2.log
- doc/example.doc
- doc/good.txt

El 10 de enero de 2015, guardó los siguientes archivos:

- log/clientlog.log
- log/serverlog.log
- doc/work.doc
- doc/travel.txt

El 10 de enero de 2015, establezca la hora de caducidad de los objetos con el prefijo **log** en un día después, es posible que encuentre las siguientes situaciones:

- Los objetos **log/test1.log** y **log/test2.log** cargados el 7 de enero de 2015 pueden eliminarse después del último análisis del sistema. La eliminación puede ocurrir el 10 de enero de 2015 o el 11 de enero de 2015, dependiendo de la hora del último análisis del sistema.
- Los objetos **log/clientlog.log** y **log/serverlog.log** cargados el 10 de enero de 2015 generalmente se eliminan el 11 de enero de 2015 o el 12 de enero de 2015, dependiendo de la hora del último análisis del sistema. Si los objetos se han almacenado durante más de un día en el momento de la última exploración del sistema, los objetos se eliminan durante la exploración. O bien, se eliminan en el siguiente análisis del sistema o más tarde siempre que su duración de almacenamiento cumpla con el requisito de tiempo de caducidad especificado.

El día de la operación, puede establecer que los objetos con el prefijo de nombre **log** se transfieran a **Infrequent Access** 30 días después, se transfieran a **Archive** 60 días después y se eliminen 100 días después, luego OBS transfiera a **log/clientlog.log**, **log/serverlog.log**, **log/test1.log** y **log/test2.log** a **Infrequent Access** cuando su duración de almacenamiento supere

los 30 días, transfiera a **Archive** cuando su duración de almacenamiento supere los 60 días y elimínelos cuando su duración de almacenamiento supere los 100 días, respectivamente.

NOTA

En teoría, se tarda 24 horas como máximo en ejecutar una regla de ciclo de vida. Dado que OBS calcula el ciclo de vida de un objeto a partir de las siguientes 00:00 (hora UTC) después de cargar el objeto, puede haber un retraso en la transición de objetos entre clases de almacenamiento y la eliminación de objetos caducados. Generalmente, el retardo no excede de 48 horas. Si realiza cambios en una regla de ciclo de vida existente, la regla volverá a surtir efecto.

Paso 7 Haga clic en **OK** para completar la configuración de la regla del ciclo de vida.

----Fin

Replicación de reglas del ciclo de vida

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Overview**.

Paso 4 En el área **Basic Configurations**, haga clic en **Lifecycle Rules**. Se muestra la página **Lifecycle Rules**.

También puede elegir **Basic Configurations** > **Lifecycle Rules** en el panel de navegación.

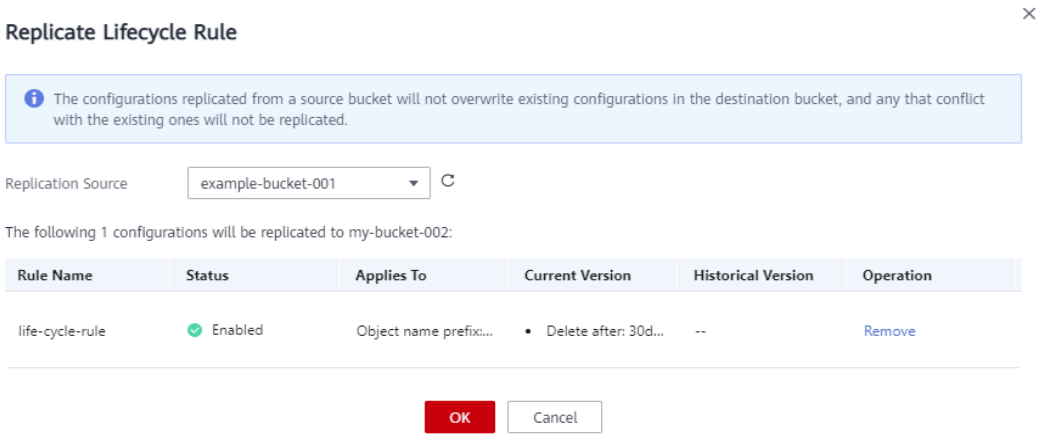
Paso 5 Elija **More** > **Replicate**.

Paso 6 Seleccione un origen de replicación, es decir, el depósito de origen para el que se configuraron las reglas del ciclo de vida.

NOTA

- Las reglas del ciclo de vida replicadas desde un bucket de origen no sobrescribirán las reglas existentes en el bucket de destino y no se replicarán las que entren en conflicto con las existentes.
- La versión de los bucket de origen y destino debe ser 3.0.
- Puede quitar las reglas que no desea replicar.
- Si el bucket de destino no tiene activado el control de versiones, las reglas relacionadas con el control de versiones no se replicarán.

Figura 19-3 Replicación de reglas del ciclo de vida



Paso 7 Haga clic en **OK** para replicar las reglas en el bucket de destino.

----Fin

Procedimiento de seguimiento

Puede hacer clic en **Edit** debajo de la columna **Operation** de una regla de ciclo de vida para editar la regla. También puede hacer clic en **Disable** o **Enable** para desactivarlo o habilitarlo.

Si desea eliminar más de una regla de ciclo de vida a la vez, selecciónelas y haga clic en **Delete** encima de la lista.

20 Configuración de nombres de dominio definidos por el usuario

20.1 Overview

Application Scenario

After you upload a file to a bucket, you can access this file using the bucket's access domain name by default. If you want to use a custom domain name to access the file, bind the custom domain name to the bucket.

Assume that you have a domain name **www.example.com** and you upload an image **image.png** to an OBS bucket. As long as you bind **www.example.com** to the bucket, you can use **http://www.example.com/image.png** to access **image.png**. The steps below describe the configurations:

1. Create a bucket on OBS and upload file **image.png** to the bucket.
2. On OBS Console, bind **www.example.com** to the created bucket.
3. On the DNS server, add a CNAME record and map **www.example.com** to the domain name of the bucket.
4. Send a request for image **image.png**. After the request for **http://www.example.com/image.png** reaches OBS, OBS finds the mapping between the **www.example.com** and the bucket's domain name, and redirects the request to the **image.png** file stored in the bucket. This way, a request for **http://www.example.com/image.png** actually accesses **http://***Bucket domain name***/image.png**.

Limitations and Constraints

1. Only buckets with version 3.0 or later support user-defined domain name configuration. The version number of a bucket is displayed in the **Basic Information** area.
2. By default, a bucket can have up to 20 user-defined domain names bound.
3. User-defined domain names currently allow requests over only HTTP, but not HTTPS.

   If you want to use a bound domain name to access OBS over HTTPS, you need to enable CDN to manage HTTPS certificates.

For details about how to manage HTTPS certificates on the CDN management console, see **HTTPS Settings**.

4. A user-defined domain name can be bound to only one bucket.
5. The suffix of a user-defined domain name can contain 2 to 6 uppercase or lowercase letters.

20.2 Configuración de un nombre de dominio definido por el usuario

Requisitos previos

Como lo requiere el MIIT, debe completar la inscripción de ICP, si el bucket al que está vinculado su nombre de dominio se encuentra en cualquiera de las siguientes regiones:

CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2 y CN South-Guangzhou

Has creado un bucket y has subido el archivo de tu sitio web.

NOTA

Si también se necesita un nombre de dominio de aceleración, para evitar que los objetos de los bucket de OBS se descarguen directamente al acceder, deberá realizar otras operaciones necesarias después de configurar el nombre de dominio personalizado y el nombre de dominio de aceleración. Para obtener más información, consulte **Con la aceleración de CDN activada, ¿por qué se descargan directamente los objetos de mi bucket de OBS cuando accedo a ellos?**

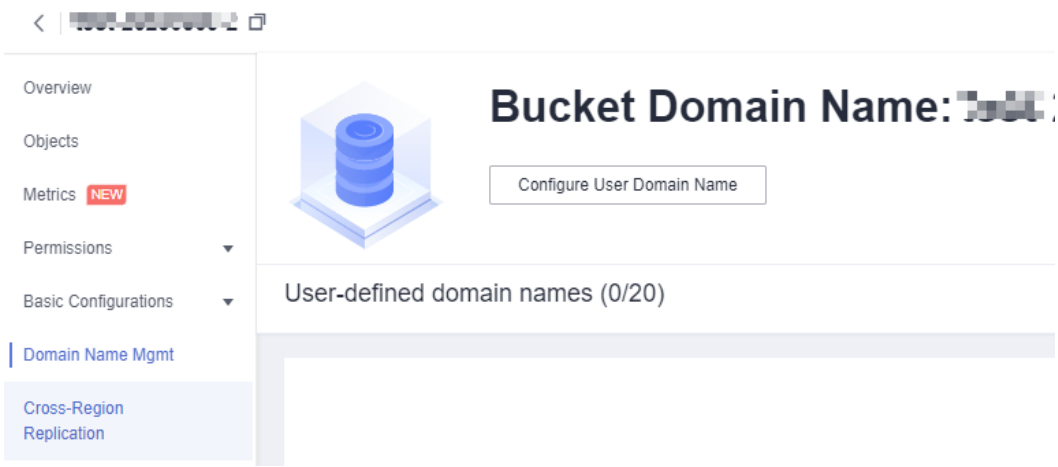
Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Domain Name Mgmt**.

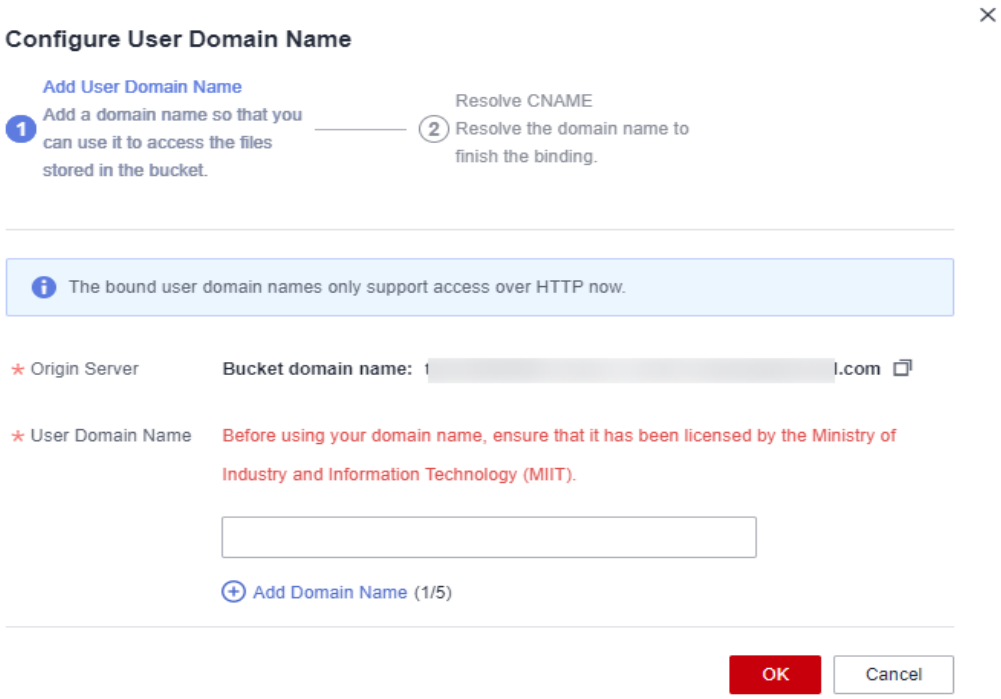
Figura 20-1 Página de gestión de nombres de dominio



Paso 4 Haga clic en **Configure User Domain Name** en la parte superior de la página. También puede hacer clic en **Configure User Domain Name** en el área inferior de la tarjeta de la página cuando no haya nombres de dominio definidos por el usuario disponibles. En el cuadro de diálogo que se muestra, escriba el nombre de dominio que desea configurar, como se muestra en **Figura 20-2**.

El sufijo de un nombre de dominio definido por el usuario puede contener de 2 a 6 letras mayúsculas o minúsculas.

Figura 20-2 Configurar un nombre de dominio de usuario



Paso 5 Haga clic en **OK**.

Paso 6 En función de las sugerencias, haga clic en **Resolve** o agregue manualmente un conjunto de registros de CNAME.Then, click **OK**.

NOTA

Al hacer clic en **Resolve** se agregarán automáticamente conjuntos de registros de CNAME para los nombres de dominio de Huawei Cloud. Para resolver los nombres de dominio no registrados en Huawei Cloud, debe configurar las reglas de resolución usted mismo.

Paso 7 Configure un registro de CNAME en el DNS y asigne el nombre de dominio definido por el usuario (por ejemplo, **example.com**) al nombre de dominio del bucket.

La configuración de CNAME varía según los proveedores de DNS. Para obtener más información acerca de cómo configurar los registros de CNAME con otros proveedores de DNS, consulte la **Descripción general**.

