

Object Storage Service

Console Operation Guide

Issue 31
Date 2023-11-16



Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

| | |
|----------------------------------------------------------------|-----------|
| 1 Console Function Overview | 1 |
| 2 Web Browser Compatibility | 4 |
| 3 Getting Started | 5 |
| 3.1 Process Description | 5 |
| 3.2 Configuring User Permissions | 6 |
| 3.3 Logging In to OBS Console | 7 |
| 3.4 Creating a Bucket | 8 |
| 3.5 Uploading an Object | 12 |
| 3.6 Downloading an Object | 15 |
| 3.7 Deleting an Object | 16 |
| 3.8 Deleting a Bucket | 17 |
| 4 Managing Buckets | 19 |
| 4.1 Creating a Bucket | 19 |
| 4.2 Viewing Basic Information of a Bucket | 24 |
| 4.3 Searching for a Bucket | 30 |
| 4.4 Deleting a Bucket | 32 |
| 5 Managing Objects | 33 |
| 5.1 Uploading an Object | 33 |
| 5.2 Downloading an Object | 36 |
| 5.3 Managing Folders | 37 |
| 5.3.1 Creating a Folder | 37 |
| 5.3.2 Sharing a Folder | 38 |
| 5.4 Other Object Operations | 41 |
| 5.4.1 Listing Objects | 41 |
| 5.4.2 Searching for an Object or Folder | 42 |
| 5.4.3 Accessing an Object Using Its URL | 45 |
| 5.4.4 Sharing an Object | 46 |
| 5.4.5 Restoring an Object from Archive or Deep Archive Storage | 48 |
| 5.4.6 Configuring Direct Reading | 50 |
| 5.4.7 Configuring Object Metadata | 51 |
| 5.5 Deleting Objects | 52 |
| 5.5.1 Deleting an Object or Folder | 52 |

| | |
|---------------------------------------------------------------|------------|
| 5.5.2 Undeleting an Object..... | 55 |
| 5.5.3 Managing Fragments..... | 58 |
| 6 Permissions Control..... | 60 |
| 6.1 Configuring IAM Permissions..... | 60 |
| 6.1.1 Creating an IAM User and Granting OBS Permissions..... | 60 |
| 6.1.2 OBS Custom Policies..... | 61 |
| 6.1.3 OBS Resources..... | 64 |
| 6.1.4 OBS Request Conditions..... | 65 |
| 6.2 Configuring a Bucket Policy..... | 65 |
| 6.2.1 Creating a Bucket Policy with a Template..... | 65 |
| 6.2.2 Creating a Custom Bucket Policy (Visual Editor)..... | 78 |
| 6.2.3 Creating a Custom Bucket Policy (JSON View)..... | 82 |
| 6.2.4 Replicating Bucket Policies..... | 83 |
| 6.3 Configuring an Object Policy..... | 84 |
| 6.4 Configuring a Bucket ACL..... | 85 |
| 6.5 Configuring an Object ACL..... | 86 |
| 7 Data Management..... | 89 |
| 7.1 Configuring a Lifecycle Rule..... | 89 |
| 7.2 Configuring Tags for a Bucket..... | 93 |
| 7.3 Configuring a Bucket Inventory..... | 94 |
| 7.4 Viewing Usage..... | 96 |
| 8 Data Access..... | 98 |
| 8.1 Static Website Hosting..... | 98 |
| 8.1.1 Configuring Static Website Hosting..... | 98 |
| 8.1.2 Configuring Redirection..... | 104 |
| 8.2 Configuring a Back-to-Source Rule..... | 107 |
| 8.3 Configuring a User-Defined Domain Name..... | 113 |
| 9 Data Security..... | 117 |
| 9.1 Configuring Server-Side Encryption..... | 117 |
| 9.1.1 Configuring Bucket Default Encryption..... | 117 |
| 9.1.2 Uploading an Object in Server-Side Encryption Mode..... | 119 |
| 9.2 Configuring WORM Retention..... | 121 |
| 9.3 Configuring CORS..... | 127 |
| 9.4 Configuring Versioning..... | 131 |
| 9.5 Configuring Cross-Region Replication..... | 133 |
| 9.6 Configuring URL Validation..... | 137 |
| 10 Data Processing..... | 139 |
| 10.1 Configuring an Online Decompression Policy..... | 139 |
| 11 Monitoring and Logging..... | 144 |
| 11.1 Monitoring..... | 144 |

| | |
|----------------------------------------------------------------------------------------------------------|------------|
| 11.1.1 Monitoring OBS..... | 144 |
| 11.1.2 OBS Monitoring Metrics..... | 145 |
| 11.2 Cloud Trace Service..... | 147 |
| 11.3 Configuring Access Logging for a Bucket..... | 151 |
| 12 Managing Resource Packages..... | 154 |
| 13 Task Center..... | 156 |
| 14 Related Operations..... | 157 |
| 14.1 Creating an IAM Agency..... | 157 |
| 15 Troubleshooting..... | 160 |
| 15.1 An Object Fails to Be Downloaded Using Internet Explorer 11..... | 160 |
| 15.2 OBS Console Cannot Be Opened in Internet Explorer 9..... | 160 |
| 15.3 The Object Name Changes After an Object with a Long Name Is Downloaded to a Local Computer | 161 |
| 15.4 Time Difference Is Longer Than 15 Minutes Between the Client and Server..... | 162 |
| 16 Error Code List..... | 163 |
| 17 Change History..... | 165 |

1 Console Function Overview

Table 1-1 lists functions provided by OBS Console.

Table 1-1 OBS Console functions

| Function | Description |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic bucket operations | Allow you to create and delete buckets of different storage classes in specified regions (service areas), copy existing bucket configurations, as well as change bucket storage classes. |
| Basic object operations | Allow you to manage objects, including uploading (multipart uploads included), downloading, sharing, and deleting objects, as well as changing object storage classes and restoring Archive objects. |
| Server-side encryption | Encrypts objects on the server side to enhance security of objects stored on OBS. |
| WORM | Protects objects from being deleted or tampered with within a specified period. |
| Object metadata | Allows you to set properties for objects. |
| Monitoring | <ul style="list-style-type: none">• Cloud Eye can monitor the following OBS metrics:<ul style="list-style-type: none">- Download Traffic- Upload Traffic- GET Requests- PUT Requests- First Byte Download Delay- 4xx Errors- 5xx Errors |
| Auditing | With Cloud Trace Service (CTS), you can record data operations associated with OBS for later query, audit, and backtrack operations. |

| Function | Description |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fragment management | Manages and clears fragments generated due to object upload failures. |
| Versioning | Stores multiple versions of an object in the same bucket. |
| Logging | Logs bucket access requests for analysis and auditing. |
| Permission control | Controls access to OBS using IAM permissions, bucket/object policies, and bucket/object access control lists (ACLs). |
| Lifecycle management | Allows you to configure lifecycle rules to periodically expire and delete objects or transition objects between storage classes. |
| Cross-region replication | Implements object replication across regions under the same account. A cross-region replication rule enables OBS to automatically, asynchronously copy data from a source bucket in one region to a destination bucket in a different region. This provides disaster recovery across regions, catering to your needs for remote backup. |
| Tags | Help you identify and classify buckets in OBS. |
| Static website hosting | Supports the hosting of static websites in buckets and the redirection of access requests for buckets. |
| User-defined domain name configuration | Enables you to bind your website domain name to a bucket domain name. If you want to migrate files from your website to OBS while keeping the website address unchanged, you can use this function. |
| Back to source | Helps you obtain the requested data from the source site if the data is not found in OBS. Usually, if the data you requested is not found in OBS, a 404 error will be returned. |
| URL validation | Prevents object links in OBS from being stolen by other websites. |
| Cross origin resource sharing | Allows a web client in one origin to interact with resources in another one. Cross origin resource sharing (CORS) is a browser-standard mechanism defined by the World Wide Web Consortium (W3C). For general web page requests, website scripts and contents in one origin cannot interact with those in another because of Same Origin Policies (SOPs). |

| Function | Description |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Direct reading | Allows you to directly download objects in the Archive storage class without restoring them first. Direct reading is a billable function. |
| Bucket inventory | Periodically provides CSV files that list object information in the bucket and delivers the CSV files to the specified bucket. |

2 Web Browser Compatibility

Table 2-1 lists the web browser versions compatible with OBS Console.

Table 2-1 Supported web browser versions

| Web Browser | Version |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Internet Explorer | <ul style="list-style-type: none">• Internet Explorer 9 (IE9)• Internet Explorer 10 (IE10)• Internet Explorer 11 (IE11) |
| Firefox | Firefox 55 and later |
| Chrome | Chrome 60 and later |

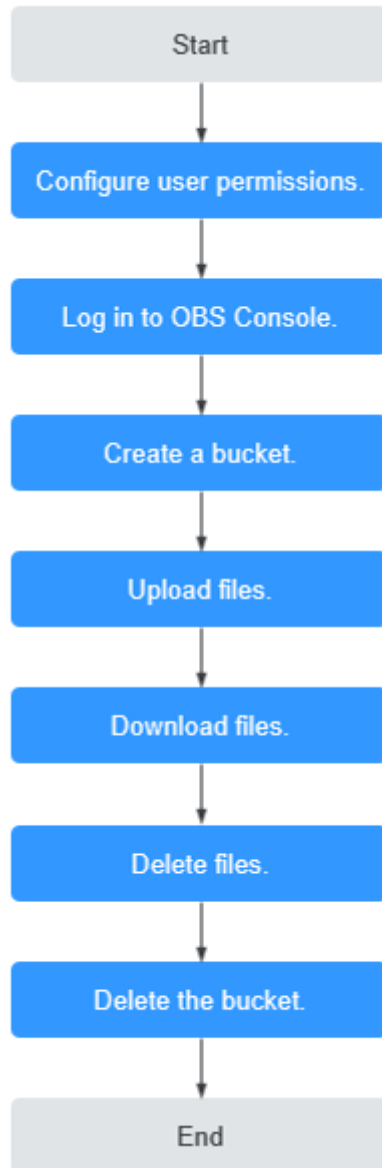
3 Getting Started

3.1 Process Description

OBS basic operations include bucket creation, object upload and object download.

The follow-up sections describe how to complete the tasks illustrated in [Figure 3-1](#).

Figure 3-1 OBS Console quick start



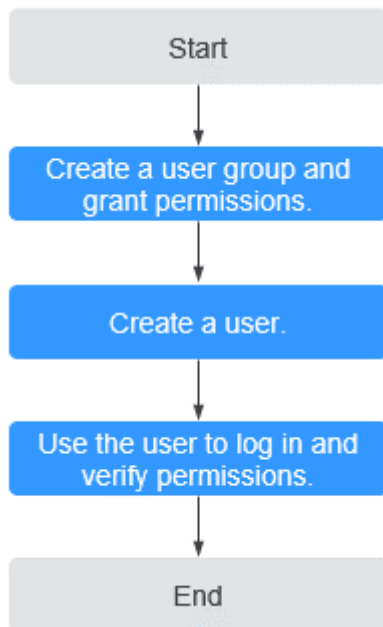
3.2 Configuring User Permissions

If your cloud service account does not need individual IAM users, then you may skip this section. Your permissions to use OBS functions are not affected.

OBS is separately deployed from other cloud resources. If IAM users are required, you need to grant them access permissions for OBS.

Process

Figure 3-2 Process of granting an IAM user the OBS permissions



The below example describes how to grant an IAM user the **Tenant Guest** permission for OBS.

1. **Create a user group and assign permissions.**
Create a user group on the IAM console, and assign the group the **Tenant Guest** permission.
2. **Create an IAM user and add it to the user group.**
Create a user on the IAM console and add the user to the group created in **1**.
3. **Log in** and verify the permission granting.
Log in to OBS Console using the newly created user, and verify that the assigned permission has taken effect:
 - Choose **Object Storage Service** from the service list to go to the OBS homepage. If the list of buckets is displayed and you can view the basic information about any bucket, but you cannot create or delete buckets or perform any other operations, the granted **Tenant Guest** permission has already taken effect.
 - Go to an OBS bucket. If the list of objects is displayed and you can download objects, but you cannot upload or delete objects or perform any other operations, the **Tenant Guest** permission granted has already taken effect.

3.3 Logging In to OBS Console

You can log in to OBS Console using a web browser.