Si su servicio DNS es proporcionado por Huawei Cloud, realice los siguientes pasos para configurar un registro de CNAME:

1. Inicie sesión en la consola de Huawei Cloud. En la página de inicio, elija **Networking** > **Domain Name Service**. Se muestra la consola de DNS.

2. En el panel de navegación, elija **Public Zones**. Se muestra la página de lista de nombres de dominio.
3. Haga clic en el nombre de dominio al que desea agregar un conjunto de registros.
4. Elija la ficha **Record Sets** y haga clic en **Add Record Set**.
5. Configure los parámetros basados en **Tabla 20-1**. Conserve los valores predeterminados para aquellos que no aparecen en la siguiente tabla.

Tabla 20-1 Parámetros para agregar un conjunto de registros

Parámetro	Descripción	Valor de ejemplo
Name	Prefijo del nombre de dominio	www
Type	Tipo del conjunto de registros, que debe ser un nombre CNAME-Canonical aquí.	CNAME - Asignar un dominio a otro
Line	Línea de resolución. El servidor de DNS devolverá la dirección IP de la línea especificada, dependiendo de dónde provenga el visitante. Debe agregar una línea **Default** para asegurarse de que el sitio web sea accesible para cualquier persona.	Default
TTL (s)	Duración de caché del conjunto de registros, en segundos	El intervalo predeterminado es **5 min** (300 segundos).
Value	Nombre de dominio al que apuntar	– Si no se utiliza la aceleración de CDN, establezca este parámetro en el nombre de dominio del bucket. – Si se utiliza la aceleración de CDN, establezca este parámetro en el registro de CNAME asignado por CDN.

6. Haga clic en **OK**.
7. Compruebe si la configuración de CNAME tiene efecto.

   Abra la interfaz de línea de comandos de Windows y ejecute el siguiente comando:

   ```
   nslookup -qt=cname User-defined domain name bound to the bucket
   ```

   – Sin aceleración de CDN: Si la salida es el nombre de dominio del bucket, la configuración de CNAME ha tenido efecto.

   – With CDN acceleration: If the output is the CNAME record allocated by CDN, the CNAME configuration has taken effect.

----Fin

21 Vuelta a la fuente

21.1 Overview

When a client does not access the requested data in OBS, the 404 error is returned. However, OBS provides the back-to-source function to help you obtain the requested data from its source site if it is not found in OBS.

Back-to-Source by Mirroring

If a mirroring back-to-source rule is configured for an OBS bucket and the requested data is not found in the bucket, the system will retrieve the data, when the back-to-source rule applies to the data, from the origin server, upload it to the bucket, and then return it to the requesting client. This process does not interrupt services. Therefore, you can use this function to seamlessly migrate data from the origin server to OBS, or migrate services to OBS without being sensed by users, at low costs. **Figura 21-1** illustrates the mirroring back-to-source process.

Figura 21-1 Back-to-source by mirroring

Limitations and Constraints

- Back to source is currently available only in the following regions: AP-Singapore, CN East-Shanghai1, CN North-Beijing4, CN-Hong Kong, AP-Bangkok, CN South-Guangzhou, and AP-Jakarta.
- Anonymous users cannot configure mirroring back-to-source rules for a bucket.
- Parallel file systems do not support mirroring back-to-source rules.

- A mirroring back-to-source rule is not compatible with the static website hosting function. Specifically, if a 404 error occurs when objects are downloaded from an OBS hosted static website domain, it does not trigger the mirroring back-to-source process.
- The bucket, to which a back-to-source rule is configured, cannot be specified as the source site.
- Currently, mirroring back to source from private buckets is supported for only some cloud vendors.
- The origin server cannot transfer data in **Transfer-Encoding: chunked** mode. That is, the response to the request for downloading an object from the origin server must contain the **Content-Length** header to specify the size of the source object.
- An object cannot match two different mirroring back-to-source rules.
- Only buckets of version 3.0 or later support the mirroring back-to-source function.
- A mirroring back-to-source rule takes effect five minutes later after any change to the rule.
- A maximum of 10 mirroring back-to-source rules can be configured for a bucket.
- The mirroring back-to-source function is offered for free.

21.2 Configuración de una regla de vuelta a la fuente

Escenarios

Para obtener más información, consulte **Vuelta a la fuente**.

Puede crear reglas de vuelta a la fuente o replicar reglas de vuelta a la fuente existentes desde otro bucket.

Limitaciones y restricciones

Para obtener más información, consulte **Vuelta a la fuente**.

Creación de una regla de vuelta a la fuente de mirroring

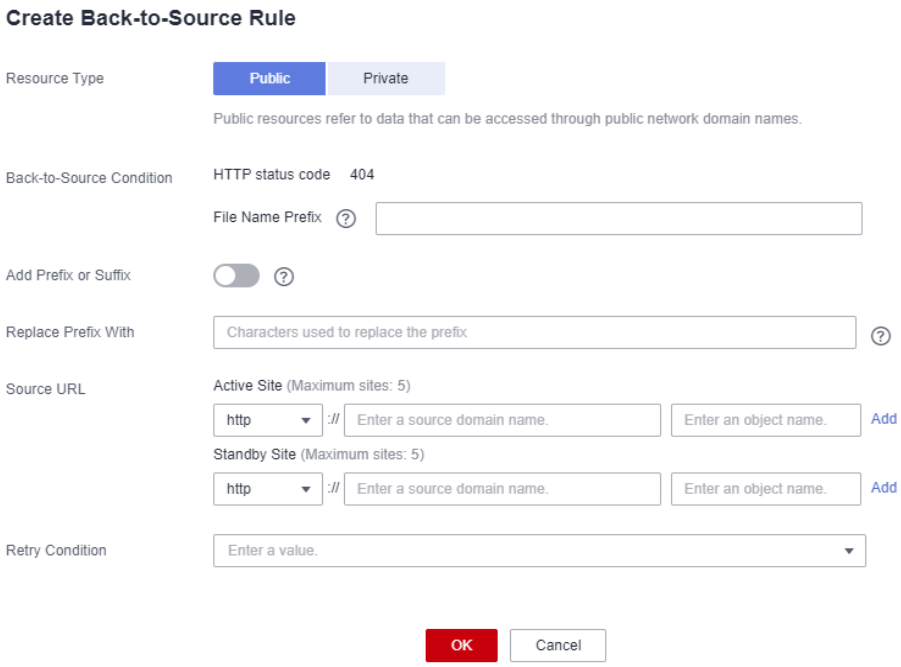
Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Back to Source**. Se muestra la lista de reglas de vuelta a la fuente.

Paso 4 Haga clic en **Create**.

Figura 21-2 Creación de una regla de vuelta a la fuente de mirroring



Paso 5 Configura una regla de duplicación vuelta a la fuente haciendo referencia a los parámetros listados en **Tabla 21-1**.

Tabla 21-1 Parámetros en una regla de vuelta a la fuente de mirroring

Parámetro	Descripción
Resource Type	Tipo de los recursos en el sitio de origen (servidor de origen). ● **Public**: Los datos del servidor de origen provienen del almacenamiento de objetos públicos. ● **Private**: Los datos del servidor de origen provienen del almacenamiento de objetos privados de algunos proveedores en la nube.

Parámetro	Descripción
Back-to-Source Condition	Condiciones que activan la regla de vuelta a la fuente. Una regla de duplicación vuelta a la fuente se activa cuando se cumplen las siguientes condiciones: El objeto solicitado comienza con el prefijo de nombre de archivo especificado, y se devuelve un código de estado HTTP 404 porque el objeto no se encuentra en el bucket. Reglas para especificar un prefijo de nombre de archivo: ● El prefijo de nombre de archivo especificado no puede superar los 1023 caracteres. ● El prefijo de nombre de archivo especificado no puede contener ni solaparse con ningún otro prefijo de nombre de archivo especificado para una regla existente. ● Si no se especifica ningún prefijo de nombre de archivo, la regla se aplica a todos los archivos que no cumplan las condiciones de otras reglas de vuelta a la fuente configuradas para el bucket. Un bucket solo puede tener una regla vuelta a la fuente que no tenga un prefijo de nombre de archivo especificado. Por ejemplo, si el prefijo de nombre de archivo se establece en **123/**, la regla se activa cuando se solicita el archivo **123/456.txt** pero no está disponible en el bucket.
Add Prefix or Suffix	Cuando OBS solicita datos del sitio de origen, el prefijo o el sufijo se agrega delante o después del nombre del objeto solicitado. Sin embargo, el objeto devuelto a OBS y el cliente conserva su nombre original sin el prefijo o sufijo agregado. Ejemplo: Un cliente solicita **abc.txt** de OBS, lo que activa la regla vuelta a la fuente. Si el prefijo especificado es **123**, OBS solicita **123abc.txt** desde el sitio de origen. Sin embargo, el objeto todavía se descarga como **abc.txt** en OBS y luego se devuelve al cliente.
Replace Prefix With	OBS utiliza el prefijo especificado para reemplazar el prefijo de nombre de archivo establecido en la condición vuelta a la fuente cuando solicita datos del sitio de origen. Sin embargo, el objeto devuelto al cliente conserva el prefijo original en su nombre. Ejemplo: El prefijo de nombre de archivo se establece en **123** como la condición vuelta a la fuente y el prefijo de reemplazo se establece en **abc**. Cuando el cliente solicita **123456.txt**, se activa la regla de vuelta a la fuente. A continuación, OBS solicita **abc456.txt** desde el sitio de origen. Sin embargo, el objeto obtenido todavía se guarda como **123456.txt** en OBS y se devuelve al cliente.

Parámetro	Descripción
Source URL	Dirección del sitio de origen. Puede configurar sitios activos y sitios en espera. La dirección del sitio activo se utiliza preferentemente durante el proceso de vuelta a la fuente. Si se configuran varias direcciones de sitio activas, se accede a todos los sitios activos en modo de sondeo. Si se configuran dos o más direcciones de sitio activas, cuando falla la primera solicitud a una dirección activa y se cumplen las condiciones de reintento, la solicitud volverá a intentar otra dirección de sitio activa. Configure al menos un sitio activo. Se admiten hasta cinco sitios activos. Si no puede recuperar el contenido de todos los sitios activos, la solicitud probará los sitios en espera. Archivo de la etiqueta: *http(https)://source domain name/static path* ● El nombre de dominio de origen es el nombre de dominio del sitio de origen. – Si el sitio de origen es un bucket al que se puede acceder a través de HTTP, la dirección es el nombre de dominio del bucket. – Si el sitio de origen es un bucket privado proporcionado por otros proveedores en la nube, la dirección es el nombre de dominio de la región. En la actualidad, solo se admiten los bucket privados de algunos proveedores de nube. ● La ruta estática indica el directorio donde reside el archivo de destino. Por ejemplo, si la ruta estática es de **123/** el archivo de destino está en el directorio **123/**.
Retry Condition	Condición cuando se activa un reintento. Los códigos de error que comienzan con **4XX** y **4** no se pueden configurar juntos. Los códigos de error que comienzan con **5XX** y **5** no se pueden configurar juntos. Se puede configurar un máximo de 20 códigos de error.
Carry Request String	Cuando esta función está habilitada, los parámetros de consulta en el URL de solicitud se pasan al sitio de origen.
Redirect Request	Cuando esta función está habilitada, la solicitud seguirá la respuesta de redirección de 3*xx*, si la redirección está configurada para el sitio de origen, para obtener el recurso solicitado y guardar el recurso en OBS. Una solicitud puede seguir un máximo de 10 redirecciones.
Redirect without Referer	Con esta función habilitada, si se ha configurado la redirección para el servidor de origen, el encabezado Referer de la solicitud se filtrará durante la redirección.

Parámetro	Descripción
HTTP Header Pass Rule	Puede especificar los parámetros de encabezado HTTP que se pueden pasar al sitio de origen cuando una solicitud enviada a OBS activa la regla de vuelta a la fuente de mirroring. **Referencias** proporciona un ejemplo de configuración y enumera los encabezados HTTP que no son compatibles. ● **Pass all parameters/Pass specified parameters**: Establezca los parámetros de encabezado HTTP que se pueden pasar. ● **Do not pass specified parameters**: Establezca los parámetros de encabezado HTTP que no se pueden pasar. En este caso, OBS no pasa los encabezados especificados al sitio de origen. Si se especifica un encabezado para las categorías de paso y de no paso, se considera como un parámetro de no paso. ● **Configure custom parameters**: Puede establecer un valor personalizado para un encabezado especificado. Si una solicitud de cliente lleva este encabezado, OBS cambia el valor del encabezado al valor personalizado antes de pasarlo al sitio de origen.
IAM Agency	Se requiere que una delegación de IAM delegue OBS para obtener datos del sitio de origen. La delegación debe otorgar a OBS el permiso **Tenant Administrator**, con un período de validez ilimitado. Si no hay una delegación de IAM apropiada disponible, cree una. Para obtener más información, véase **Creación de una delegación de IAM**.

Paso 6 Haga clic en **OK**.

----Fin

Replicando reglas de vuelta a la fuente de mirroring

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Back to Source**. Se muestra la lista de reglas de vuelta a la fuente.

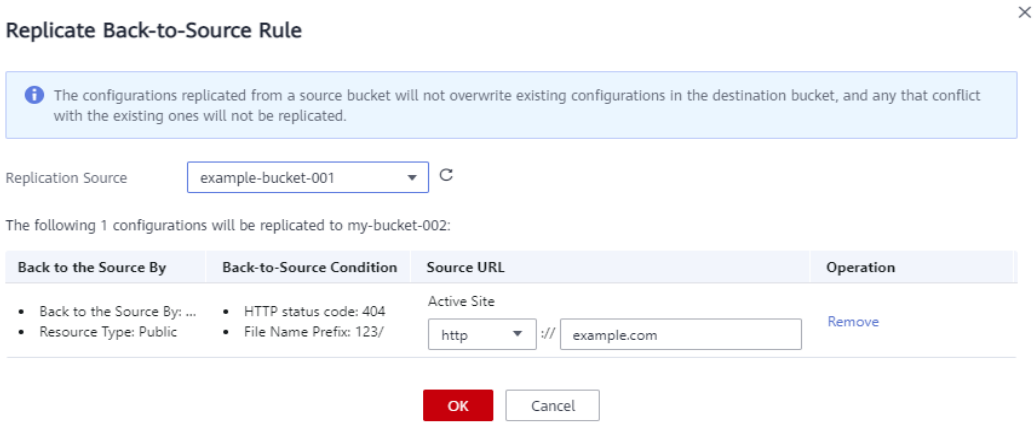
Paso 4 Haga clic en **Replicate**.

Paso 5 Seleccione un origen de replicación, es decir, el bucket de origen para el que se configuraron las reglas de vuelta a la fuente.

NOTA

- Las reglas de vuelta a la fuente replicadas desde un bucket fuente no sobrescribirán las reglas existentes en el bucket de destino, y las que entren en conflicto con las existentes no serán replicadas.
- La versión de los bucket de origen y destino debe ser 3.0.
- Antes de replicar las reglas de vuelta a la fuente, puedes cambiar su URL de origen. Para obtener más información sobre la configuración del URL de origen, consulte **Tabla 21-1**.
- Puede quitar las reglas que no desea replicar.
- Puede haber cinco reglas de vuelta a la fuente como máximo en un bucket. Si el número de reglas que replicará más el número de reglas existentes en el bucket de destino supera las cinco, la replicación producirá un error. Antes de replicar las reglas, elimine algunas si es necesario.

Figura 21-3 Replicando las reglas de la vuelta a la fuente



Paso 6 Haga clic en **OK** para replicar las reglas en el bucket de destino.

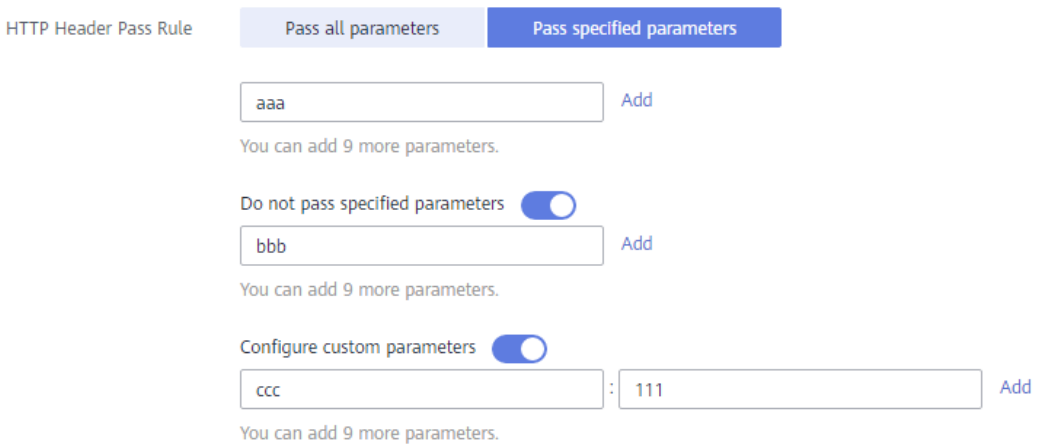
----Fin

Referencias

Ejemplo para configurar una regla de paso de encabezado HTTP:

Supongamos que los parámetros se establecen como se muestra en **Figura 21-4**.

Figura 21-4 Configuración de una regla de paso de encabezado de HTTP



Basado en la configuración anterior, si el encabezado de la solicitud enviada a OBS es el siguiente:

```
GET /ObjectName HTTP/1.1
Host: bucketname.obs.region.myhuaweicloud.com
aaa:aaa
bbb:bbb
ccc:ccc
```

OBS envía la siguiente solicitud al sitio de origen cuando se activa la regla vuelta a la fuente:

```
GET /ObjectName HTTP/1.1
Host: source.com
aaa:aaa
ccc:111
```

Los siguientes encabezados de HTTP no se pueden pasar al sitio de origen:

1. Encabezados de HTTP que comienzan con los siguientes prefijos:
   - x-obs-
2. Todos los encabezados HTTP estándar, por ejemplo:
   - Content-Length
   - Authorization2
   - Authorization
   - Range
   - Date

22 Alojamiento de sitio web estático

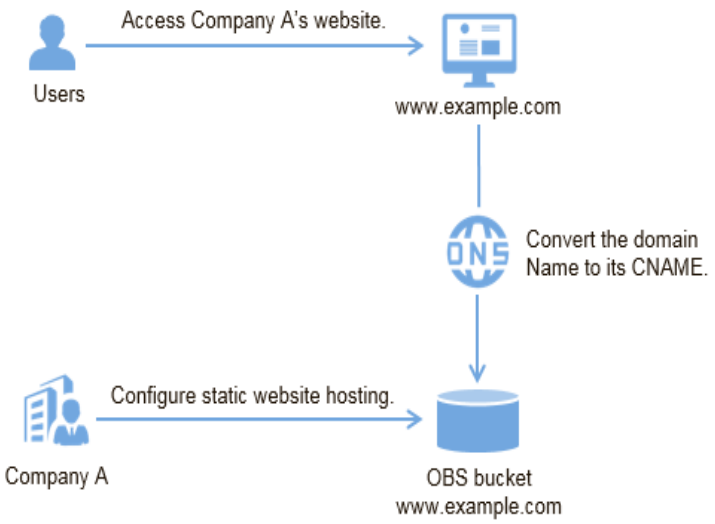
22.1 Alojamiento de sitios web estático

Puede cargar los archivos de contenido de sitios web estáticos a su bucket en OBS, autorizar a los usuarios anónimos el permiso para leer estos archivos y configurar el alojamiento de sitios web estáticos para que el bucket aloje estos archivos.

Los sitios web estáticos contienen páginas estáticas y algunos scripts que pueden ejecutarse en clientes, como JavaScript y Flash. A diferencia de los sitios web estáticos, los sitios dinámicos dependen de los servidores para procesar los scripts, entre ellos los scripts PHP, JSP y ASP.NET. OBS no admite scripts que se ejecutan en servidores.

La configuración del alojamiento web estático tiene efecto en dos minutos. Después de que el alojamiento web estático sea efectivo en OBS, puede acceder al sitio web estático utilizando el URL proporcionada por OBS.

Figura 22-1 Alojamiento de sitio web estático



22.2 Redirection Overview

When using static website hosting, you can also configure redirection to redirect specific or all requests.

If the structure, address, or file name extension of a website is changed, users will fail to access the website using the old address (such as the address saved in the folder of favorites), and the 404 error message is returned. In this case, you can configure redirection for the website to redirect user access requests to the specified page instead of returning the 404 error page.

Typical configurations include:

- Redirecting all requests to another website.
- Redirecting specific requests based on redirection rules.

22.3 Configuración del alojamiento de sitios web estáticos

Puede configurar el alojamiento de sitios web estáticos para un bucket y luego usar un nombre de dominio del bucket para acceder a sitios web estáticos alojados en el bucket.

El alojamiento de sitios web estáticos entra en vigor dentro de los dos minutos después de que se complete su configuración.

NOTA

En el escenario de alojamiento de sitios web estáticos, los usuarios anónimos deben tener acceso al archivo de sitio web estático alojado. Durante su acceso al archivo alojado, se incurrirán en tarifas por el tráfico de Internet saliente y las solicitudes.

Precauciones

Por motivos de seguridad y cumplimiento, utilizar el alojamiento de sitios web estático a través del nombre de dominio de OBS predeterminado (**nombre de dominio de bucket o nombre de dominio de sitio web estático**) será prohibido por OBS. Cuando utiliza dicho nombre de dominio para acceder a páginas web a través de un navegador, no se mostrará ningún contenido, en su lugar, el contenido se descargará como un archivo adjunto.

Esta prohibición entrará en vigor en diferentes regiones en los dos momentos siguientes:

1 de enero de 2022: CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, and CN South-Guangzhou

25 de marzo de 2022: CN-Hong Kong, AP-Bangkok, AP-Singapore, AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago

Todavía puede utilizar el alojamiento de sitios web estático a través de un nombre de dominio definido por el usuario. De esta manera, el contenido aún se puede previsualizar. Para obtener más información, consulte **¿Cómo previsualizo objetos en OBS a través de un navegador?**

Requisitos previos

Los archivos de página web del sitio web estático se han subido a un bucket.

Los usuarios anónimos pueden acceder a los archivos de sitios web estáticos alojados en el bucket.

Si los archivos de página web están en la clase de almacenamiento Archive o Deep Archive, restáurelos primero. Para obtener más información, consulte **Restauración de objetos del almacenamiento Archive**.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

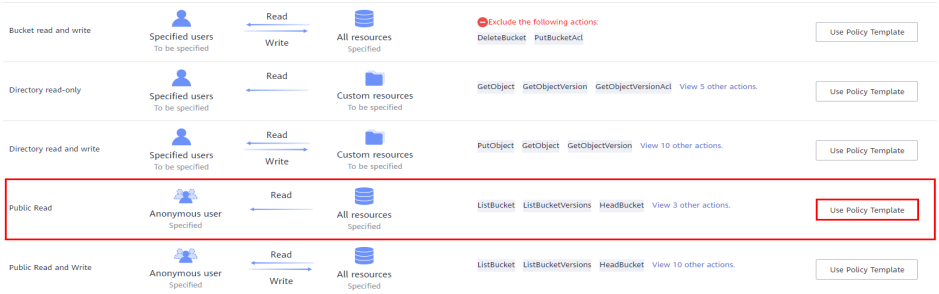
Paso 3 (**Optional**) Si los usuarios anónimos no pueden acceder a los archivos de sitio web estáticos del bucket realice este paso. Si ya son accesibles para todos, omita este paso.

Otorgar el permiso de lectura para archivos de sitio web estáticos a usuarios anónimos. Para obtener más información, consulte **Concesión de permisos de lectura pública en objetos a usuarios anónimos**.

Si el bucket solo contiene archivos de sitio web estáticos, configure la política **Public Read** para el bucket para que se pueda acceder públicamente a todos los archivos.

1. Elija **Permissions** > **Bucket Policy**.
2. Haga clic en **Create**.
3. En la lista de plantillas, busque **Public Read** en la columna **Template Name** y haga clic en **Use Policy Template** a la derecha.

Figura 22-2 Configuración del permiso de lectura pública



4. Mantenga la configuración predeterminada de la plantilla y haga clic en **Next** y, a continuación, en **Create**.

Paso 4 En el panel de navegación, elija **Overview**.

Paso 5 En el área **Basic Configurations**, haga clic en **Static Website Hosting**. Se muestra la página **Static Website Hosting**.