Procedure

Step 1 Visit the [Huawei Cloud official website](#).

Step 2 Create a HUAWEI ID.

If you already have one, start from [Step 3](#).

1. On the right of the top navigation menu, click **Register**.
2. Complete the creation as instructed.

After the creation is complete, you will be navigated to your ID information page.

Step 3 On the right of the top navigation menu, click **Log In**, and enter the username and password.

Step 4 On the right of the top navigation bar, click **Console** to go to the management console.

Step 5 In the upper left corner of the navigation pane, click  and choose **Storage > Object Storage Service**. The OBS Console page is displayed.

Step 6 (Recommended) Top up your account or buy OBS resource packages, for you to properly use OBS.

----End

3.4 Creating a Bucket

This section describes how to create a bucket on OBS Console. A bucket is a container that stores objects in OBS. Before you can store data in OBS, you must create a bucket.

NOTE

An account (including all IAM users under this account) can create a maximum of 100 buckets and parallel file systems. You can use the fine-grained access control of OBS to properly plan and use buckets. For example, you can create folders in a bucket based on object prefixes and use [fine-grained permission control](#) to implement permission isolation between departments.

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the upper right corner, click **Create Bucket**. The **Create Bucket** page is displayed. For details, see [Figure 3-3](#).

Figure 3-3 Creating a bucket

Step 3 Configure bucket parameters.

Table 3-1 Bucket parameters

| Parameter | Description |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Replicate Existing Settings | Optional. To use this function, click Select Bucket and select a bucket from the list as the replication source. After the replication source is selected, the following settings are replicated to the bucket you are creating: region, data redundancy policy, storage class, bucket policy, server-side encryption, direct reading, enterprise project, and tags. You can still change some or all of the replicated settings as needed. |
| Region | Geographic area where a bucket resides. For low latency and faster access, select the region nearest to you. Once the bucket is created, its region cannot be changed. Most OBS features are available in all regions, but some are only available for certain regions. Consider the feature availability in each region when you select a region for a bucket. For details, see Function Overview . If your ECS needs to access an OBS bucket over the intranet, ensure that the bucket and the ECS are in the same region. For details, see Accessing OBS over an Intranet . |

| Parameter | Description |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bucket Name | <p>Name of the bucket. A bucket name must be unique across all accounts and regions. Once a bucket is created, its name cannot be changed.</p> <p>According to the globally applied DNS naming rules, an OBS bucket name:</p> <ul style="list-style-type: none"> • Must be unique across all accounts and regions. The name of a deleted bucket can be reused for another bucket or a parallel file system at least 30 minutes after the deletion. • Must be 3 to 63 characters long. Only lowercase letters, digits, hyphens (-), and periods (.) are allowed. • Cannot start or end with a period (.) or hyphen (-), and cannot contain two consecutive periods (..) or contain a period (.) and a hyphen (-) adjacent to each other. • Cannot be formatted as an IP address. <p>NOTE When you access OBS through HTTPS using virtual hosted-style URLs, if the bucket name contains a period (.), the certificate verification will fail. To work around this issue, you are advised not to use periods (.) in bucket names.</p> |
| Data Redundancy Policy | <ul style="list-style-type: none"> • Multi-AZ storage: Data is stored in multiple AZs to achieve higher reliability. • Single-AZ storage: Data is stored in a single AZ, with lower costs. <p>For details about the performance comparison between multi-AZ and single-AZ storage, see Comparison of Storage Classes.</p> <p>Once a bucket is created, the data redundancy policy cannot be changed, so choose the policy that can meet your needs.</p> <ul style="list-style-type: none"> • Multi-AZ storage is not available for buckets in the Archive storage class. • Multi-AZ storage is not available for buckets in the Deep Archive storage class. |

| Parameter | Description |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Storage Class | <p>Storage classes of a bucket. Different storage classes meet different requirements for storage performance and costs.</p> <ul style="list-style-type: none"> • The Standard storage class is for storing a large number of hot files or small files that are frequently accessed (multiple times per month on average) and require quick retrieval. • The Infrequent Access storage class is for storing data that is less frequently accessed (less than 12 times per year on average) and requires quick retrieval. • The Archive storage class is for archiving data that is rarely accessed (once a year on average) and has no requirements for quick retrieval. • The Deep Archive storage class is for storing data that is rarely accessed (a lower frequency than the archived data) and has no requirements for quick retrieval. <p>For details, see Storage Classes.</p> |
| Bucket Policy | <p>Controls read and write permissions for buckets.</p> <ul style="list-style-type: none"> • Private: No access beyond the bucket ACL settings is granted. • Public Read: Anyone can read objects in the bucket. • Public Read and Write: Anyone can read, write, or delete objects in the bucket. |
| Server-Side Encryption | <p>Select SSE-KMS. For the encryption key type, you can choose Default or Custom. If Default is used, the default key of the current region will be used to encrypt your objects. If there is no such a default key, OBS creates one the first time you upload an object. If Custom is used, you can choose a custom key you created on the KMS console to encrypt your objects.</p> <p>If SSE-OBS is chosen, the keys created and managed by OBS are used for encryption.</p> <p>When server-side encryption is enabled for a bucket, you can configure the object you upload to inherit encryption from the bucket or choose SSE-KMS or SSE-OBS.</p> |
| WORM | <p>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.</p> |

| Parameter | Description |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Direct Reading | <p>Direct reading allows you to directly download objects from the Archive storage class without restoring them first. Direct reading is a billable function. For details, see Product Pricing Details.</p> <p>No matter which default storage class you select, you can enable direct reading for your bucket. For example, if you select the Standard storage class and enable direct reading for your bucket, you can directly download objects stored in the Archive storage class from your bucket.</p> |
| Enterprise Project | <p>You can add a bucket to an enterprise project for unified management.</p> <p>Create an enterprise project by referring to Creating an Enterprise Project. The default enterprise project is named default.</p> <p>On the Enterprise Project Management page, create an enterprise project, and add a user group to the enterprise project. By doing so, users in this user group obtain the operation permissions for the buckets and objects in the enterprise project.</p> <p>NOTE</p> <p>Only an enterprise account can configure enterprise projects.</p> <p>OBS ReadOnlyAccess and OBS OperateAccess are the fine-grained authorizations of the enterprise project user group in OBS.</p> |
| Tags | <p>Optional. Tags are used to identify and classify buckets in OBS. Each tag is represented by a key-value pair.</p> <p>For more information, see Tags.</p> |

Step 4 Click **Create Now**.

----End

3.5 Uploading an Object

This section describes how to upload local files to OBS over the Internet. These files can be texts, images, videos, or any other type of files.

Constraints

OBS Console puts limits on the size and number of files you can upload.

- In regions where batch upload is supported, a maximum of 100 files can be uploaded at a time, with a maximum total size of 5 GB.
- In regions where batch upload is not supported, only one file can be uploaded at a time, with a maximum size of 50 MB.

Therefore, for a single file to be uploaded, its maximum size can be 5 GB in a batch upload or 50 MB in a single upload.

To upload a file larger than 5 GB, but no larger than 48.8 TB, you can use [OBS Browser+](#) or [obsutil](#), or the multipart upload of OBS SDKs or APIs.

OBS Browser+ allows you to upload a maximum of 500 files at a time. There is no limit on the number of files you can upload using [obsutil](#) at a time.

If you have more data to upload, refer to [Migrating Local Data to OBS](#).

NOTE

Batch upload is available only when both of the following conditions are met:

1. The region where the bucket is located supports batch upload.
2. The bucket version is 3.0. To view the bucket version, see [Viewing Basic Information of a Bucket](#).

If versioning is disabled for your bucket and you upload a new file with the same name as the one you previously uploaded to your bucket, the new file automatically overwrites the previous one and does not retain its ACL information. If you upload a new folder using the same name that was used with a previous folder in the bucket, the two folders will be merged, and files in the new folder will overwrite those with the same name in the previous folder.

After versioning is enabled for your bucket, if the new file you upload has the same name as the one you previously uploaded to the bucket, a new file version will be added in the bucket. For details, see [Versioning](#).

Prerequisites

- At least one bucket has been created.
- If you want to classify files, you can create folders and upload files to different folders. For details, see [Creating a Folder](#).

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 Go to the folder where you want to upload files and click **Upload Object**. The **Upload Object** dialog box is displayed.

Batch upload is used as an example here. If the region you are using supports only single upload, perform operations as instructed.

NOTE

If the files that you want to upload to OBS are stored in Microsoft OneDrive, it is recommended that the names of these files contain a maximum of 32 characters to ensure compatibility.

Figure 3-4 Uploading objects



Step 4 Select a storage class. If you do not specify a storage class, the objects you upload inherit the default storage class of the bucket.

NOTE

An object can have a different storage class from its bucket. You can specify a storage class for an object when uploading it, or you can change the object storage class after the object is uploaded.

Step 5 In the **Upload Object** area, drag and drop the files or folders you want to upload. You can also click **add files** in the **Upload Object** area to select files.

Step 6 Server-Side Encryption: Choose **Disable**, **SSE-KMS**, or **SSE-OBS**. For details, see [Uploading an Object in Server-Side Encryption Mode](#).

NOTE

If a bucket has server-side encryption configured, you can select **Inherit from bucket** when uploading an object to the bucket, for the object to inherit the encryption settings from the bucket.

Step 7 (Optional) To configure metadata or WORM retention policies, click **Next: (Optional) Configure Advanced Settings**.

NOTE

WORM retention policies can be configured in the advanced settings only when WORM is enabled for the bucket.

Configuring metadata: Add metadata ContentDisposition, ContentLanguage, WebsiteRedirectLocation, ContentEncoding, or ContentType as needed. For more information, see [OBS Object Metadata](#). Metadata is a set of name-value pairs.

The metadata value cannot be left blank. You can add two or more metadata entries by clicking **Add**.

Configuring WORM retention: Choose **Inherit from bucket**, or choose **Configure** and then specify a retention period, to automatically protect new objects uploaded to the bucket from being deleted.

Figure 3-5 Configuring metadata or WORM retention

Upload Object [How to Upload a File Larger than 5 GB?](#) ×

1 Upload Object ——— 2 (Optional) Configure Advanced Settings

Metadata Object metadata is a pair of name and value. Metadata can be used to manage objects. [Learn more](#)

Metadata name Metadata value

+ Add

Retention **Inherit from bucket** **Configure**

Protects only the current object from being deleted or overwritten. This object retention policy takes precedence over that of the bucket.

Retention Mode **Compliance**

No users can delete protected object versions or change their retention mode during the retention period.

Retain Until

Before the specified date, OBS prevents protected object versions from being deleted.

Previous: Upload Objects

Step 8 Click **Upload**.

----End

3.6 Downloading an Object

You can download files from OBS Console to your local computer.

Constraints

- Objects in the Archive or Deep Archive storage class can be downloaded only when they are in the **Restored** state.
- Batch download is not supported on OBS Console. To batch download files or folders, you can use OBS Browser+ or obsutil.
 - [Downloading Files or Folders Using OBS Browser+](#)
 - [Downloading Objects Using obsutil](#)

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 Select the file you want to download, and click **Download** or choose **More > Download As** on the right.

 **NOTE**

In the **Download As** dialog box, right-click the object and choose **Copy Link Address** from the shortcut menu to obtain the object's download address.

----End

3.7 Deleting an Object

You can delete unnecessary files one by one or in a batch on OBS Console to save space and money.