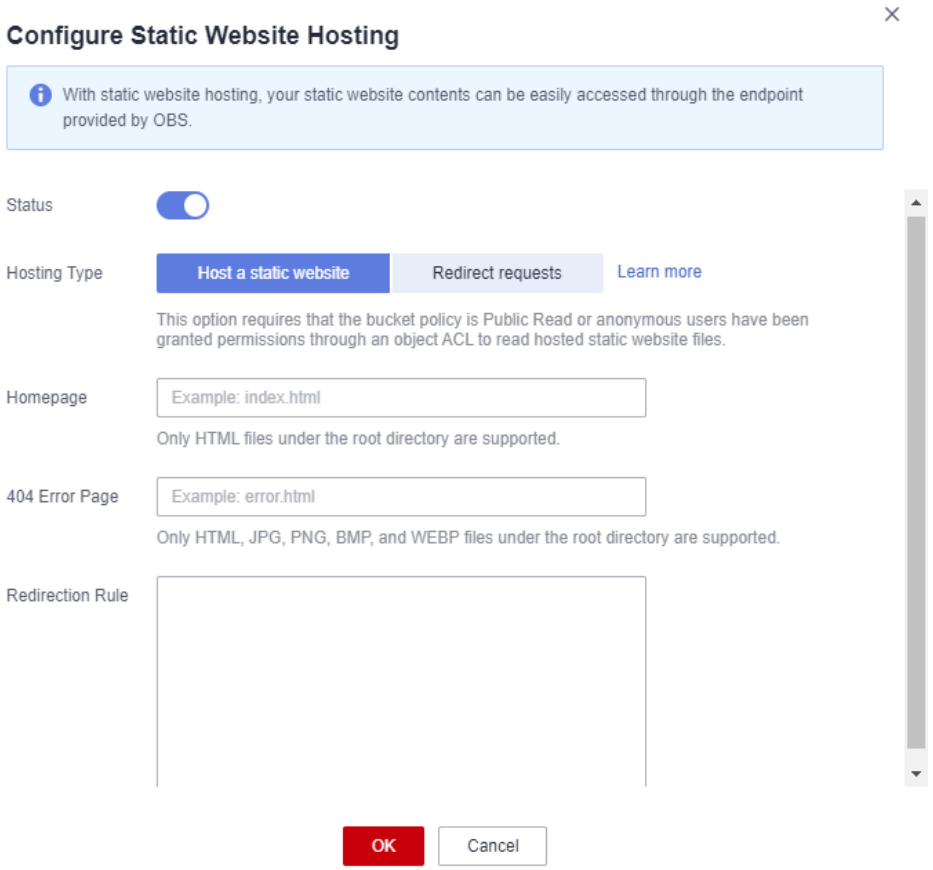
Alternativamente, puede elegir **Basic Configurations** > **Static Website Hosting** en el panel de navegación de la izquierda.

Paso 6 Haga clic en **Configure Static Website Hosting**. Aparece el cuadro de diálogo **Configure Static Website Hosting**.

Paso 7 Actívelo encendiendo el interruptor de estado.

Paso 8 Establezca el tipo de alojamiento en el bucket actual. Para obtener más información, consulte **Figura 22-3**.

Figura 22-3 Configurar el alojamiento de sitios web estáticos



Paso 9 Establezca los valores de la página de inicio y de la página de error 404.

- **Homepage**: especifica la página de inicio predeterminada del sitio web estático. Cuando se utiliza OBS Console para configurar el alojamiento de sitios web estático, solo se admiten páginas web HTML. Cuando las API se utilizan para configurar el alojamiento de sitios web estático, OBS no tiene ninguna restricción, pero se debe especificar **Content-Type** de los objetos.

  OBS solo permite que archivos como **index.html** en el directorio raíz de un bucket funcionen como la página de inicio por defecto. No establezca la página de inicio predeterminada con una estructura de directorios de varios niveles (por ejemplo, **/page/index.html**).
- **404 Error Page**: especifica la página de error devuelta cuando se produce un error durante el acceso estático al sitio web. Cuando se utiliza OBS Console para configurar el alojamiento de sitios web estático, solo se admiten archivos HTML, JPG, PNG, BMP y WEBP bajo el directorio raíz. Cuando las API se utilizan para configurar el alojamiento de sitios web estático, OBS no tiene ninguna restricción, pero se debe especificar **Content-Type** de los objetos.

Paso 10 **Optional**: En **Redirection Rules**, configure las reglas de redirección. Las solicitudes que cumplen con las reglas de redirección se redirigen al host o página específico.

Una regla de redirección se compila en formato JSON o XML. Cada regla contiene un **Condition** y un **Redirect**. Los parámetros se describen de la siguiente manera:

Tabla 22-1 Descripción del parámetro

Contenedor	Clave	Descripción
Condición	KeyPrefixEquals	Prefijo de nombre de objeto en el que se aplica la regla de redirección. Cuando se envía una solicitud para acceder a un objeto, la regla de redirección tiene efecto si el prefijo del nombre del objeto coincide con el valor especificado para este parámetro. Por ejemplo, para redirigir la solicitud de objeto **ExamplePage.html**, establezca **KeyPrefixEquals** en **ExamplePage.html**.
	HttpErrorCodeReturnedEquals	Códigos de error de HTTP sobre los que la regla de redirección entra en vigor. La redirección especificada sólo se aplica cuando el código de error devuelto es igual al valor especificado para este parámetro. Por ejemplo, si desea redirigir las solicitudes a **NotFound.html** cuando se devuelve el código de error HTTP 404, establezca **HttpErrorCodeReturnedEquals** en **404** en **Condition**, y establezca **ReplaceKeyWith** a **NotFound.html** en **Redirect**.
Redireccionar	Protocol	Protocolo utilizado para la redirección. El valor puede ser **http** o **https**. Si no se especifica este parámetro, se utiliza el valor predeterminado **http**.
	HostName	Nombre de host al que apunta la redirección. Si no se especifica este parámetro, la solicitud se redirige al host desde el que se inicia la solicitud original.
	ReplaceKeyPrefixWith	Prefijo de nombre de objeto en el que entra en vigor la regla de redirección
	ReplaceKeyWith	Nombre del objeto en el que entra en vigor la regla de redirección
	HttpRedirectCode	Código de estado HTTP devuelto a la solicitud de redirección. El valor predeterminado es **301**, que indica que las solicitudes se redirigen permanentemente a la ubicación especificada por **Redirect**. También puede establecer este parámetro en función de sus necesidades de servicio.

Ejemplo de configuración de una regla de redirección

- Ejemplo 1: Todas las solicitudes de objetos con el prefijo **folder1/** se redirigen automáticamente a las páginas con el prefijo **target.html** en el host **www.example.com** usando HTTPS.

```
[
    {
    "Condition": {
        "KeyPrefixEquals": "folder1/"
        },
    "Redirect":{
        "Protocol": "https",
        "HostName": "www.example.com",
        "ReplaceKeyPrefixWith": "target.html"
        }
    }
]
```

- Ejemplo 2: Todas las solicitudes de objetos con el prefijo **folder2/** se redirigen automáticamente a objetos con el prefijo **folder/** en el mismo bucket.

```
[
    {
    "Condition": {
        "KeyPrefixEquals": "folder2/"
        },
    "Redirect":{
        "ReplaceKeyPrefixWith": "folder/"
        }
    }
]
```

- Ejemplo 3: Todas las solicitudes de objetos con el prefijo **folder.html** se redirigen automáticamente al objeto **folderdeleted.html** en el mismo bucket.

```
[
    {
    "Condition": {
        "KeyPrefixEquals": "folder.html"
        },
    "Redirect":{
        "ReplaceKeyWith": "folderdeleted.html"
        }
    }
]
```

- Ejemplo 4: Si se devuelve el código de estado de HTTP 404, la solicitud se redirige automáticamente a la página con el prefijo **report-404/** en el host **www.example.com**.

  For example, if you request the page **ExamplePage.html** but the HTTP 404 error is returned, the request will be redirected to the **report-404/ExamplePage.html** page on the **www.example.com**. If the 404 redirection rule is not specified, the default 404 error page configured in the previous step is returned when the HTTP 404 error occurs.

```
[
    {
    "Condition": {
        "HttpErrorCodeReturnedEquals": "404"
        },
    "Redirect":{
        "HostName": "www.example.com",
        "ReplaceKeyPrefixWith": "report-404/"
        }
    }
]
```

Paso 11 Haga clic en **OK**.

Después de que el alojamiento web estático sea efectivo en OBS, puede acceder al sitio web estático utilizando el URL proporcionada por OBS.

NOTA

En algunas condiciones, es posible que tenga que borrar la caché del navegador antes de que se muestren los resultados esperados.

----Fin

22.4 Configuración de redirección

Puede redirigir todas las solicitudes de un bucket a otro bucket o URL configurando reglas de redirección.

Requisitos previos

Los archivos de página web del sitio web estático se han subido a un bucket.

Los usuarios anónimos pueden acceder a los archivos de sitios web estáticos alojados en el bucket.

Si los archivos de página web están en la clase de almacenamiento Archive o Deep Archive, restáurelos primero. Para obtener más información, consulte **Restauración de objetos del almacenamiento Archive**.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Overview**.

Paso 4 En el área **Basic Configurations**, haga clic en **Static Website Hosting**. Se muestra la página **Static Website Hosting**.

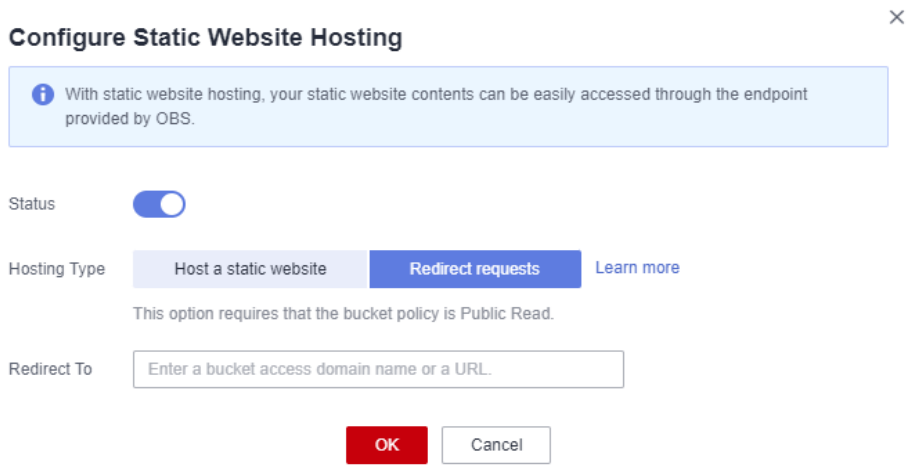
Alternativamente, puede elegir **Basic Configurations** > **Static Website Hosting** en el panel de navegación de la izquierda.

Paso 5 Haga clic en **Configure Static Website Hosting**. Aparece el cuadro de diálogo **Configure Static Website Hosting**.

Paso 6 Actívelo encendiendo el interruptor de estado.

Paso 7 Ajuste **Hosting By** a **Redirection**. Vea **Figura 22-4** para más detalles. Ingrese un nombre de dominio o URL de acceso al bucket en el cuadro de texto de **Redirect To**.

Figura 22-4 Configuración de redirección



Paso 8 Haga clic en **OK**.

Paso 9 En la lista de bucket, haga clic en el bucket al que se redirigen las solicitudes para el sitio web estático.

Paso 10 **Verification**: Ingrese el nombre de dominio de acceso del bucket en el navegador web y presione **Enter**. Se mostrará el bucket o URL al que se redirigen las solicitudes.

NOTA

En algunas condiciones, es posible que tenga que borrar la caché del navegador antes de que se muestren los resultados esperados.

----Fin

23 Intercambio de recursos entre orígenes

23.1 CORS Overview

CORS is a browser-standard mechanism provided by the World Wide Web Consortium (W3C). It defines the interaction methods between client-side web applications in one origin and resources in another origin. For general web page requests, website scripts and contents in one origin cannot interact with those in another origin because of Same Origin Policies (SOPs).

The CORS specification is supported to allow cross-origin requests to access OBS resources.

OBS supports static website hosting. Static websites stored in OBS can respond to website requests from another origin only when CORS is configured for the bucket.

Typical application scenarios of CORS are as follows:

- Enables JavaScript and HTML5 to be used for establishing web applications that can directly access resources in OBS. No proxy servers are required for transfer.
- Enables the dragging function of HTML5 to be used to upload files to OBS (with the upload progress displayed) or update OBS contents using web applications.
- Hosts external web pages, style sheets, and HTML5 applications in different origins. Web fonts or pictures in OBS can be shared by multiple websites.

The configuration of CORS takes effect within two minutes.

23.2 Configuración de CORS

Esta sección describe cómo usar CORS en HTML5 para implementar el acceso entre origen.

Puede crear reglas de CORS o replicar reglas de CORS existentes desde otro bucket.

Requisitos previos

El alojamiento estático de sitios web ha sido configurado. Para obtener más información, véase **Configuración del alojamiento de sitios web estáticos**.

Creación de una regla de CORS

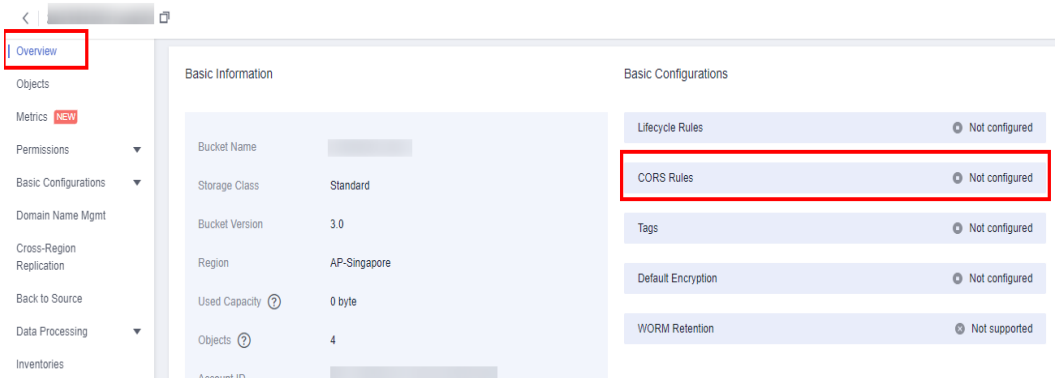
Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Overview**.

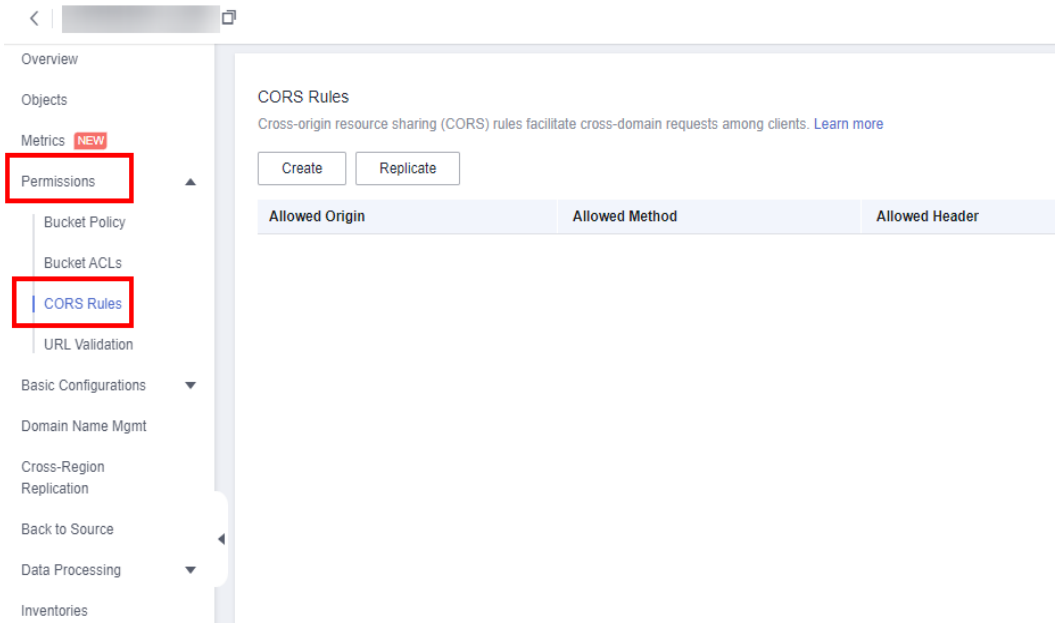
Paso 4 En el área **Basic Configurations**, haga clic en **CORS Rules**. Se muestra la página **CORS Rules**.

Figura 23-1 Descripción general > Configuraciones básicas > Reglas de CORS



Alternativamente, puede elegir **Permissions** > **CORS Rules** en el panel de navegación.

Figura 23-2 Permisos > Reglas de CORS

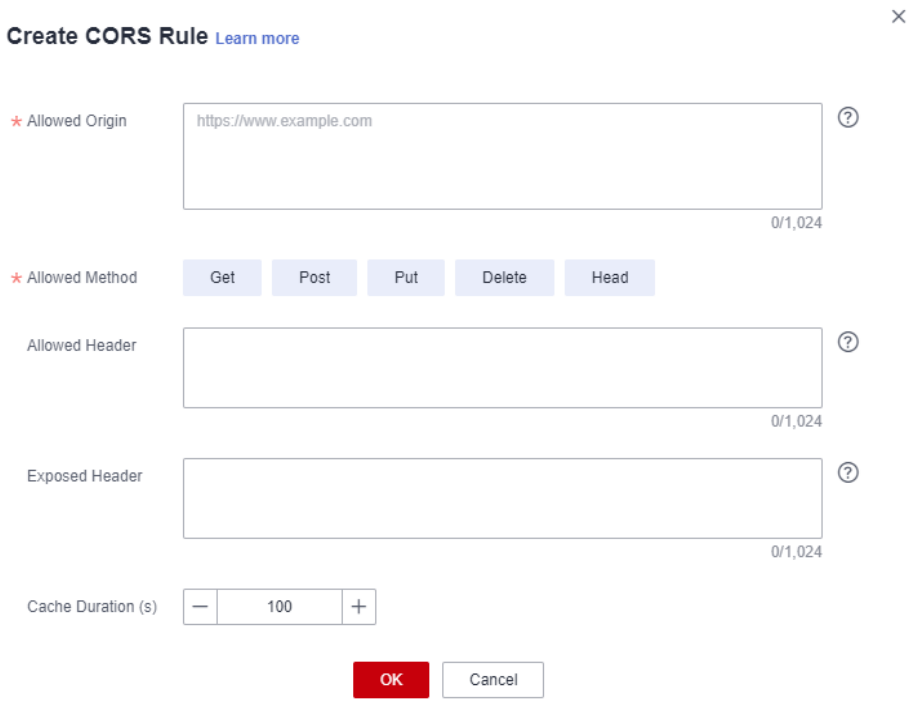


Paso 5 Haga clic en **Create**. Aparece el cuadro de diálogo **Create CORS Rule**. Vea **Figura 23-3** para más detalles.

NOTA

Un bucket puede tener un máximo de 100 reglas de CORS configuradas.

Figura 23-3 Creación de una regla de CORS



Paso 6 En el cuadro de diálogo **CORS Rule**, configure **Allowed Origin**, **Allowed Method**, **Allowed Header**, **Exposed Header** y **Cache Duration (s)**.

NOTA

Si la aceleración de CDN está habilitada para el bucket, se debe configurar el encabezado de HTTP en CDN. Para obtener más información, consulte **Configuración de encabezado HTTP**.

Tabla 23-1 Parámetros en las reglas de CORS

Parámetro	Descripción

Allowed Origin	Obligatorio
	Las solicitudes de este origen pueden acceder al bucket.
	Se permiten varias reglas de coincidencia. Una regla ocupa una línea, y permite un carácter comodín (*) como máximo. Ejemplo:
	`http://rds.example.com`
	`https://*.vbs.example.com`

Allowed Method	Obligatorio Especifica el tipo de operación aceptable de buckets y objetos. Los métodos incluyen Get, Post, Put, Delete y Head.

Parámetro	Descripción
Allowed Header	Opcional Especifica el encabezado permitido de las solicitudes entre orígenes. Solo las solicitudes CORS que coincidan con el encabezado permitido son válidas. Puede introducir varios encabezados permitidos (uno por línea) y cada línea puede contener como máximo un carácter comodín (*). No se permiten espacios ni caracteres especiales como **&:<**.
Exposed Header	Opcional Especifica el encabezado expuesto en las respuestas CORS y proporciona información adicional para los clientes. Por defecto, un navegador solo puede acceder a los encabezados **Content-Length** y **Content-Type**. Si el navegador desea acceder a otros encabezados, debe configurar esos encabezados en este parámetro. Se pueden ingresar múltiples encabezados expuestos (uno por línea). No se permiten espacios ni caracteres especiales que incluyen ***&:<**.
Cache Duration (s)	Obligatorio Especifica la duración que el navegador puede almacenar en caché las respuestas de CORS, expresada en segundos. El valor predeterminado es **100**.

Paso 7 Haga clic en **OK**.

Aparece el mensaje "The CORS rule created successfully.". La configuración de CORS entra en vigor en dos minutos.

Una vez que CORS se ha configurado correctamente, solo las direcciones especificadas en **Allowed Origin** pueden acceder a un bucket en OBS mediante los métodos especificados en **Allowed Method**. Por ejemplo, puede configurar los parámetros de CORS para bucket **testbucket** de la siguiente manera:

- **Allowed Origin**: **https://www.example.com**
- **Allowed Method**: **GET**
- **Allowed Header**: *
- **Exposed Header**: *
- **Cache Duration (s)**: **100**

Al hacerlo, OBS solo permite que las solicitudes GET de **https://www.example.com** accedan al bucket **testbucket** sin restricciones en los encabezados de solicitud. El cliente puede almacenar en caché las respuestas de CORS durante 100 segundos.

----Fin

Replicación de reglas de CORS

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Overview**.

Paso 4 En el área **Basic Configurations**, haga clic en **CORS Rules**. Se muestra la página **CORS Rules**.

Alternativamente, puede elegir **Permissions** > **CORS Rules** en el panel de navegación.

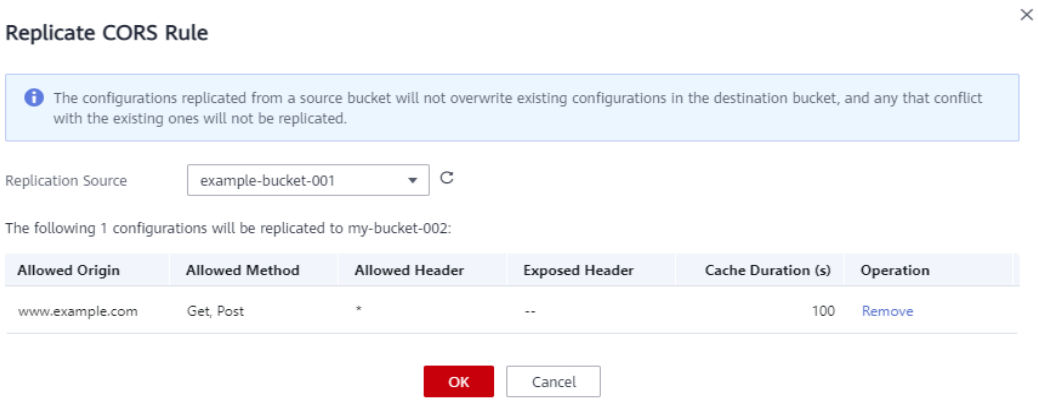
Paso 5 Haga clic en **Replicate**.

Paso 6 Seleccione un origen de replicación, es decir, el bucket de origen para el que se configuraron las reglas de CORS.

NOTA

- Las reglas de CORS replicadas desde un bucket de origen no sobrescribirán las reglas existentes en el bucket de destino, y las que entren en conflicto con las existentes no se replicarán.
- La versión de los bucket de origen y destino debe ser 3.0.
- Puede quitar las reglas que no desea replicar.
- Puede haber 100 reglas de CORS como máximo en un bucket. Si el número de reglas que replicará más el número de reglas existentes en el bucket de destino supera las 100, la replicación fallará. Antes de replicar las reglas, elimine algunas si es necesario.

Figura 23-4 Replicación de reglas de CORS



Paso 7 Haga clic en **OK** para replicar las reglas de CORS en el bucket de destino.

----Fin

24 Validación de URL

24.1 URL Validation Overview

To reduce costs, some websites steal links from other websites to enrich their own contents. Link stealing not only damages interests of the original websites but also increases workloads on the original websites' servers. Therefore URL is used to resolve this problem.

In HTTP, a website can detect the web page that accesses a target web page using the **Referer** field. As the **Referer** field can trace sources, specific techniques can be used to block or return to specific web pages if the pages are not from the website. URL validation checks whether the **Referer** field in requests matches the whitelist or blacklist by setting **Referers**. If the field matches the whitelist, the requests are allowed. Otherwise, the requests are blocked or specific pages are displayed.

OBS supports URL validation based on the **Referer** header field in HTTP requests to prevent a user's data in OBS from being stolen by other users. OBS supports both whitelists and blacklists.

24.2 Configurar la validación de URL

OBS bloquea las solicitudes de acceso desde los URL de la lista negra y permite las de los URL de la lista blanca.

Requisitos previos

El alojamiento estático de sitios web ha sido habilitado.

Procedimiento

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Overview**.

Paso 4 En el área **Basic Configurations**, haga clic en **URL Validation**. Se muestra la página **URL Validation**.

Paso 5 Haga clic en junto al cuadro de texto de **Whitelisted Referers** o **Blacklisted Referers** e introduzca los referidos.

Principios para el establecimiento de **Referers**:

- La longitud de una lista blanca o negra no puede exceder los 1024 caracteres.
- Formato de referencia:
  - Puede introducir varios referentes, cada uno en una línea.
  - El parámetro referer admite asteriscos (*) y signos de interrogación (?). Un asterisco funciona como un comodín que puede reemplazar cero o varios caracteres, y un signo de interrogación (?) puede reemplazar a un solo carácter.
  - Si el campo de encabezado de referencia contiene **http** o **https** durante la descarga, el referenciador debe contener **http** o **https**.
- Si **Whitelisted Referers** se deja en blanco pero **Blacklisted Referers** no, todos los sitios web, excepto los especificados en la lista negra, pueden acceder a los datos del depósito de destino.
- Si **Whitelisted Referers** no se deja en blanco, solo los sitios web especificados en la lista blanca pueden acceder al depósito de destino sin importar si **Blacklisted Referers** se deja en blanco o no.