 **NOTE**

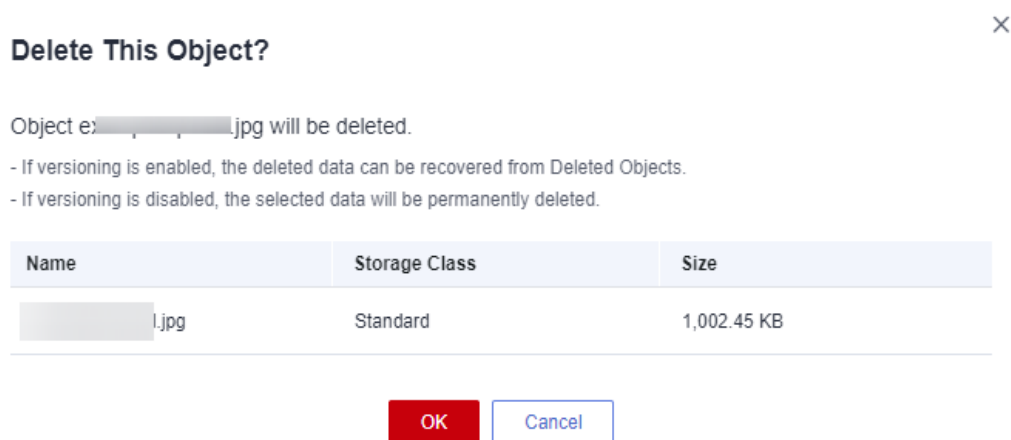
When WORM has been enabled for a bucket, versioning is also enabled for the bucket by default. If an object version has any WORM retention policy configured, this object version cannot be permanently deleted during the retention period. On the **Versions** tab of the object details page, you can choose **More > Extend Retention Period** in the **Operation** column in the row of the object version to check whether this version is within the retention period. If no WORM retention policy is configured for an object version, you can delete it on the **Versions** tab of the object details page.

Procedure

- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** Select the file you want to delete, and choose **More > Delete** on the right.

You can select multiple files and click **Delete** above the file list to batch delete them.
- Step 4** Click **OK** to confirm the deletion.

Figure 3-6 Deleting an object



----End

Important Notes

In big data scenarios, parallel file systems usually have deep directory levels and each directory has a large number of files. In such case, deleting directories from parallel file systems may fail due to timeout. To address this problem, you are advised to configure a [lifecycle rule](#) for directories so that they can be deleted in background based on the preset lifecycle rule.

3.8 Deleting a Bucket

You can delete unwanted buckets on OBS Console to free up the quota of buckets.

Prerequisites

- All objects in the bucket have been permanently deleted. A bucket must be emptied before it can be deleted.

NOTICE

Objects under the **Objects**, **Deleted Objects**, and **Fragments** tabs must be all deleted.

- A bucket can only be deleted by the bucket owner.

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

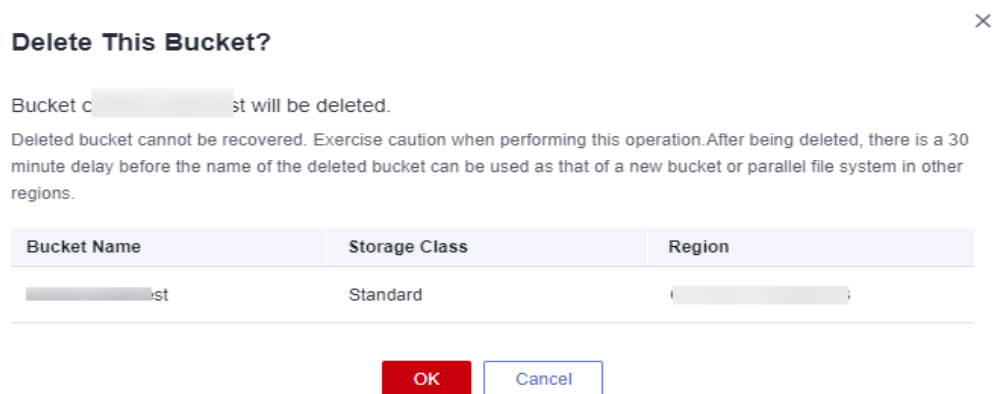
Step 2 In the bucket list, select the bucket you want to delete, and then click **Delete** on the right.

NOTE

The name of a deleted bucket can be reused for another bucket or parallel file system at least 30 minutes after the deletion.

Step 3 Click **OK** to confirm the deletion.

Figure 3-7 Deleting a bucket



----End

4 Managing Buckets

4.1 Creating a Bucket

A bucket is a container that stores objects in OBS. Before you store data in OBS, you need to create a bucket.

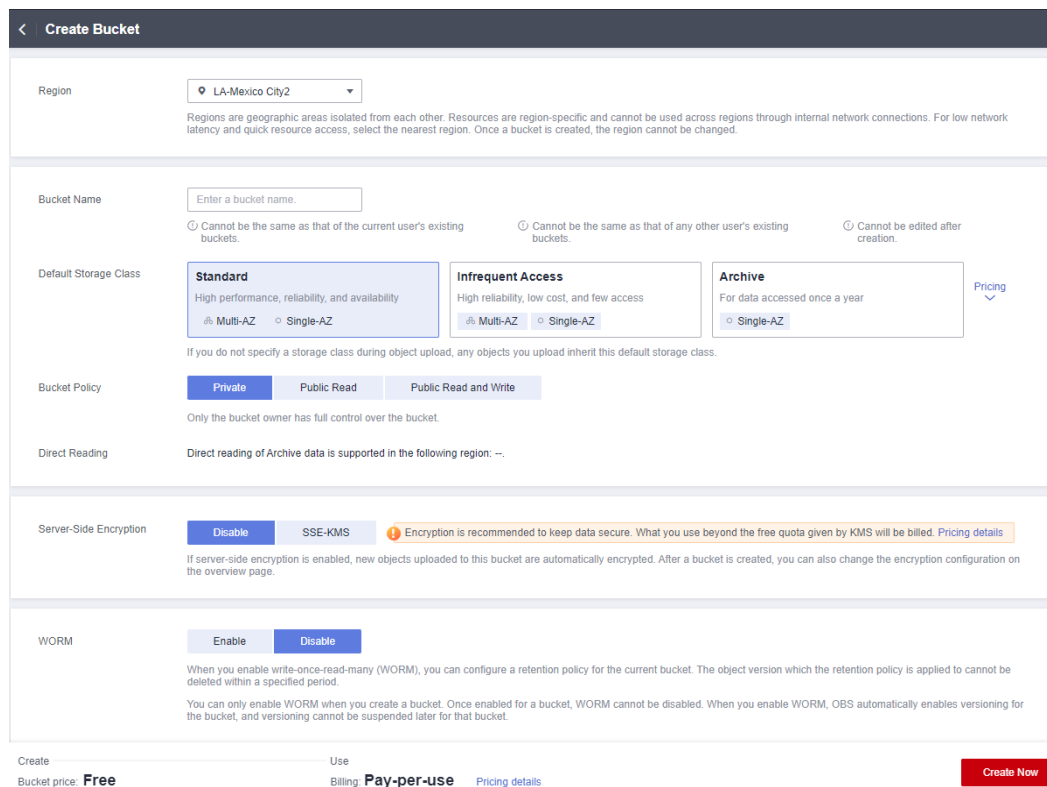
 **NOTE**

An account (including all IAM users under this account) can create a maximum of 100 buckets and parallel file systems. You can use the fine-grained access control of OBS to properly plan and use buckets. For example, you can create folders in a bucket based on object prefixes and use [fine-grained permission control](#) to implement permission isolation between departments.

Procedure

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the upper right corner, click **Create Bucket**. The **Create Bucket** page is displayed. For details, see [Figure 4-1](#).

Figure 4-1 Creating a bucket



Step 3 Configure bucket parameters.

Table 4-1 Bucket parameters

| Parameter | Description |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Replicate Existing Settings | Optional. To use this function, click Select Bucket and select a bucket from the list as the replication source. After the replication source is selected, the following settings are replicated to the bucket you are creating: region, data redundancy policy, storage class, bucket policy, server-side encryption, direct reading, enterprise project, and tags. You can still change some or all of the replicated settings as needed. |
| Region | Geographic area where a bucket resides. For low latency and faster access, select the region nearest to you. Once the bucket is created, its region cannot be changed. Most OBS features are available in all regions, but some are only available for certain regions. Consider the feature availability in each region when you select a region for a bucket. For details, see Function Overview . If your ECS needs to access an OBS bucket over the intranet, ensure that the bucket and the ECS are in the same region. For details, see Accessing OBS over an Intranet . |

| Parameter | Description |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bucket Name | <p>Name of the bucket. A bucket name must be unique across all accounts and regions. Once a bucket is created, its name cannot be changed.</p> <p>According to the globally applied DNS naming rules, an OBS bucket name:</p> <ul style="list-style-type: none"> • Must be unique across all accounts and regions. The name of a deleted bucket can be reused for another bucket or a parallel file system at least 30 minutes after the deletion. • Must be 3 to 63 characters long. Only lowercase letters, digits, hyphens (-), and periods (.) are allowed. • Cannot start or end with a period (.) or hyphen (-), and cannot contain two consecutive periods (..) or contain a period (.) and a hyphen (-) adjacent to each other. • Cannot be formatted as an IP address. <p>NOTE When you access OBS through HTTPS using virtual hosted-style URLs, if the bucket name contains a period (.), the certificate verification will fail. To work around this issue, you are advised not to use periods (.) in bucket names.</p> |
| Data Redundancy Policy | <ul style="list-style-type: none"> • Multi-AZ storage: Data is stored in multiple AZs to achieve higher reliability. • Single-AZ storage: Data is stored in a single AZ, with lower costs. <p>For details about the performance comparison between multi-AZ and single-AZ storage, see Comparison of Storage Classes.</p> <p>Once a bucket is created, the data redundancy policy cannot be changed, so choose the policy that can meet your needs.</p> <ul style="list-style-type: none"> • Multi-AZ storage is not available for buckets in the Archive storage class. • Multi-AZ storage is not available for buckets in the Deep Archive storage class. |

| Parameter | Description |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Storage Class | <p>Storage classes of a bucket. Different storage classes meet different requirements for storage performance and costs.</p> <ul style="list-style-type: none"> • The Standard storage class is for storing a large number of hot files or small files that are frequently accessed (multiple times per month on average) and require quick retrieval. • The Infrequent Access storage class is for storing data that is less frequently accessed (less than 12 times per year on average) and requires quick retrieval. • The Archive storage class is for archiving data that is rarely accessed (once a year on average) and has no requirements for quick retrieval. • The Deep Archive storage class is for storing data that is rarely accessed (a lower frequency than the archived data) and has no requirements for quick retrieval. <p>For details, see Storage Classes.</p> |
| Bucket Policy | <p>Controls read and write permissions for buckets.</p> <ul style="list-style-type: none"> • Private: No access beyond the bucket ACL settings is granted. • Public Read: Anyone can read objects in the bucket. • Public Read and Write: Anyone can read, write, or delete objects in the bucket. |
| Server-Side Encryption | <p>Select SSE-KMS. For the encryption key type, you can choose Default or Custom. If Default is used, the default key of the current region will be used to encrypt your objects. If there is no such a default key, OBS creates one the first time you upload an object. If Custom is used, you can choose a custom key you created on the KMS console to encrypt your objects.</p> <p>If SSE-OBS is chosen, the keys created and managed by OBS are used for encryption.</p> <p>When server-side encryption is enabled for a bucket, you can configure the object you upload to inherit encryption from the bucket or choose SSE-KMS or SSE-OBS.</p> |
| WORM | <p>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.</p> |

| Parameter | Description |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Direct Reading | <p>Direct reading allows you to directly download objects from the Archive storage class without restoring them first. Direct reading is a billable function. For details, see Product Pricing Details.</p> <p>No matter which default storage class you select, you can enable direct reading for your bucket. For example, if you select the Standard storage class and enable direct reading for your bucket, you can directly download objects stored in the Archive storage class from your bucket.</p> |
| Enterprise Project | <p>You can add a bucket to an enterprise project for unified management.</p> <p>Create an enterprise project by referring to Creating an Enterprise Project. The default enterprise project is named default.</p> <p>On the Enterprise Project Management page, create an enterprise project, and add a user group to the enterprise project. By doing so, users in this user group obtain the operation permissions for the buckets and objects in the enterprise project.</p> <p>NOTE Only an enterprise account can configure enterprise projects. OBS ReadOnlyAccess and OBS OperateAccess are the fine-grained authorizations of the enterprise project user group in OBS.</p> |
| Tags | <p>Optional. Tags are used to identify and classify buckets in OBS. Each tag is represented by a key-value pair.</p> <p>For more information, see Tags.</p> |

Step 4 Click **Create Now**.

----End

Related Operations

After the bucket is created, you can change its storage class by performing the following steps:

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, locate the bucket you want and click **Change Storage Class** on the right.

Step 3 Select the desired storage class and click **OK**.

 **NOTE**

- Changing the storage class of a bucket does not change the storage class of existing objects in the bucket.
- If you do not specify a storage class for an object when uploading it, it inherits the bucket's storage class by default. After the bucket's storage class is changed, newly uploaded objects will inherit the new storage class of the bucket by default.

----End

4.2 Viewing Basic Information of a Bucket

On OBS Console, you can view a bucket's details, including basic bucket information, usage statistics, alarms, process flows for common scenarios, domain name details, FAQs, basic configurations, and others. You can also export all buckets of the current account and view their basic information in the exported Excel file.

Viewing Bucket Details

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the navigation pane, choose **Overview**.
- Step 4** On the top of the page, view the bucket information, including the bucket name, storage class, data redundancy policy, region, and creation time.

Figure 4-2 Bucket information

[Bucket List](#) / Overview



Table 4-2 Bucket information

| Item | Description |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bucket name | Name of the bucket |
| Storage class | Storage class of the bucket, which can be Standard , Infrequent Access , Archive , or Deep Archive . |
| Data redundancy | Data redundancy storage policy of a bucket, which can be multi-AZ storage or single-AZ storage. This setting cannot be changed after the bucket is created. |
| Region | Region where the bucket is located |
| Created | Creation time of the bucket |

- Step 5** In the **Basic Information** area, view the number of objects, storage usage, bucket version, versioning status, enterprise project, and account ID.

Figure 4-3 Bucket's basic information



Table 4-3 Parameters in the Basic Information area

| Parameter | Description |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Objects | The total number of stored folders and objects of all versions in a bucket |
| Used Capacity | Total storage space occupied by objects of all versions in the bucket NOTE If usage statistics is available for the bucket, storage usage data is not displayed here. |
| Bucket Version | Version number of the bucket. 3.0 indicates the latest bucket version, and -- indicates versions earlier than 3.0. |
| Versioning | Versioning status |
| Enterprise Project | Enterprise project where the bucket belongs |
| Account ID | Unique identity of the bucket owner. It is the same as Account ID on the My Credentials page. |

Step 6 In the **Usage Statistics** area, view the storage, traffic, and request information of the bucket, as shown in **Figure 4-4**.

Figure 4-4 Bucket usage statistics

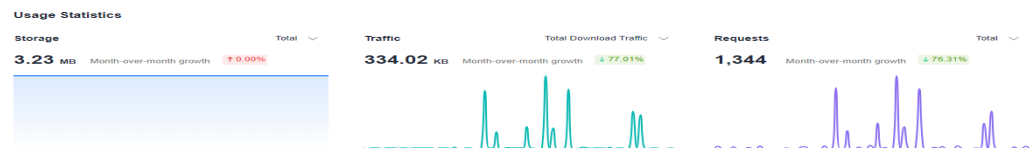


Table 4-4 Bucket usage metrics

| Metric | Description |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Storage | Measures the storage occupied by all objects, Standard objects, Infrequent Access objects, and Archive objects in the bucket. |
| Traffic | Total Download Traffic: It measures the total download traffic for the bucket in the current month. Both intranet and Internet traffic are covered. |

| Metric | Description |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>Download Traffic (Intranet): It measures the total intranet download traffic for the bucket in the current month.</p> <p>Download Traffic (Internet): It measures the total Internet download traffic for the bucket in the current month.</p> <p>Total Upload Traffic: It measures the total upload traffic for the bucket in the current month. Both intranet and Internet traffic are covered.</p> <p>Upload Traffic (Intranet): It measures the total intranet upload traffic for the bucket in the current month.</p> <p>Upload Traffic (Internet): It measures the total Internet upload traffic for the bucket in the current month.</p> |
| Requests | <p>Total: It measures the total number of requests (including PUT, POST, COPY, LIST, GET, HEAD, and DELETE requests) made for the bucket and the objects in it in the current month.</p> <p>GET: It measures the total number of GET and HEAD requests made for the bucket and the objects in it in the current month.</p> <p>PUT: It measures the total number of PUT, POST, COPY, and LIST requests made for the bucket and the objects in it in the current month.</p> <p>DELETE: It measures the total number of DELETE requests made for the bucket and the objects in it in the current month.</p> |
| Month-over-month growth | <p>It compares the current month's data with the previous month's data, showing the data increase or decrease.</p> <p>Take the comparison between January 2023 and February 2023 as an example.</p> <p>Month-over-month (MoM) growth = (Current month's data - Previous month's data)/Previous month's data x 100%</p> <p>Suppose the Standard storage in January was 60 MB and that in February was 120 MB, the MoM growth was calculated as follows: $(120 - 60) \div 60 \times 100\% = 100\%$. This tells that the standard storage in February was doubled compared to January.</p> |

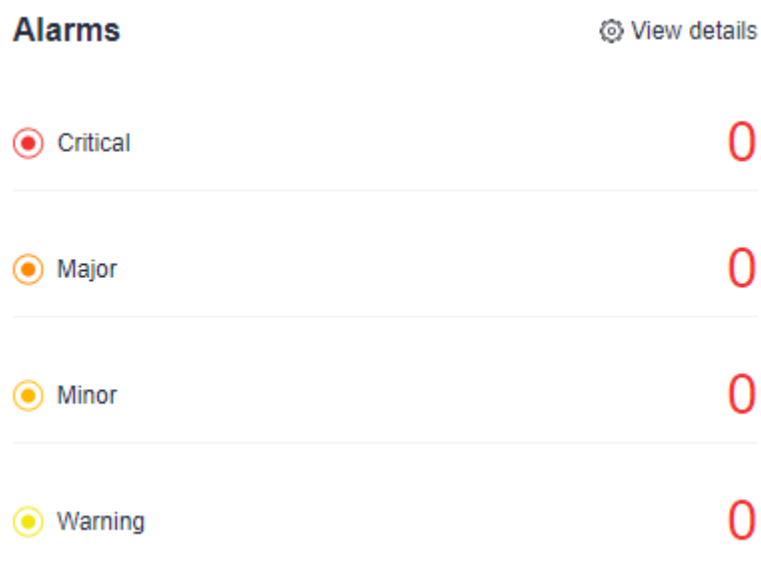
 NOTE






The data is not displayed in real time. There may be approximately one hour delay.
To view the number of requests and traffic statistics, you must have the **CES ReadOnlyAccess** permission or a higher Cloud Eye permission for the region where the bucket is located.

Usage Statistics is only available for buckets that support usage analysis.

Step 7 In the **Alarms** area, view the alarm severities and the alarm number of each severity. By clicking **View details**, you can explore more on the **Alarm Records** page of Cloud Eye.

Figure 4-5 Information about bucket alarms



| Alarms | |  View details |
|---------------------------------------------------------------------------------------------|---|--------------------------------------------------------------------------------------------------|
|  Critical | 0 | |
|  Major | 0 | |
|  Minor | 0 | |
|  Warning | 0 | |

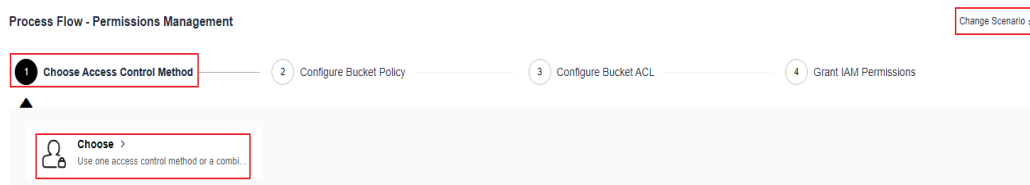
 NOTE

Alarms is only available for buckets that support usage analysis.

Step 8 In the **Process Flow** area, view the process flows for common scenarios. You can click **Change Scenario** in the upper right corner to choose a desired scenario, as shown in **Figure 4-6**.

In each flow, you can click a node to view relevant details, or click a card to navigate to the operation guide or console page.

Figure 4-6 Process flows for common scenarios



Step 9 In the **Domain Information Details** area, view information about the endpoint, access domain name, and static website hosting domain name. You can also

perform related operations by clicking buttons in the **Operation** column, as shown in [Figure 4-7](#).

Figure 4-7 Domain name details of the bucket

Domain Name Details

| Type | Domain Name | Protocol | Operation |
|------------------------------------|-------------|------------|-----------------------|
| Endpoint | | HTTPS/HTTP | -- |
| Access Domain Name | | HTTPS/HTTP | Bind User Domain Name |
| Static website hosting domain name | -- | HTTPS/HTTP | Configure |

Step 10 In the **Basic Configurations** area, view the bucket's basic configurations, including lifecycle rules, static website hosting, and CORS rules. You can click a card to make required configurations, as shown in [Figure 4-8](#).

Figure 4-8 Basic configurations of the bucket

Basic Configurations

| | | | | | | | |
|-----------------|----------------|------------------------|----------------|--------------------|----------------|----------------|----------------|
| Lifecycle Rules | Not configured | Static Website Hosting | Not configured | CORS Rules | Not configured | URL Validation | Not configured |
| Tags | Not configured | Logging | Not configured | Default Encryption | Not configured | Direct Reading | Not configured |
| WORM Retention | Not supported | Versioning | Disabled | | | | |

Step 11 In the **FAQs** area, view bucket-related FAQs. You can click **More** in the upper right corner to view more FAQs, as shown in [Figure 4-9](#).

Figure 4-9 Bucket FAQs

FAQs More

| | |
|-------------------------------------------------------------------------|------------------------------------------|
| Why am I unable to create a bucket? | Why am I unable to upload an object? |
| Why can't I access OBS (403 AccessDenied) after being granted O... | Common permission configuration examples |
| Why am I still being billed for pay-per-use usage after I purchased ... | How do I migrate data to OBS? |

Step 12 In the **Learn More** area, choose to view best practices or usage guide, as shown in [Figure 4-10](#).

Figure 4-10 Learn More

Learn More

Best Practices

Quickly master skills and acquire knowledge.

Usage Guide

Learn how to make better use of OBS.

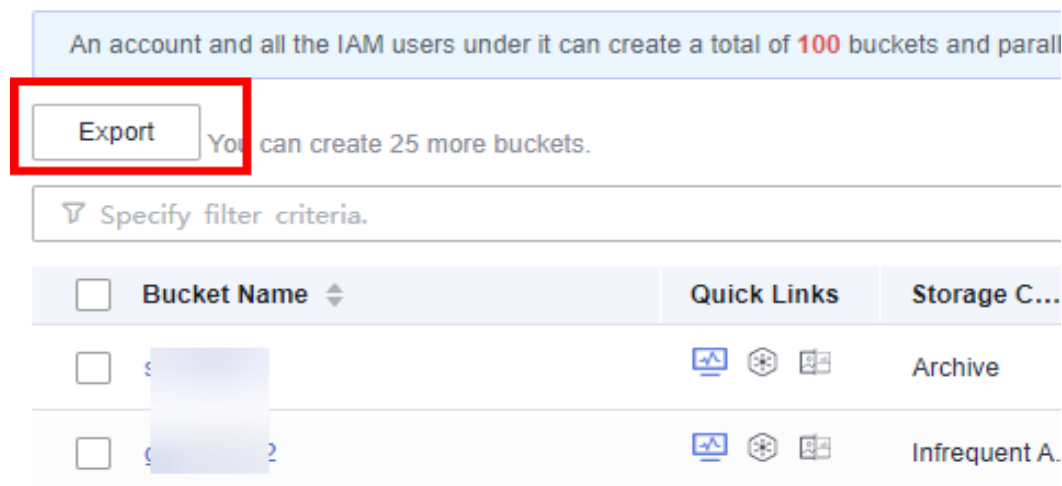
----End

Exporting a Bucket List

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

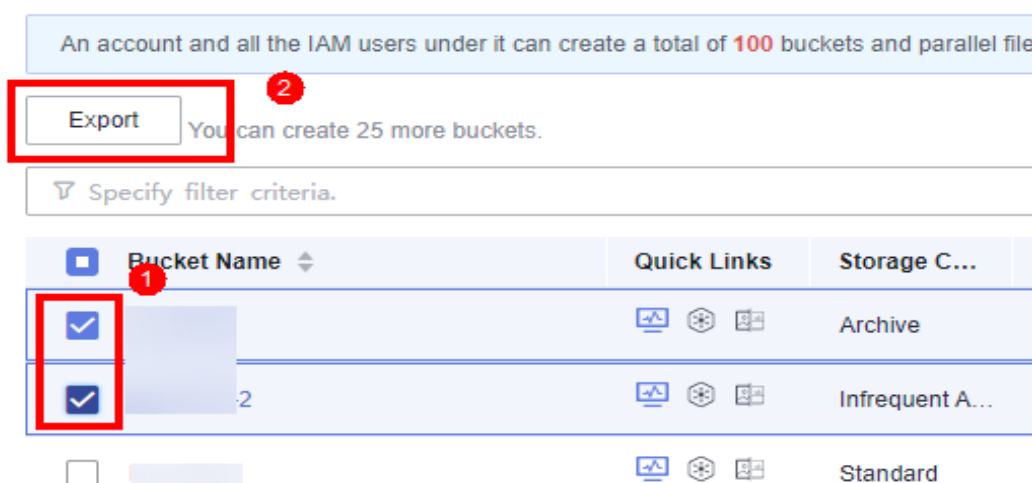
Step 2 Export all buckets. Specifically, click **Export** in the upper left corner of the bucket list.