NOTA

Si **Whitelisted Referers** está configurado de la misma manera que **Blacklisted Referers**, la lista negra tiene efecto. Por ejemplo, si **Whitelisted Referers** y **Blacklisted Referers** están configurados en **https://www.example.com**, se bloquearán las solicitudes de acceso desde esta dirección.

- Si **Whitelisted Referers** y **Blacklisted Referers** se dejan en blanco, todos los sitios web pueden acceder a los datos del depósito de destino de forma predeterminada.
- Antes de determinar si un usuario tiene los cuatro tipos de permisos (lectura, escritura, lectura de ACL y escritura de ACL) para un bucket u objetos en el bucket, compruebe si este usuario cumple con los principios de validación de URL del campo **Referer**.

Paso 6 Haga clic en para guardar la configuración.

----Fin

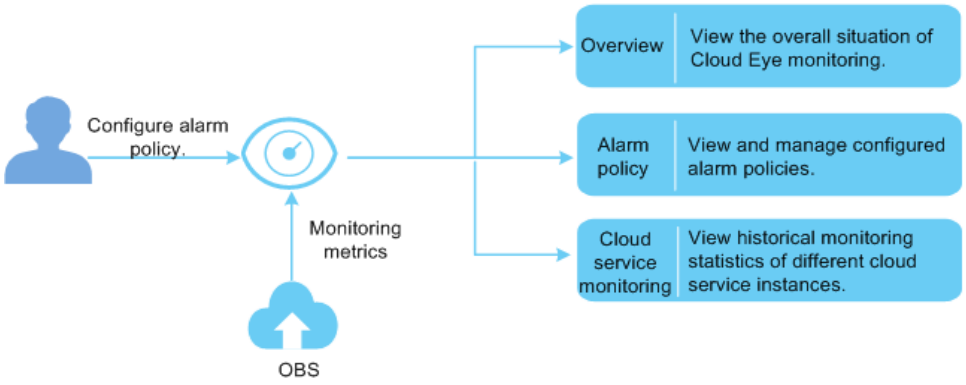
25 Monitoreo

25.1 Monitoreo de OBS

Escenarios

Puede enviar solicitudes PUT y GET continuamente cuando utilice OBS, que genera tráfico de carga y descarga. También puede recibir respuestas de error del servidor. Cloud Eye puede realizar un monitoreo automático y en tiempo real de sus bucket. Activa alarmas y notificaciones sobre las operaciones para ayudarle a comprender sus solicitudes de acceso a bucket, tráfico y respuestas a errores de manera oportuna.

Figura 25-1 Monitoreo de Cloud Eye



Configuración de reglas de alarma

Además de la supervisión automática y en tiempo real, puede configurar reglas de alarma en Cloud Eye para enviar notificaciones de alarma cuando se produzca una situación específica.

Consulta de métricas de monitoreo de OBS

Cloud Eye monitoriza las **métricas de monitoreo de OBS** en tiempo real. Puedes ver estadísticas de monitorización detalladas de cada métrica en la consola de Cloud Eye.

25.2 Métricas de monitoreo de OBS

Funciones

En esta sección se define el espacio de nombres, la lista y las dimensiones de las métricas de supervisión que OBS notifica a Cloud Eye. Puede utilizar la consola de gestión o la API proporcionada por Cloud Eye para buscar métricas de monitoreo y alarmas generadas por OBS.

Espacio de nombres

SYS.OBS

Métricas de monitoreo

ID de la métrica	Métrica	Descripción	Rango de valores	Entidad supervisada	Período de supervisión (métrica original)
download_bytes	Bytes descargados	Especifica los bytes de respuesta de todas las solicitudes de descarga realizadas a todos los bucket de una región, los bytes de que incluyen en los cuerpos de entidades de HTTP. Unidad: byte	≥ 0 bytes	Bucket	5 min
upload_bytes	Bytes cargados	Especifica los bytes de todas las solicitudes de carga realizadas a todos los bucket de una región, los bytes de que incluyen en los cuerpos de entidad HTTP. Unidad: byte	≥ 0 bytes	Bucket	5 min
get_request_count	Solicitudes de GET	Especifica el número de solicitudes de GET, HEAD u OPTIONS realizadas a todos los buckets y objetos de los buckets de una región. Unidad: Vez	≥ 0 vez	Bucket	5 min

ID de la métrica	Métrica	Descripción	Rango de valores	Entidad supervisada	Período de supervisión (métrica original)
put_request_count	Solicitudes de PUT	Especifica el número de solicitudes PUT, POST y DELETE realizadas a todos los bucket y objetos de los bucket de una región. Unidad: Vez	≥ 0 vez	Bucket	5 min
first_byte_latency	Retraso en la descarga de primer byte	Especifica el tiempo medio desde la recepción de una solicitud de GET, HEAD u OPTIONS hasta el tiempo que el sistema comienza a responder en un período de medición. Unidad: milisegundo	≥ 0 ms	Bucket	5 min
request_count_4xx	Errores 4*xx*	Especifica las veces que el servidor responde a las solicitudes cuyos códigos de error son 4xx. Unidad: Vez	≥ 0 vez	Bucket	5 min
request_count_5xx	Errores 5*xx*	Especifica las veces que el servidor responde a las solicitudes cuyos códigos de error son 5xx. Unidad: Vez	≥ 0 vez	Bucket	5 min

Dimensiones

Tabla 25-1 Dimensiones

Clave	Valor
bucket_name	Dimensión del bucket. El valor es el nombre del bucket.

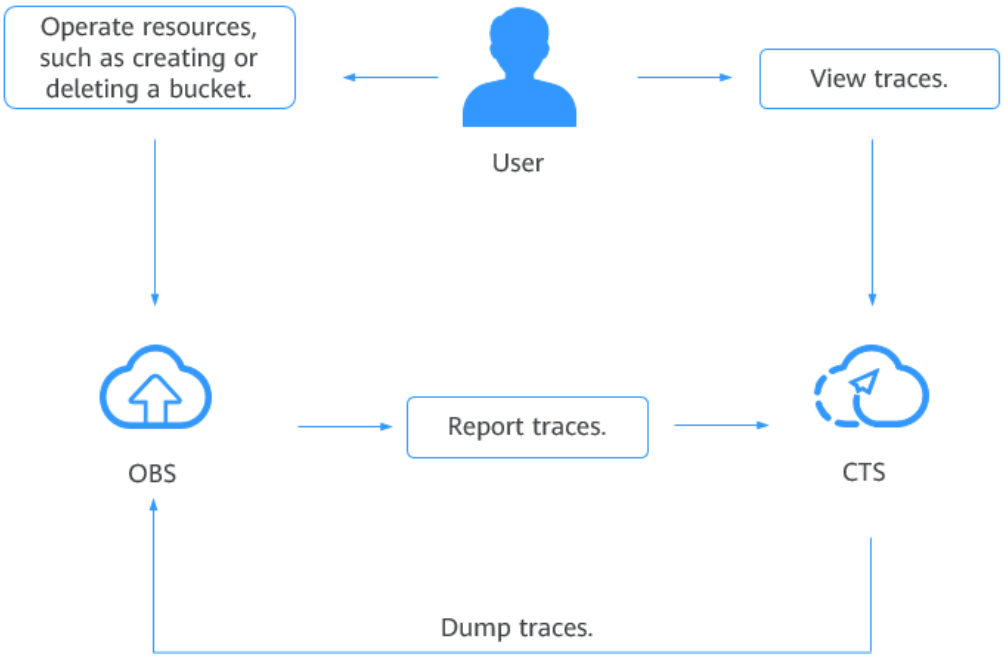
26 Cloud Trace Service

Cloud Trace Service (CTS) registra las operaciones en los recursos de la nube en su cuenta. Puede utilizar los registros para realizar análisis de seguridad, realizar un seguimiento de los cambios de recursos, auditar el cumplimiento y localizar fallos.

Después de habilitar CTS y configurar un rastreador, CTS puede registrar la gestión y las trazas de datos de OBS para su auditoría.

Para obtener más información acerca de cómo habilitar y configurar CTS, consulte **Habilitación de CTS**.

Figura 26-1 CTS



Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 En la esquina superior izquierda del menú de navegación superior, haga clic en  para seleccionar una región.

Paso 3 Elija **Service List** > **Management & Governance** > **Cloud Trace Service**. Se muestra la página **Trace List**.

Paso 4 Configure la auditoría en la nube para OBS haciendo referencia a **Configuración de un rastreador** en la *Guía de usuario de Cloud Trace Service*.

----Fin

Tabla 26-1 Operaciones de gestión de OBS registradas por CTS

Tipo de rastreador	Operación	Recurso	Nombre de seguimiento
Gestión	Eliminación de un bucket	bucket	deleteBucket
Gestión	Eliminación de la configuración de CORS de un bucket	bucket	deleteBucketCors
Gestión	Eliminar la configuración personalizada del nombre de dominio	bucket	deleteBucketCustomdo-main
Gestión	Eliminación de la configuración del ciclo de vida de un bucket	bucket	deleteBucketLifecycle
Gestión	Eliminación de una política de bucket	bucket	deleteBucketPolicy
Gestión	Eliminación de la configuración de replicación entre regiones de un bucket	bucket	deleteBucketReplication
Gestión	Eliminar la configuración de etiqueta de un bucket	bucket	deleteBucketTagging
Gestión	Eliminación de la configuración de alojamiento de sitios web estáticos de un bucket	bucket	deleteBucketWebsite
Gestión	Eliminación de datos de bucket	bucket	deleteBucketdata
Gestión	Creación de un bucket	bucket	createBucket

Tipo de rastreador	Operación	Recurso	Nombre de seguimiento
Gestión	Configuración de la ACL del bucket	bucket	setBucketAcl
Gestión	Configuración de la regla de CORS para un bucket	bucket	setBucketCors
Gestión	Configuración del nombre de dominio personalizado para un bucket	bucket	setBucketCustomdomain
Gestión	Configuración de las reglas del ciclo de vida de bucket	bucket	setBucketLifecycle
Gestión	Configuración de la función de registro de bucket	bucket	setBucketLogging
Gestión	Configuración de la función de notificación de eventos para bucket	bucket	setBucketNotification
Gestión	Configuración de la política de bucket	bucket	setBucketPolicy
Gestión	Configuración de la cuota de bucket	bucket	setBucketQuota
Gestión	Configuración de la función de replicación entre regiones para bucket	bucket	setBucketReplication
Gestión	Configuración de la clase de almacenamiento de bucket	bucket	setBucketStorageclass
Gestión	Configuración de la etiqueta de bucket	bucket	setBucketTagging
Gestión	Configuración de la función de control de versiones para bucket	bucket	setBucketVersioning
Gestión	Configuración del nombre de dominio estático para bucket	bucket	setBucketWebsite

Tipo de rastreador	Operación	Recurso	Nombre de seguimiento
Gestión	Configuración de la encriptación predeterminada de bucket	bucket	setBucketEncryption
Gestión	Eliminación de la configuración de encriptación predeterminada de bucket	bucket	deleteBucketEncryption

Tabla 26-2 Operaciones de datos de OBS registradas por CTS

Tipo de rastreador	Operación	Recurso	Nombre de seguimiento
Data_Read	Descarga de un objeto	object	GET.OBJECT
Data_Read	Consultar la ACL del objeto	object	GET.OBJECT.ACL
Data_Read	Consultar la configuración del sitio web del bucket	object	GET.OBJECT.WEBSITE
Data_Read	Acceso a un objeto a través del sitio web	object	HEAD.OBJECT.WEBSITE
Data_Read	Consultar los metadatos del objeto	object	HEAD.OBJECT
Data_Read	Listado de datos de piezas	object	LIST.OBJECT.UPLOAD
Data_Write	Eliminación de un objeto	object	DELETE.OBJECT
Data_Write	Cancelación de una pieza	object	DELETE.UPLOAD
Data_Write	Consulta las solicitudes entre dominios de objetos	object	OPTIONS.OBJECT
Data_Write	Carga de un objeto	object	POST.OBJECT
Data_Write	Supresión de objetos por lotes	object	POST.OBJECT.MULTIDELETE

Tipo de rastreador	Operación	Recurso	Nombre de seguimiento
Data_Write	Restaurar objetos de Archive	object	POST.OBJECT.RESTORE
Data_Write	Fusión de piezas	object	POST.UPLOAD.COMPLETE
Data_Write	Inicialización de tareas multiparte	object	POST.UPLOAD.INIT
Data_Write	Carga de un objeto	object	PUT.OBJECT
Data_Write	Configuración del objeto de ACL	object	PUT.OBJECT.ACL
Data_Write	Copiar un objeto	object	PUT.OBJECT.COPY
Data_Write	Configuración de la clase de almacenamiento de objetos	object	PUT.OBJECT.STORAGECLASS
Data_Write	Carga de una pieza	object	PUT.PART
Data_Write	Copia de una pieza	object	PUT.PART.COPY

Procedimiento de seguimiento

Puede hacer clic en **Disable** debajo de la columna **Operation** a la derecha de un rastreador para deshabilitar el rastreador. Después de deshabilitar el rastreador, el sistema detendrá las operaciones de grabación, pero aún puede ver los registros de operaciones existentes.