Figure 4-11 Exporting all buckets



Step 3 Export the selected buckets. Specifically, select the buckets to export and click **Export** in the upper left corner of the bucket list.

Figure 4-12 Exporting the selected buckets



Step 4 Obtain the bucket list in Excel, which is automatically downloaded to your local computer.

The file lists all the buckets of the current account and includes the following information: bucket name, storage class, region, data redundancy policy, used capacity, object quantity, bucket version, enterprise project, and bucket creation time.

----End

4.3 Searching for a Bucket

On OBS Console, you can search for buckets by bucket name, region, storage class, and enterprise project.

NOTE

Currently, bucket search by tag is not supported.
The keywords used for search are case-insensitive.

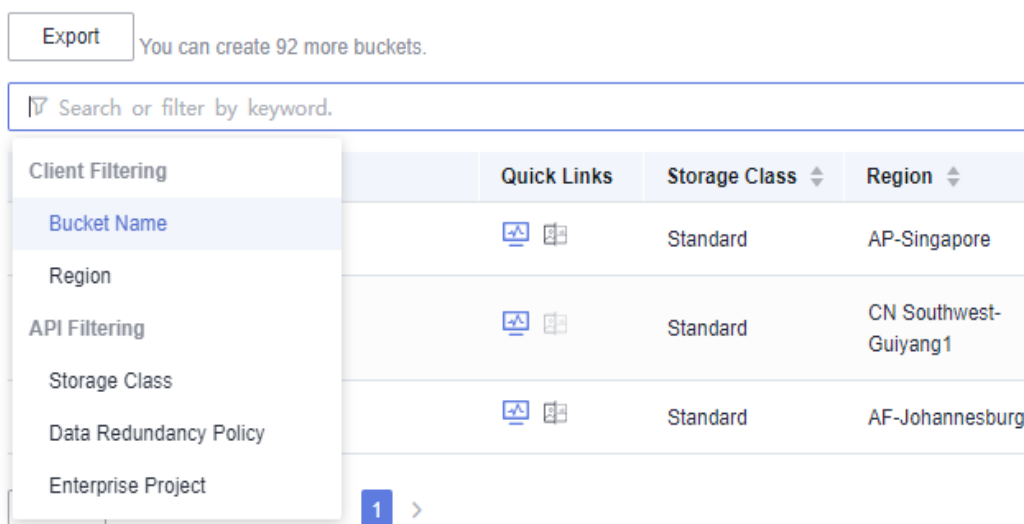
Procedure

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** Click the search box above the bucket list, select **Bucket Name**, **Region**, **Storage Class**, **Data Redundancy Policy**, or **Enterprise Project** from the level-1 drop-down list, and then the option you need from the corresponding level-2 drop-down list. Alternatively, after selecting an option from the level-1 drop-down list, you can enter a keyword in the search box and then select what you want from the level-2 drop-down list.

The found buckets are displayed in the bucket list.

For example, if you want to search for bucket **test**, click the search box, select **Bucket Name** and then **test**. Alternatively, after selecting **Bucket Name**, enter **test** in the search box, and all buckets whose names contain **test** are displayed in the level-2 drop-down list. Then, select **test** and click **OK**.

Figure 4-13 Searching for buckets



NOTE

- You can search for buckets based on combinations of different filter criteria.
 - If the filter criteria are of different types, they are in intersection logic. For example, if you select region **CN-Hong Kong** and storage class **Standard** as two criteria, buckets whose region is CN-Hong Kong and storage class is Standard will be displayed in the list.
 - If the filter criteria are of the same type, they are in union logic. For example, if you select bucket name **test-1** and then **test-2** as two criteria, both buckets **test-1** and **test-2** will be displayed in the list.
- After a keyword is entered in the search box, all buckets whose name, region, storage class, data redundancy policy, or enterprise project contains the specified keyword are displayed in the drop-down list. Click the option you want. Then, all the buckets meeting the search criteria are displayed in the bucket list.

Step 3 Enter a keyword in the search box and click  or press **Enter**.

All buckets whose name, region, storage class, data redundancy policy, or enterprise project contains the searched keyword will be displayed in the bucket list.


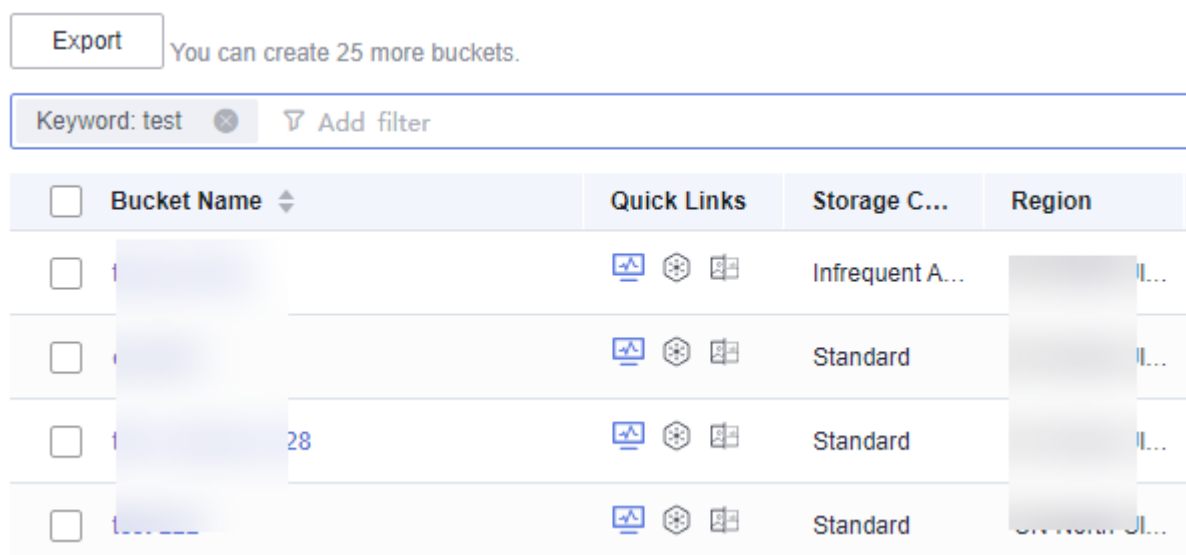

For example, if you enter **test** in the search box and click  or press **Enter**, all buckets whose name, region, storage class, data redundancy policy, or enterprise project contains keyword **test** are displayed in the bucket list.

Figure 4-14 Searching for buckets



----End

Related Operations

In the bucket list, click  next to the bucket name, storage class, region, data redundancy policy, used capacity, number of objects, enterprise project, or creation time to sort buckets.

4.4 Deleting a Bucket

You can delete unwanted buckets on OBS Console to free up the quota of buckets.

Prerequisites

- All objects in the bucket have been permanently deleted. A bucket must be emptied before it can be deleted.

NOTICE

Objects under the **Objects**, **Deleted Objects**, and **Fragments** tabs must be all deleted.

- A bucket can only be deleted by the bucket owner.

Procedure

Step 1 In the navigation pane of **OBS Console**, choose **Object Storage**.

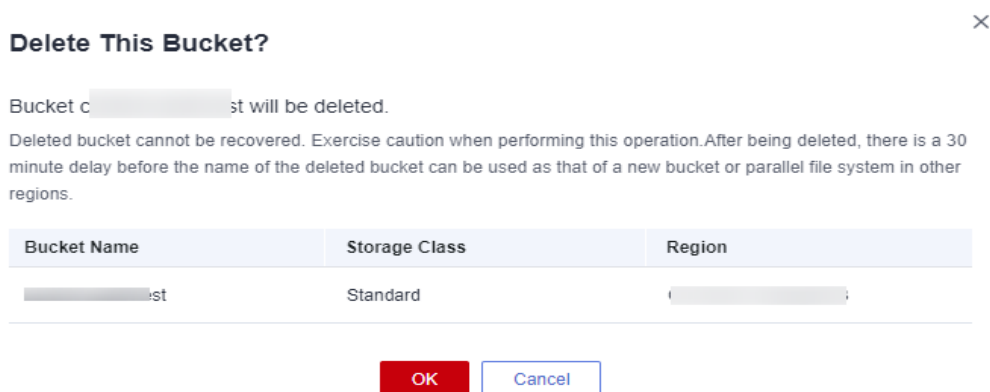
Step 2 In the bucket list, select the bucket you want to delete, and then click **Delete** on the right.

NOTE

The name of a deleted bucket can be reused for another bucket or parallel file system at least 30 minutes after the deletion.

Step 3 Click **OK** to confirm the deletion.

Figure 4-15 Deleting a bucket



----End

5 Managing Objects

5.1 Uploading an Object

This section describes how to upload local files to OBS over the Internet. These files can be texts, images, videos, or any other type of files.

Constraints

OBS Console puts limits on the size and number of files you can upload.

- In regions where batch upload is supported, a maximum of 100 files can be uploaded at a time, with a maximum total size of 5 GB.
- In regions where batch upload is not supported, only one file can be uploaded at a time, with a maximum size of 50 MB.

Therefore, for a single file to be uploaded, its maximum size can be 5 GB in a batch upload or 50 MB in a single upload.

To upload a file larger than 5 GB, but no larger than 48.8 TB, you can use [OBS Browser+](#) or [obsutil](#), or the multipart upload of OBS SDKs or APIs.

OBS Browser+ allows you to upload a maximum of 500 files at a time. There is no limit on the number of files you can upload using [obsutil](#) at a time.

If you have more data to upload, refer to [Migrating Local Data to OBS](#).

NOTE

Batch upload is available only when both of the following conditions are met:

1. The region where the bucket is located supports batch upload.
2. The bucket version is 3.0. To view the bucket version, see [Viewing Basic Information of a Bucket](#).

If versioning is disabled for your bucket and you upload a new file with the same name as the one you previously uploaded to your bucket, the new file automatically overwrites the previous one and does not retain its ACL information. If you upload a new folder using the same name that was used with a previous folder in the bucket, the two folders will be merged, and files in the new folder will overwrite those with the same name in the previous folder.

After versioning is enabled for your bucket, if the new file you upload has the same name as the one you previously uploaded to the bucket, a new file version will be added in the bucket. For details, see [Versioning](#).

Prerequisites

- At least one bucket has been created.
- If you want to classify files, you can create folders and upload files to different folders. For details, see [Creating a Folder](#).

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 Go to the folder where you want to upload files and click **Upload Object**. The **Upload Object** dialog box is displayed.

Batch upload is used as an example here. If the region you are using supports only single upload, perform operations as instructed.

NOTE

If the files that you want to upload to OBS are stored in Microsoft OneDrive, it is recommended that the names of these files contain a maximum of 32 characters to ensure compatibility.

Figure 5-1 Uploading objects



Step 4 Select a storage class. If you do not specify a storage class, the objects you upload inherit the default storage class of the bucket.

 **NOTE**

An object can have a different storage class from its bucket. You can specify a storage class for an object when uploading it, or you can change the object storage class after the object is uploaded.

Step 5 In the **Upload Object** area, drag and drop the files or folders you want to upload. You can also click **add files** in the **Upload Object** area to select files.

Step 6 Server-Side Encryption: Choose **Disable**, **SSE-KMS**, or **SSE-OBS**. For details, see [Uploading an Object in Server-Side Encryption Mode](#).

 **NOTE**

If a bucket has server-side encryption configured, you can select **Inherit from bucket** when uploading an object to the bucket, for the object to inherit the encryption settings from the bucket.