Puede hacer clic en **Delete** debajo de la columna **Operation** a la derecha de un rastreador para eliminar el rastreador. La eliminación de un rastreador no tiene ningún impacto en los registros de operaciones existentes. Cuando vuelva a activar CTS, puede ver los registros de operaciones que se han generado.

27 Configuración de una política de descompresión en línea

Puede comprimir varios archivos en un paquete ZIP y luego subirlo a OBS para descompresión automática en línea.

Para lograr la descompresión en línea, configure una política de descompresión antes de cargar un paquete. Si un paquete cargado coincide con la política configurada, OBS descomprime automáticamente el paquete. Las políticas de descompresión no se aplican a los paquetes ZIP que ya existen en OBS antes de crear las políticas.

Puede crear políticas de descompresión en línea o replicar políticas de descompresión en línea existentes desde otro bucket.

NOTA

Actualmente, la descompresión en línea solo está disponible en las regiones CN North-Beijing4, CN South-Guangzhou y CN East-Shanghai1.

Creación de una política de descompresión en línea

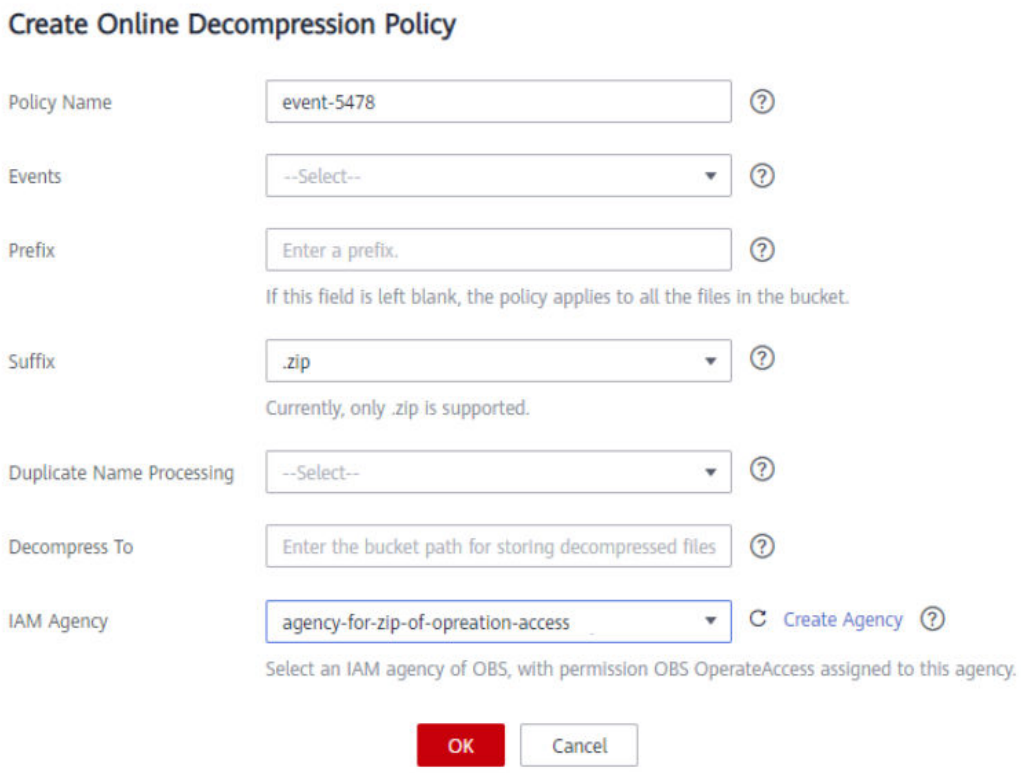
Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Data Processing** > **Online Decompression**. Se muestra la página **Online Decompression**.

Paso 4 Haga clic en **Create**. Se muestra el cuadro de diálogo mostrado en **Figura 27-1**.

Figura 27-1 Crear política de descompresión en línea



Paso 5 Configure la política de descompresión en línea. **Tabla 27-1** describe los parámetros relacionados.

Tabla 27-1 Descripción del parámetro

Parámetro	Descripción
Policy Name	Escriba un nombre de política que sea fácil de recordar. El valor puede contener de 1 a 256 caracteres, y solo se permiten letras mayúsculas y minúsculas, dígitos, guiones bajos (_), y guiones (-). Por ejemplo, **event_0001**.

Parámetro	Descripción
Events	Eventos para los que desea activar la política de descompresión en línea. Actualmente, se admiten los siguientes tipos de eventos: ● **ObjectCreated**: todo tipo de operaciones de creación de objetos, incluidos PUT, POST y COPY de objetos, así como las partes de fusión de tareas multiparte ● **Put**: carga de objetos mediante PUT ● **Post**: carga de objetos mediante POST ● **Copy**: copia de objetos mediante COPY ● **CompleteMultipartUpload**: fusión de partes de tareas de varias partes **NOTA** Para descomprimir el paquete ZIP que contiene otros paquetes ZIP, establezca el tipo de evento en **ObjectCreated** o **CompleteMultipartUpload**.
Prefix	Opcional. Si este parámetro está configurado, la política de descompresión se aplica a los paquetes cuyo nombre contiene este prefijo. El prefijo no puede comenzar con una barra (/) o contener barras dobles (//), o contener caracteres especiales (\ : * ? " < > |). La longitud total del prefijo y del sufijo no puede superar los 1024 caracteres. ● Con este parámetro configurado, los paquetes ZIP cuyo nombre contiene el prefijo especificado activarán la descompresión en línea. ● Con este parámetro dejado en blanco, la política de descompresión se aplica a todos los paquetes ZIP cargados. **ATENCIÓN** – Se recomienda configurar un prefijo. De lo contrario, puede producirse una descompresión cíclica si un paquete contiene otros paquetes. – El prefijo configurado debe contener todos los niveles del directorio para almacenar el objeto. Por ejemplo, hay un objeto **example123** que se almacena en **bucket/file/example123**. Si desea que **example** sea el prefijo, establezca el prefijo en **file/example**.
Suffix	Si se especifica este parámetro, la política de descompresión se aplica a los paquetes cuyo nombre contiene este sufijo. Actualmente, solo se admiten paquetes ZIP.

Parámetro	Descripción
Duplicate Name Processing	This parameter specifies how the decompressed objects are processed if they have the same names as the existing objects in the bucket. ● **Do not decompress**: Retains the existing objects in the bucket, and does not decompress the objects with the same name. ● **Rename the file**: Renames the decompressed objects with the CRC32 value. ● **Overwrite**: Overwrites the existing objects with the same name in the bucket.
Decompress To	Opcional, este parámetro especifica la ruta de acceso para almacenar archivos descomprimidos. No puede contener caracteres especiales (\:*?\<>|), empezar o terminar con un punto (.), ni contener dos o más barras diagonales consecutivas (/). El valor puede contener de 0 a 1023 caracteres. ● Con este parámetro configurado, la ruta debe terminar con una barra diagonal (/). Después de descomprimir un paquete ZIP, los archivos descomprimidos se almacenan en la carpeta con el mismo nombre que la ruta. Si no hay dicha carpeta en el bucket, el sistema crea automáticamente una para almacenar los archivos descomprimidos. ● Con este parámetro dejado en blanco, los objetos descomprimidos se almacenan en el directorio principal del bucket.
IAM Agency	Seleccione una delegación IAM de OBS, con el permiso OBS OperateAccess asignado a esta delegación. Si no hay tal delegación disponible, cree una.

Paso 6 Haga clic en **OK**. Se crea la política de descompresión en línea.

----Fin

Replicación de políticas de descompresión en línea

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Data Processing** > **Online Decompression**. Se muestra la página **Online Decompression**.

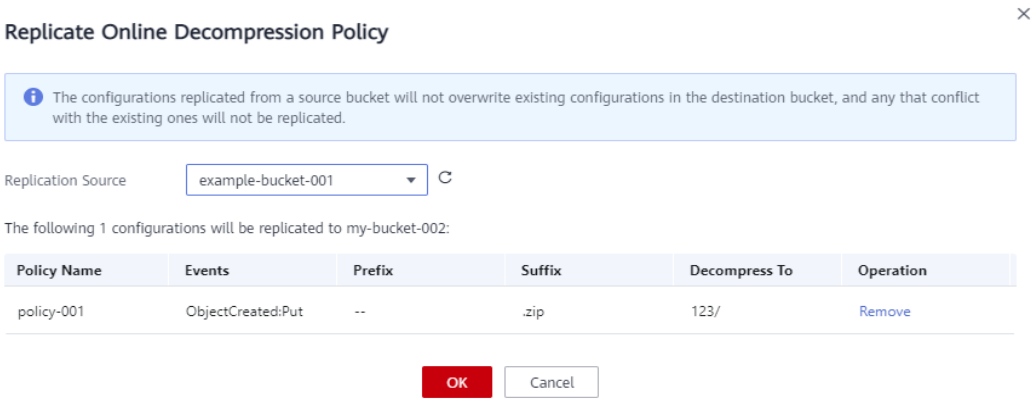
Paso 4 Haga clic en **Replicate**.

Paso 5 Seleccione un origen de replicación, es decir, el bucket de origen para el que se configuraron las políticas de descompresión en línea.

NOTA

- Las políticas de descompresión en línea replicadas desde un bucket de origen no sobrescribirán las políticas existentes en el bucket de destino y no se replicarán las que entren en conflicto con las existentes.
- La versión de los bucket de origen y destino debe ser 3.0.
- Puede quitar las políticas que no desea replicar.
- Puede haber 10 políticas de descompresión en línea como máximo en un bucket. Si el número de políticas que replicará más el número de políticas existentes en el bucket de destino supera 10, la replicación fallará. Antes de replicar las políticas, elimine algunas si es necesario.

Figura 27-2 Replicación de políticas de descompresión en línea



Paso 6 Haga clic en **OK** para replicar las políticas de descompresión en línea en el bucket de destino.

----Fin

28 Uso de visualización

En OBS Console, puede ver el almacenamiento, el tráfico y las solicitudes de un único bucket o de todos los bucket.

NOTA

Para ver el uso, debe configurar la política **ces:metricData:list** en un proyecto regional. Para obtener más información, consulte **Políticas personalizadas de Cloud Eye**.

Consulta de métricas

En la página **Metrics**, puede ver el almacenamiento, el tráfico y las solicitudes de un solo bucket.

Paso 1 En el panel de navegación de **OBS Console**, elija **Object Storage**.

Paso 2 En la lista de bucket, haga clic en el nombre del bucket que desee. Se muestra la página **Objects**.

Paso 3 En el panel de navegación, elija **Metrics**.

Paso 4 Seleccione un tipo de métrica y un período para ver estadísticas relacionadas, como se muestra en **Figura 28-1**.

Figura 28-1 Consulta de métricas

En el gráfico, puede:

- Elija una o más leyendas para mostrar lo que desea ver.

- Mueva el puntero del ratón sobre la línea estadística para ver las estadísticas de cada elemento en un punto específico en el tiempo.

----Fin

29 Gestión de tareas

Al cargar objetos, eliminar carpetas, restaurar objetos por lotes o cambiar clases de almacenamiento por lotes, los registros correspondientes de las tareas se mostrarán en el centro de tareas para que pueda ver el progreso y el estado de las tareas.

NOTA

Cuando se vuelve a cargar la página web, se perderán los registros de tareas de la lista de gestión de tareas.

Procedimiento

Paso 1 En la lista de objetos de su bucket, haga clic en **Task Center** en la esquina superior derecha.

Paso 2 Vea los registros de carga de objetos, eliminación de carpetas, restauración de objetos por lotes o cambio de clases de almacenamiento por lotes.

- Haga clic en **Clear Records** para borrar todos los registros de tareas.
- En la página de la ficha **Upload**, puede hacer clic en **Pause All** o **Start All** para gestionar las tareas de carga por lotes.

----Fin

30 Operaciones relacionadas

30.1 Creación de una delegación de IAM

Para usar algunas características de OBS, debe usar delegaciones de IAM para conceder los permisos necesarios a OBS para procesar sus datos.

Creación de una delegación para la replicación entre regiones

Paso 1 En el cuadro de diálogo **Create Cross-Region Replication Rule** de OBS Console, haga clic en **View IAM agencies** para ir a la página **Agencies** de la consola de IAM.

Paso 2 Haga clic en **Create Agency** para crear una delegación.

Paso 3 Ingrese el nombre de una delegación.

Paso 4 Seleccione **Cloud service** para el **Agency Type**.

Paso 5 Seleccione **Object Storage Service (OBS)** para **Cloud Service**.

Paso 6 Establezca un período de validez.