Step 7 (Optional) To configure metadata or WORM retention policies, click **Next: (Optional) Configure Advanced Settings**.

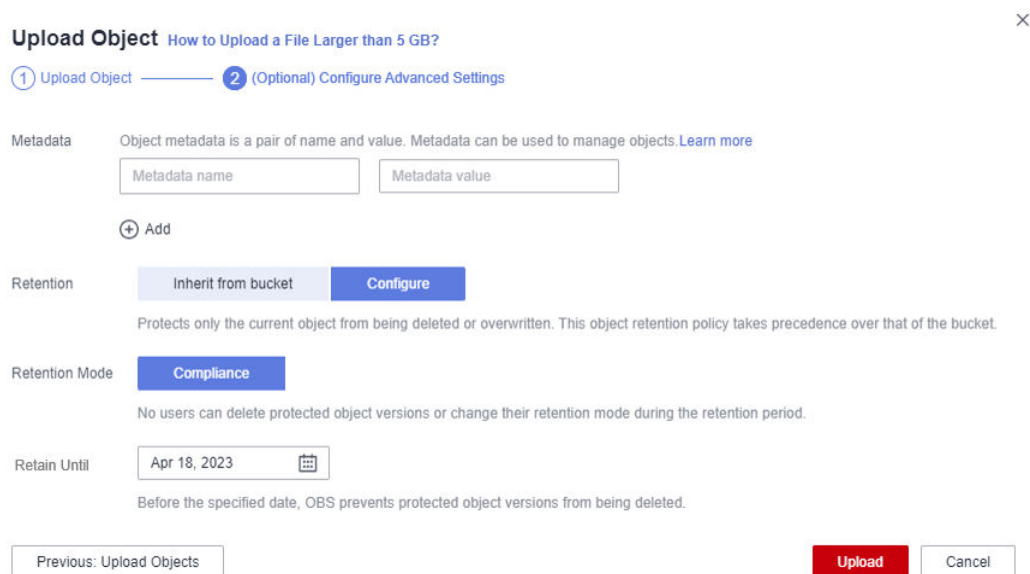
 **NOTE**

WORM retention policies can be configured in the advanced settings only when WORM is enabled for the bucket.

Configuring metadata: Add metadata ContentDisposition, ContentLanguage, WebsiteRedirectLocation, ContentEncoding, or ContentType as needed. For more information, see [OBS Object Metadata](#). Metadata is a set of name-value pairs. The metadata value cannot be left blank. You can add two or more metadata entries by clicking **Add**.

Configuring WORM retention: Choose **Inherit from bucket**, or choose **Configure** and then specify a retention period, to automatically protect new objects uploaded to the bucket from being deleted.

Figure 5-2 Configuring metadata or WORM retention



Step 8 Click **Upload**.

----End

Related Operations

When uploading an object, you can specify a storage class for it. After the object is uploaded, you can also change its storage class by doing as follows:

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 Select the target object and choose **More > Change Storage Class** on the right.

NOTE

You can also select multiple objects at a time and choose **More > Change Storage Class** above the object list, to batch change their storage classes.

Storage classes of unrestored Archive or Deep Archive objects cannot be changed in a batch.

Step 4 Select the desired storage class and click **OK**.

----End

NOTE

- You can manually change objects between storage classes:
 - From Standard to Infrequent Access, or Archive, or Deep Archive
 - From Infrequent Access to Standard, or Archive, or Deep Archive
 - From Archive to Standard, or Infrequent Access, or Deep Archive. Before changing Archive objects, you must restore them first.
 - From Deep Archive to Standard, Infrequent Access, or Archive. Before changing Deep Archive objects, you must restore them first.
- Changing objects from Infrequent Access or Archive or Deep Archive to other storage classes incurs restore costs. Select an appropriate change option based on your actual needs.
- After an object is changed to Archive, its restore status changes to **Unrestored**.
- You can also configure a lifecycle rule to change the storage class of an object. For details, see [Configuring a Lifecycle Rule](#).

Follow-up Procedure

You can click **More > Copy Path** on the right of an object to copy its path.

You can share the path with others. Then they can open the bucket where the object is stored and enter the path in the search box above the object list to find the object.

5.2 Downloading an Object

You can download files from OBS Console to the system default path or a custom download path on your local computer.

Constraints

- Objects in the Archive or Deep Archive storage class can be downloaded only when they are in the **Restored** state.
- Batch download is not supported on OBS Console. To batch download files or folders, you can use OBS Browser+ or obsutil.
 - [Downloading Files or Folders Using OBS Browser+](#)
 - [Downloading Objects Using obsutil](#)

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 Select the file you want to download. Then, click **Download** or **More > Download As** on the right.

You can also select multiple files and choose **More > Download** above the file list.

NOTE

In the **Download As** dialog box, right-click the object and choose **Copy Link Address** from the shortcut menu to obtain the object's download address.

----End

5.3 Managing Folders

5.3.1 Creating a Folder

This section describes how to create a folder on OBS Console. Folders facilitate data management in OBS.

Background Information

- Unlike a file system, OBS does not involve the concepts of file and folder. For easy data management, OBS provides a method to simulate folders. In OBS, an object is simulated as a folder by adding a slash (/) to the end of the object name on 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 does not support the download of folders. You can use OBS Browser+ to download folders.

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 Click **Create Folder**, or click a folder in the object list to open it and click **Create Folder**.

Step 4 In the **Folder Name** text box, enter a name for the folder.

- You can create single-level or multi-level folders.
- The name cannot contain the following special characters: \:*?"<>|
- The name cannot start or end with a period (.) or slash (/).
- The folder's absolute path cannot exceed 1,023 characters.
- Any single slash (/) separates and creates multiple levels of folders at once.
- The name cannot contain two or more consecutive slashes (/).

Step 5 Click **OK**.

----End

Follow-up Procedure

You can click **Copy Path** on the right to copy the path of the folder and share it with others. Then they can open the bucket where the folder is stored and enter the path in the search box above the object list to find the folder.

5.3.2 Sharing a Folder

Scenarios

You can share your folders in OBS to other users.

Background Information

Folder sharing is temporary and has a validity period. You can temporarily share folders by access code or URL:

- By access code: Specify a six-digit access code before creating a sharing task. After the sharing task is created, OBS aggregates the download links of all objects in the folder to a static website that is hosted by a public OBS bucket. Then anyone who has the created temporary URL and access code can access the static website and download the shared files.
- By URL: Specify a validity period and then share the generated link with others. Anyone can use a signature to access all objects in the shared folder.

Constraints

- A folder shared from OBS Console can be valid for one minute to 18 hours. If you need a longer validity period, use OBS Browser+ that allows a validity period of up to one year to share the folder. If you want a shared folder permanently valid, [use a bucket policy to grant anonymous users the public read permission for the folder](#).
- Folder sharing is available for a few regions only.
- Only version 3.0 buckets support folder sharing. You can view the bucket version in the **Basic Information** area on the **Overview** page of a bucket.
- Archive objects in a folder must be restored in the bucket before they can be downloaded.

- Deep Archive objects in a folder must be restored in the bucket before they can be downloaded.

Procedure

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** Locate the folder you want to share and click **Share** in the **Operation** column. The **Share Folder** dialog box is displayed.
- Step 4** Share the folder by access code or URL.
- Step 5** Method 1: Share the folder by access code.

Figure 5-3 Sharing by access code

1. Choose **Access code** for **Share By**.
2. Configure parameters.

Table 5-1 Parameters for sharing a folder with an access code

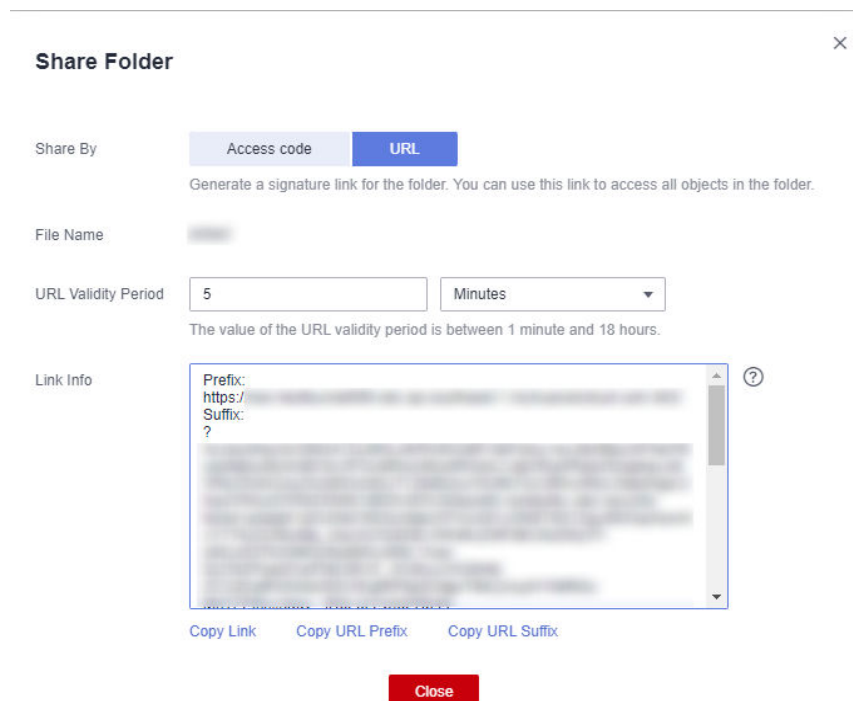
| Parameter | Description |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL Validity Period | A validity period is from one minute to 18 hours. The default value is five minutes. Within the URL validity period, anyone who has the URL can access the folder. |

| Parameter | Description |
|-------------|-----------------------------------------------------------------------------------------|
| Access Code | A six-digit code. An access code is required to access objects in the shared folder. |

3. Click **Create Share** to generate a sharing URL for the folder.
4. Send the URL and access code to others for them to access the folder.
5. Verify that other users can perform the following operations:
 - a. Access the shared folder in a browser.
 - i. Open the shared URL in a web browser.
 - ii. In the dialog box that is displayed, enter the access code and access objects in the shared folder.
 - b. Access the shared folder on OBS Browser+.
 - i. Start OBS Browser+.
 - ii. On the login page, click **Authorization Code Login**.
 - iii. Enter the authorization code and access code.
 - iv. Click **Log In** to access the shared folder.

Step 6 Method 2: Share the folder by URL.

Figure 5-4 Sharing by URL



1. Choose **URL** for **Share By**.
2. Configure parameters.

Table 5-2 Parameters for sharing a folder by URL

| Parameter | Description |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URL Validity Period | A validity period is from one minute to 18 hours. The default value is five minutes. Within the URL validity period, anyone who has the URL can access the folder. |

3. Click **Copy Link** and share the link with another user. The user then can use this link to access all objects in this folder. The sharing link consists of the bucket domain name (prefix) and signature information (suffix). Users can add an object path after the prefix of a sharing link to access or download the specified object in a folder, as shown in **Figure 5-5**.
4. Verify that a user can use the sharing link to access all objects in the folder.
 - a. Open a browser.
 - b. Enter the sharing link in the address box and press **Enter** to list all objects in the folder.
 - c. Copy the object path and paste it after the prefix.
 - d. Press **Enter**. You can then access and download the specified object.

Figure 5-5 Accessing an object with a sharing link



----End

5.4 Other Object Operations

5.4.1 Listing Objects

On OBS Console, when you go to the object list page of a bucket, objects are displayed by name by default. You can also sort objects by their size or last modification time.

Listing Objects on OBS Console

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** View the displayed objects. All objects in the bucket will be listed and each page has 50 objects displayed by default.
- End

Listing Objects with OBS Tools

- Bucket-level operations on OBS Browser+ are similar to those on OBS Console. You can list objects by following the instructions on OBS Browser+. For details about OBS Browser+, see [Introduction to OBS Browser+](#).
- The Java, Python, C, .NET, Node.js and Android SDKs all can be used to list objects in a bucket.
- To use the command line tool obsutil to list objects in a bucket, see [Listing Objects Using obsutil](#).
- To call an API to list objects in a bucket, see [Listing Objects in a Bucket](#).

Important Notes

- Listing objects by specifying a page number is not allowed.
- Objects cannot be listed by time when they were uploaded. You can search for objects by prefix only. For details, see [Searching for an Object or Folder](#).
- The size and last modification time in the object list sort only objects on the current page.