Paso 7 Haga clic en **Next**.

NOTA

La consola para crear una delegación tiene las ediciones nuevas y antiguas. Aquí se describe cómo crear una delegación en la consola de la nueva edición.

Paso 8 En la página **Select Policy/Role**, seleccione **Tenant Administrator** y haga clic en **Next**.

Paso 9 En la página **Select Scope**, seleccione **Global services** para **Scope** y haga clic en **OK**.

Paso 10 (Opcional) Si se selecciona **Replicate KMS encrypted objects**, la delegación de IAM también necesita los permisos **KMS Administrator** en las regiones donde se encuentran los bucket de origen y destino.

1. Vaya a la página **Agencies** de la consola de **Identity and Access Management** y haga clic en el nombre de la delegación creada en el paso anterior.
2. En la página de ficha **Agency Permissions**, haga clic en **Assign Permissions**.
3. En el área **Scope**, seleccione **Region-specific projects** y seleccione los proyectos en las regiones donde residen los bucket de origen y destino.

4. En el área **Permissions**, busque y seleccione **KMS Administrator** y haga clic en **OK**.

----Fin

Creación de una delegación para cargar registros

Paso 1 En el cuadro de diálogo **Logging**, haga clic en **Create Agency** para ir a la página **Agencies** en la consola de **Identity and Access Management**.

Paso 2 Haga clic en **Create** para crear una delegación.

Paso 3 Ingrese el nombre de una delegación.

Paso 4 Seleccione **Cloud service** para el **Agency Type**.

Paso 5 Seleccione **Object Storage Service (OBS)** como el servicio en la nube.

Paso 6 Establezca un período de validez.

Paso 7 Haga clic en **Next**.

Paso 8 En la página **Select Policy/Role**, seleccione una política personalizada que tenga el permiso para cargar datos en el bucket de almacenamiento de registros y haga clic en **Next**.

Si no hay ninguna política personalizada disponible, cree una haciendo referencia a **Creación de una política personalizada**.

Cuando cree una política personalizada, seleccione **Global services** para **Scope** y seleccione **JSON** para **Policy View**. El contenido de la política es el siguiente.

NOTA

Cuando codifique el contenido de la política en un escenario real, reemplace **mybucketlogs** con el nombre de bucket actual:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "obs:object:PutObject"
            ],
            "Resource": [
                "OBS:*:*:object:mybucketlogs/*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Paso 9 En la página **Select Scope**, seleccione **Global services** para **Scope** y haga clic en **OK**.

Paso 10 (Opcional) Si la encriptación predeterminada está habilitada para el bucket de almacenamiento de registro, la delegación de IAM también requiere el permiso **KMS Administrator** en la región donde reside el bucket de almacenamiento de registro.

1. Vaya a la página **Agencies** de la consola de **Identity and Access Management** y haga clic en el nombre de la delegación creada en el paso anterior.
2. En la página de ficha **Agency Permissions**, haga clic en **Assign Permissions**.
3. En el área **Scope**, seleccione **Region-specific projects** y seleccione los proyectos en la región donde reside el bucket de registro.

4. En el área **Permissions**, busque y seleccione **KMS Administrator** y haga clic en **OK**.

----Fin

31 Solución de problemas

31.1 Un objeto no se puede descargar mediante Internet Explorer 11

Síntoma

Un usuario inicia sesión en OBS Console mediante Internet Explorer 11 y carga un objeto. Cuando el usuario intenta descargar el objeto a la ruta original para reemplazar el objeto original sin cerrar el navegador, se muestra un mensaje que indica un fallo de descarga. ¿Por qué sucede esto?

Por ejemplo, un usuario carga el objeto **abc** desde el directorio raíz de la unidad local C a un bucket en OBS Console. Cuando el usuario intenta descargar el objeto al directorio raíz de la unidad local C para reemplazar el objeto original sin cerrar el navegador, aparece un mensaje que indica que no se pudo descargar.

Respuesta

Este problema se debe a la incompatibilidad del navegador. Se puede resolver utilizando un navegador web diferente.

Si se produce este problema, cierre el navegador e inténtelo de nuevo.

31.2 No se puede abrir OBS Console en Internet Explorer 9

Pregunta

¿Por qué no se puede abrir OBS Console en Internet Explorer 9, incluso si la dirección de OBS Console se puede hacer ping?

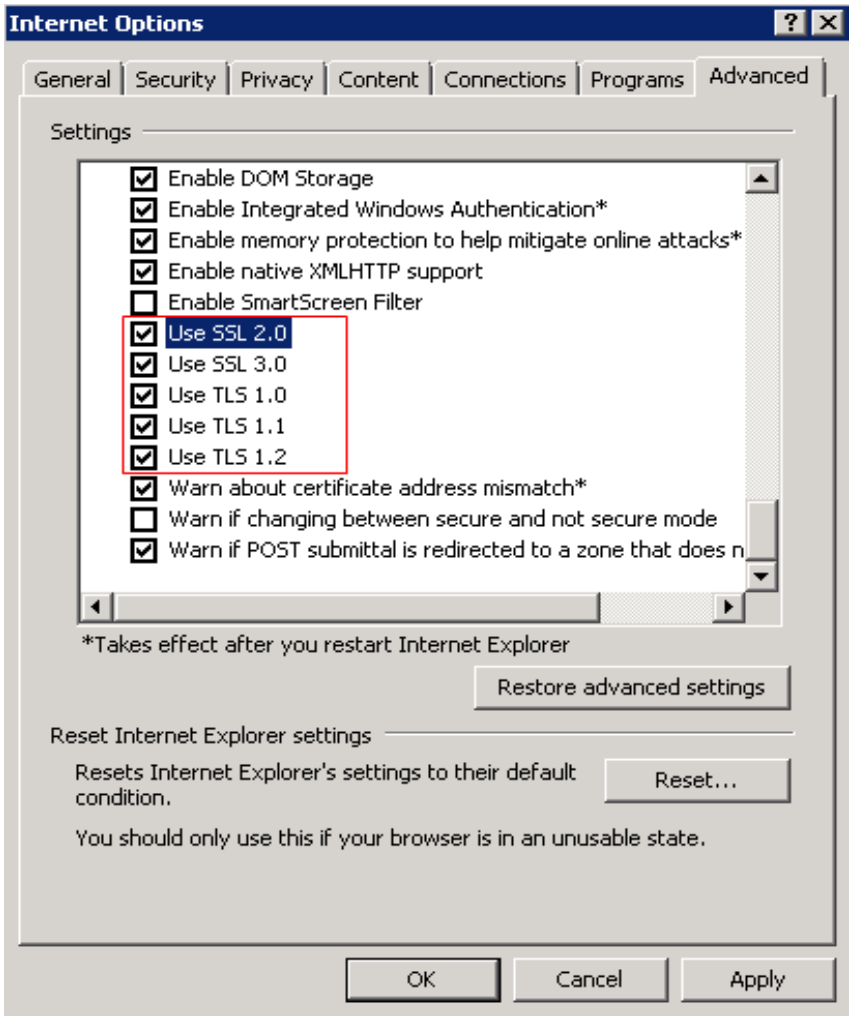
Respuesta

Confirme si **Use SSL** y **Use TLS** están seleccionados en **Internet Options**. Si no es así, realice el siguiente procedimiento e inténtelo de nuevo:

Paso 1 Abre Internet Explorer 9.

Paso 2 Haga clic en **Tools** en la esquina superior derecha y elija **Internet Options** > **Advanced**. A continuación, seleccione **Use SSL 2.0**, **Use SSL 3.0**, **Use TLS 1.0**, **Use TLS 1.1** y **Use TLS 1.2** como se muestra en **Figura 31-1**.

Figura 31-1 Opciones de Internet



Paso 3 Haga clic en **OK**.

----Fin

31.3 El nombre del objeto cambia después de que un objeto con un nombre largo se descarga en un equipo local

Pregunta

Después de descargar un objeto con un nombre relativamente largo en una ruta local, el nombre del objeto cambia.

Respuesta

Para Windows, un nombre de archivo, incluida la extensión de nombre de archivo, puede contener un máximo de 255 caracteres. Cuando un objeto cuyo nombre contiene más de 255 caracteres se descarga en un equipo local, el sistema mantiene solo los primeros 255 caracteres automáticamente.

31.4 Failed to Configure Event Notification

Question

When configuring event notification on OBS, the user is prompted by the message "OBS is not authorized to use this topic. Go to SMN to authorize OBS to use this topic."

Answer

Go to the SMN console. On the **Configure Topic Policy** page, select **OBS** under **Services that can publish messages to this topic**.

For details about how to use the SMN service, see "Topic Policy" in the *SMN User Guide*.

31.5 La diferencia horaria es superior a 15 minutos entre el cliente y el servidor

Pregunta

El mensaje de error "La diferencia de tiempo es mayor de 15 minutos entre el cliente y el servidor" o "La diferencia entre la hora de solicitud y la hora actual es demasiado grande" se muestra durante el uso de OBS.

Respuesta

Por motivos de seguridad, OBS verifica la diferencia de tiempo entre el cliente y el servidor. Si la diferencia de tiempo es superior a 15 minutos, el servidor de OBS rechazará sus solicitudes y se notifica este mensaje de error. Para resolver este problema, ajuste la hora local (UTC) e inténtelo de nuevo.

32 Lista de códigos de error

Si una solicitud no se procesa debido a errores, se devuelve una respuesta de error. Una respuesta de error contiene un código de error y detalles de error. **Tabla 32-1** enumera algunos códigos de error comunes en las respuestas de error de OBS.

Tabla 32-1 Códigos de error de OBS

Código de error	Descripción
Obs.0000	Parámetro no válido.
Obs.0001	Ninguna de las solicitudes de acceso a este objeto es válida.
Obs.0002	La ruta de acceso absoluta de un archivo no puede exceder de 1023 caracteres. Vuelva a intentarlo.
Obs.0003	Finalizó el tiempo de espera de la conexión.
Obs.0004	La diferencia de la hora entre el cliente y el servidor es superior a 15 minutos. Establezca correctamente la hora local. Por motivos de seguridad, OBS verifica el desfase de tiempo entre el cliente y el servidor. Si el offset es superior a 15 minutos, el servidor OBS rechazará sus solicitudes y se notifica este mensaje de error. Para resolver este problema, ajuste la hora local (UTC) e inténtelo de nuevo.
Obs.0005	La carga del servidor es demasiado pesada. Vuelva a intentarlo más tarde.
Obs.0006	La cantidad de buckets alcanzó el límite superior. Una cuenta (incluidos todos los usuarios de IAM de esta cuenta) puede crear un máximo de 100 buckets y sistemas de archivos paralelos. Puede utilizar el control de acceso de grano fino de OBS para planificar y usar adecuadamente los bucket.
Obs.0007	El bucket objetivo no existe o no está en la misma región que el bucket actual.
Obs.0008	La cuenta no se ha registrado en el sistema. Solo se puede usar una cuenta registrada.

Código de error	Descripción
Obs.0009	Una de las operaciones que se está ejecutando en este recurso está ocasionando un conflicto. Vuelva a intentarlo. Esto se debe a que hay un bucket con el mismo nombre que el bucket que está creando en OBS y el bucket existente ha sido liberado en el período reciente debido a atrasos. En tal caso, pruebe con otro nombre de bucket.
Obs.0010	Error en la eliminación. Compruebe si el bucket contiene objetos u objetos de versiones históricas.
Obs.0011	La política de bucket no es válida. Configúrela nuevamente.
Obs.0012	El nombre del bucket solicitado ya existe. El espacio de nombres del bucket es compartido por todos los usuarios del sistema. Introduzca un nombre diferente e inténtelo de nuevo.
Obs.0013	El nombre de la carpeta solicitada ya existe. Introduzca un nombre diferente e inténtelo de nuevo.
Obs.0014	El tamaño del archivo ha excedido los 50 MB. Use OBS Browser+ para subirlo.
Obs.0015	La ruta de acceso absoluta en los criterios de búsqueda no puede superar los 1023 caracteres. Vuelva a intentarlo.
Obs.0016	Error en la carga. Causas posibles: 1. Estado anormal de la red. 2. Tiene permisos incorrectos o no tiene permisos para escribir el bucket. 3. Su cuenta está en mora o no tiene saldo suficiente. 4. Su cuenta ha sido suspendida.
Obs.0017	La fecha y la hora del período de validez nuevo deben ser posteriores a las del período de validez anterior.
Obs.0018	El período de validez no puede ser inferior al período restante.
Obs.0019	No se puede determinar si el bucket tiene objetos o fragmentos. Verifique si cuenta con permiso de lectura para este bucket.
Obs.0020	Error del sistema de TMS. Vuelva a intentarlo más tarde.
Obs.0021	No tiene permisos para acceder al TMS. Utilice IAM para agregar el permiso para acceder a TMS.
Obs.0022	El sistema de TMS está ocupado. Vuelva a intentarlo más tarde.