5.4.2 Searching for an Object or Folder

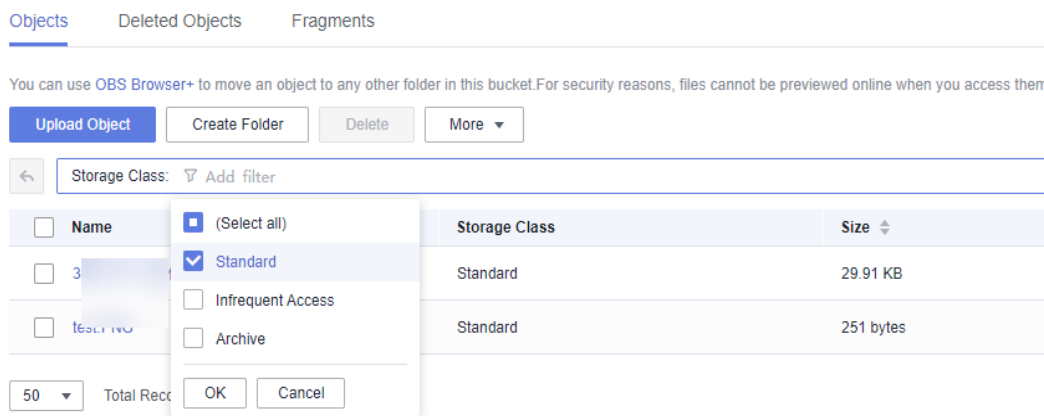
On OBS Console, you can search for files or folders by storage class, last modification time, or object name prefix.

Procedure

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3 Search for objects by storage class:**
1. Click the search box above the object list and choose **Storage Class** from the drop-down list.
 2. Select your desired option, or enter a keyword and then select the option displayed.
 3. Click **OK**. The searched objects are displayed in the object list.

Suppose you want to search for objects in the Standard storage class. Click the search box and choose **Storage Class** from the drop-down list. Then, select **Standard**, or enter **standard** in the search box and select the option displayed. After that, click **OK**. Objects in the Standard storage class will be displayed in the object list.

Figure 5-6 Searching for objects by storage class



Step 4 Search for objects by last modification time:

1. Click the search box above the object list and choose **Last Modified** from the drop-down list.
2. Select a start date or an end date.

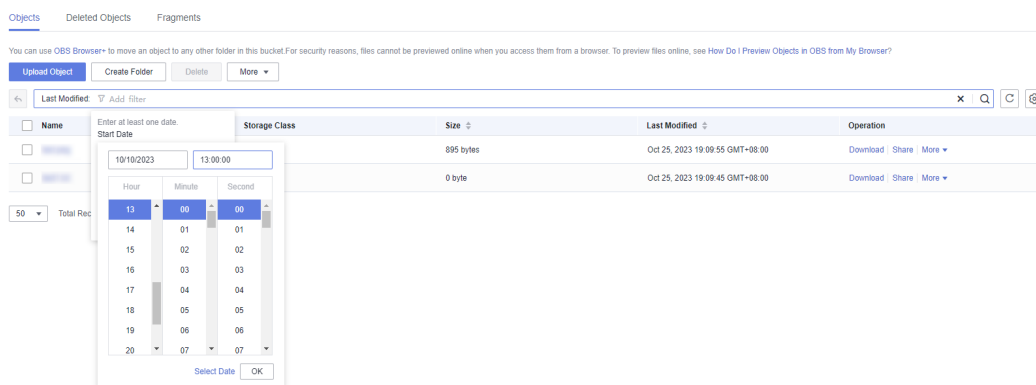
NOTE

The time can be accurate to seconds.
Either start date or end date must be specified.

3. Click **OK**. The objects last modified within the specified time range are displayed in the object list.

Suppose you want to search for objects uploaded from 13:00:00 on October 10, 2023. Click the search box and choose **Last Modified** from the drop-down list. Then, click the text box for **Start Date**, specify the time (13:00:00 on October 10, 2023) and click **OK**. Objects uploaded from 13:00:00 on October 10, 2023 will be displayed in the object list.

Figure 5-7 Searching for objects by last modification time



Step 5 Search for objects by object name prefix:

1. Click the search box above the object list and choose **Object Name Prefix** from the drop-down list.
2. In the search box, enter the name prefix of the files or folders you want to search for.

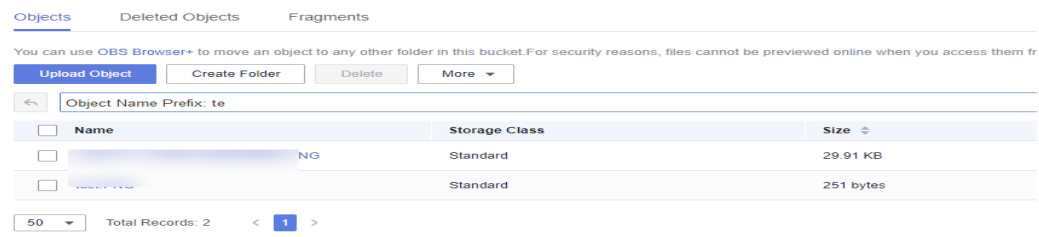
NOTE

The object name prefix is case sensitive.

- Click  or press **Enter**. The searched objects are displayed in the object list.

Suppose you want to search for objects whose prefix is **te**. Click the search box and choose **Object Name Prefix** from the drop-down list box. Then, enter **te**, and press **Enter**. Objects with the **te** prefix will be displayed in the object list.

Figure 5-8 Searching for objects by object name prefix



NOTE

To search for objects within a folder, use either of the following methods:

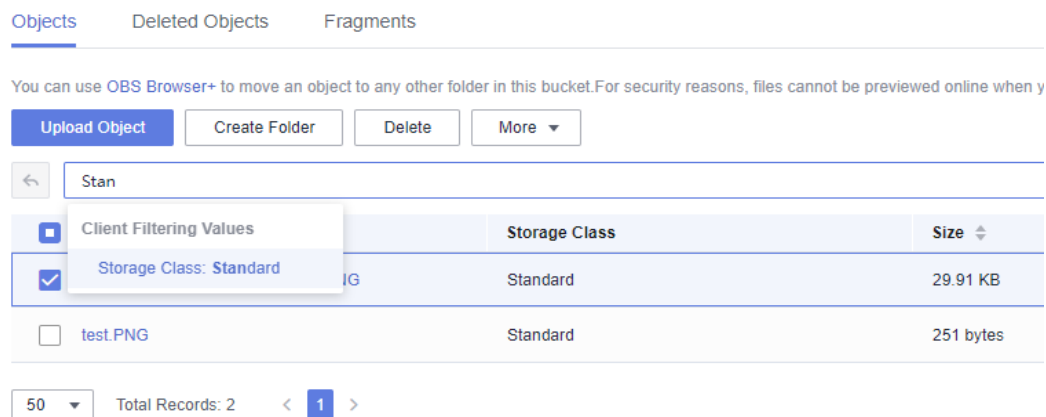
- In the root directory, click the search box above the object list and choose **Object Name Prefix** from the drop-down list. Then, enter *Folder path/Prefix* in the search box. For example, if you enter **abc/123/example**, all files and folders with the **example** prefix in the **abc/123** folder will be displayed.
- Open the folder, and enter the object name prefix in the search box. For example, after you open the **abc/123** folder and enter **example** in the search box, all files and folders with the **example** prefix in the **abc/123** folder will be displayed.

Step 6 Search for objects by entering a storage class keyword or an object name prefix in the search box above the object list.

- Enter a storage class keyword. All objects whose storage class contains the specified keyword will be displayed in the object list.

Suppose you enter **Stan** in the search box. The system will then display the **Standard** storage class. After you click this storage class, all objects whose storage class is Standard will be displayed in the object list.

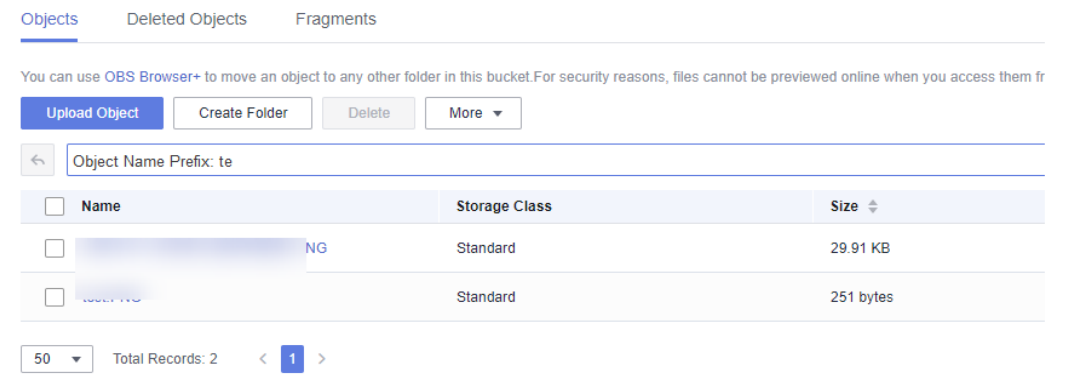
Figure 5-9 Searching for objects by storage class keyword



- Enter an object name prefix and click  or press **Enter**. All files and folders with the specified prefix will be displayed in the object list.

Suppose you want to search for objects with the **te** prefix. Enter **te** in the search box and press **Enter**. Then, all objects with the **te** prefix will be displayed in the object list.

Figure 5-10 Searching for objects by object name prefix




 **NOTE**

You can search for objects based on a combination of different filter criteria.

- If the filter criteria are of different types, they are in intersection logic. For example, if you select storage class **Standard** and object name prefix **te** as two criteria, objects whose storage class is Standard and prefix is **te** will be displayed in the object list.
- If the filter criteria are of the same type, they are in union logic. For example, if you select storage class **Standard** and then **Infrequent Access** as two criteria, objects in both Standard and Infrequent Access storage classes will be displayed in the object list.

----End

Related Operations

In the object list, click  next to the size or last modification time to sort objects.

 **NOTE**

Object search by last modification time can only display the first 1,000 records.

If there are more than 5,000 objects in a bucket, the objects are sorted in alphabetical order and can be searched only by object name prefix.

5.4.3 Accessing an Object Using Its URL

You can grant anonymous users the read permission for an object so they can access the object using the shared object URL.

Prerequisites

Anonymous users have the read permission for the object.

For details about permission granting, see [Granting All Accounts the Read Permission for Certain Objects](#).

 NOTE

Encrypted objects cannot be shared.

Procedure

- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** Click the object to be shared. The object information is displayed on the top part of the page. You can find the link for accessing the object in the **Link** area, as shown in **Figure 5-11**.

Anonymous users can access the object by clicking this link. An object link (URL) is in the format of **https://*Bucket name.Domain name/Directory level/Object name***. If the object is in the root directory of the bucket, its URL does not contain any directory level. To learn more about domain names, see **OBS Domain Names**.

Figure 5-11 Object link

| | | | | |
|---------------|-----------------------------------------------------------------------------------|---------------|-----------------------------------------------|----|
| Name | object_002.PNG | Storage Class | Standard Change Storage Class | |
| Last Modified | Jun 07, 2022 09:50:12 GMT+08:00 | Size | 37.51 KB | |
| Link |  | | Version ID | -- |
| Encrypted | No | | | |

 NOTE

- To allow anonymous users to access objects in Archive or Deep Archive storage using URLs, ensure that these objects are in the **Restored** state.

----End

5.4.4 Sharing an Object

Scenarios

You can share temporary URLs of your objects with others for them to access your objects stored in OBS.

Background Information

File sharing is temporary. All sharing URLs are only valid for a limited period of time.

A temporary URL consists of the access domain name and the temporary authentication information of a file. Example:

```
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
```

The temporary authentication information contains the **AccessKeyId**, **Expires**, **x-obs-security-token**, and **Signature** parameters. **AccessKeyId**, **x-obs-security-token**, and **Signature** are used for authentication. The **Expires** parameter specifies the validity period of the authentication. For more information about temporary

authentication methods and parameters, see [Authentication of Signature in a URL](#) in *Object Storage Service API Reference*.

After an object is shared on OBS Console, the system will generate a URL that contains the temporary authentication information, valid for five minutes since its generation by default. Each time you change the validity period of a URL, OBS obtains the authentication information again to generate a new URL for sharing, which takes effect since the time when the validity period is changed.

Constraints

- An object shared from OBS Console can be valid for one minute to 18 hours. If you need a longer validity period, use OBS Browser+ that allows a validity period of up to one year to share the object. If you want a shared object permanently valid, [use a bucket policy to grant anonymous users the public read permission for the object](#).
- Only version 3.0 buckets support file sharing. You can view the bucket version in the **Basic Information** area on the **Overview** page of a bucket.
- Archive objects can be shared only after they have been restored.
- Deep Archive objects can be shared only after they have been restored.
- Object sharing is available in all regions except CN Southwest-Guiyang1.

Procedure

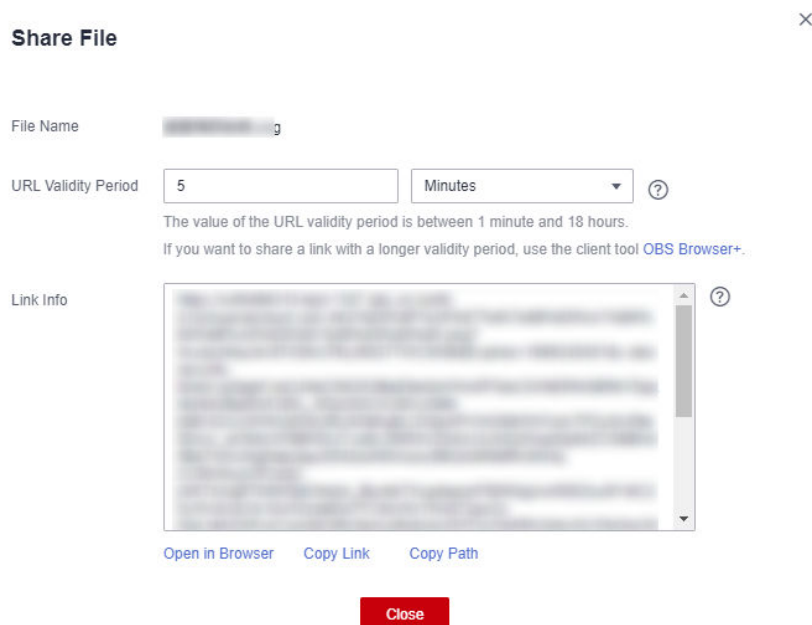
Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 Locate the file to be shared and click **Share** in the **Operation** column.

Once the **Share File** dialog box is opened, the URL is effective and valid for five minutes by default. If you change the validity period, the authentication information in the URL changes accordingly, and the URL's new validity period starts upon the change.

Figure 5-12 Sharing a file



Step 4 Operate the URL as follows:

- Click **Open URL** to preview the file on a new page or directly download it to your default download path.
- Click **Copy Link** to share the link to others for them to access this file using a browser.
- Click **Copy Path** to share the file path to users who have access to the bucket. The users then can search for the file by pasting the shared path to the search box of the bucket.

NOTE

Within the URL validity period, anyone who has the URL can access the file.

----End

5.4.5 Restoring an Object from Archive or Deep Archive Storage

You must restore an object in the Archive or Deep Archive storage class before you can download it or access it with a URL.

To learn the costs involved in data restore, see [Product Pricing Details](#).

Constraints

- If an Archive or a Deep Archive object is being restored, its restore task cannot be suspended or deleted.
- An object being restored cannot be restored again.
- After an object is restored, an object copy in the Standard storage class will be generated. This way, there is an Archive or a Deep Archive object and a Standard object copy in the bucket at the same time. During the restore

validity period, you will be charged for the space taken up by both the object and its copy. The copy will be automatically deleted once the restore expires.

Procedure

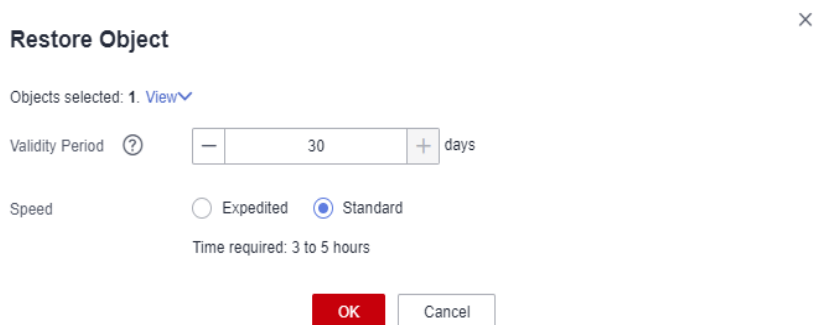
- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** Select the file you want to restore, and click **Restore** on the right. The following dialog box shown in **Figure 5-13** is displayed.

You can select multiple files and choose **More > Restore** above the file list to batch restore them.

NOTE

Objects that are being restored cannot be added for batch restore.

Figure 5-13 Restoring an object



- Step 4** Configure the validity period and speed of the restore. The following table describes the parameters.

Table 5-3 Parameters for restoring objects

| Parameter | Description |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Validity Period | How long the object will remain in the Restored state. It starts once the object is restored. The value is an integer ranging from 1 to 30 (days). The default value is 30 . For example, if you set Validity Period to 20 when restoring an object, 20 days after the object is successfully restored, its status will change from Restored to Unrestored . |
| Speed | How fast an object will be restored. <ul style="list-style-type: none"> • Expedited: Archive objects can be restored within 1 to 5 minutes, and Deep Archive objects can be restored within 3 to 5 hours. • Standard: Archive objects can be restored within 3 to 5 hours, and Deep Archive objects can be restored within 5 to 12 hours. |

Step 5 Click **OK**.

 **NOTE**

The system checks the file restore status at UTC 00:00 every day. The system starts counting down the expiration time from the time when the latest check is complete.

----End

Related Operations

Within the validity period of a restored object, you can restore the object again. The validity period is then extended because it will start again when the latest restore is complete.

 **NOTE**

If a restored object is restored again, its expiration time should be later than the time set for the previous restore. Assume that an object is restored on January 1 and will expire 30 days later (on January 30). If the object is restored again on January 10 and is made to be expired earlier than January 30 (less than 20 days later), this restore action is considered invalid.

5.4.6 Configuring Direct Reading

With direct reading enabled for a bucket, you can access objects in the Archive storage class without restoring them first. Downloading or copying Archive objects will incur costs for directly reading these objects. For details, see [Product Pricing Details](#).

You can enable direct reading for a bucket during its creation. For details, see [Creating a Bucket](#). Alternatively, you can enable direct reading for an existing bucket by doing as follows:

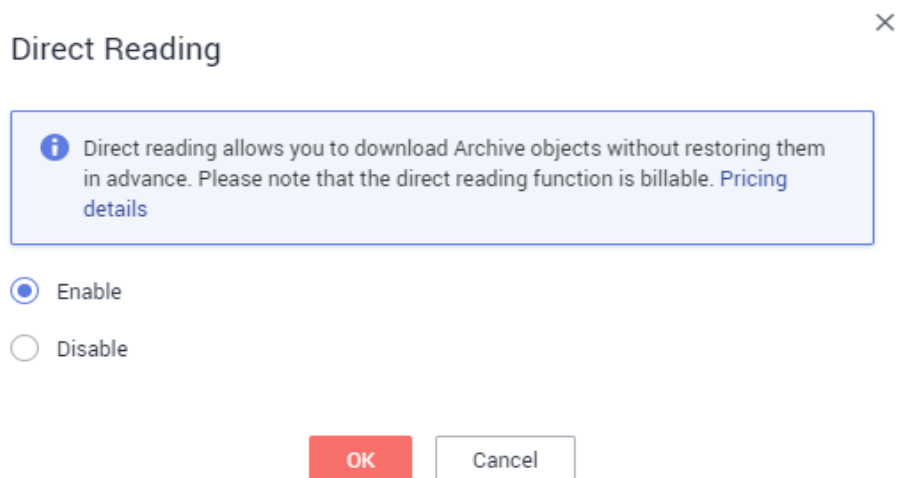
 **NOTE**

Direct reading is only available in some regions. For details, see [Function Overview](#).

Procedure

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the navigation pane, choose **Overview**.
- Step 4** In the **Basic Configurations** area, click **Direct Reading**. The **Direct Reading** dialog box is displayed.
- Step 5** Select **Enable**.

Figure 5-14 Enabling direct reading



Step 6 Click **OK**.

----End

5.4.7 Configuring Object Metadata

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 Click the object to be operated, and then click the **Metadata** tab.

Step 4 Click **Add** and specify the metadata information, as shown in [Figure 5-15](#).

Figure 5-15 Adding metadata



Step 5 Click **OK**.

----End

5.5 Deleting Objects

5.5.1 Deleting an Object or Folder

Scenarios

On OBS Console, you can manually delete unneeded files or folders to release space and reduce costs.

Alternatively, you can configure lifecycle rules to periodically, automatically delete some or all of the files and folders from a bucket. For details, see [Configuring a Lifecycle Rule](#).

In big data scenarios, parallel file systems usually have deep directory levels and each directory has a large number of files. In such case, deleting directories from parallel file systems may fail due to timeout. To address this problem, you are advised to delete directories in either of the following ways:

1. On the Hadoop client that has OBSA, an OBS client plugin, embedded, run the **hadoop fs - rmr obs://***{Name of a parallel file system}***/{Directory name}** command.
2. Configure [a lifecycle rule](#) for directories so that they can be deleted in background based on the preset lifecycle rule.

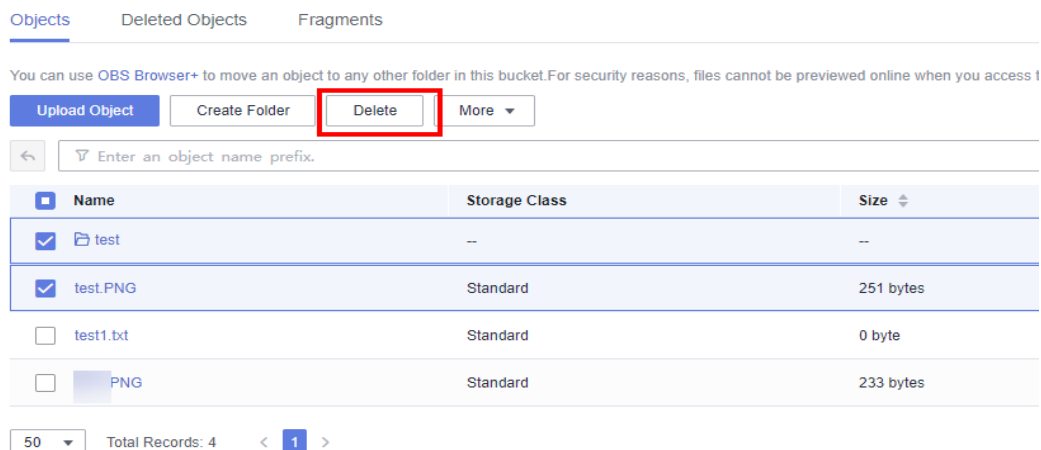
Background Information

Object Deletion with Versioning Enabled

When versioning is enabled for a bucket, OBS works slightly different when deleting different objects.

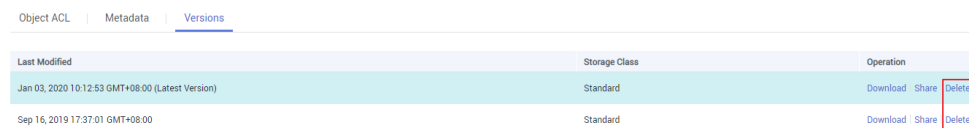
- Deleting a file or folder: The file or folder is not permanently deleted, but is retained in the **Deleted Objects** list and marked with the **Delete Marker**. In **Deleted Objects**, click the object name. On the **Versions** tab, you can see that the latest object version has the delete marker.

Figure 5-16 Deleting a file or folder



- To permanently delete the file or folder, delete it again from the **Deleted Objects** list. For details, see [Procedure](#).
- To recover the deleted file, undelete it from the **Deleted Objects** list. For details, see [Undeleting an Object](#).
- Deleting an object version: The version will be permanently deleted and cannot be recovered. If the deleted version is the latest one, the next latest version becomes the latest version.

Figure 5-17 Deleting a version of an object

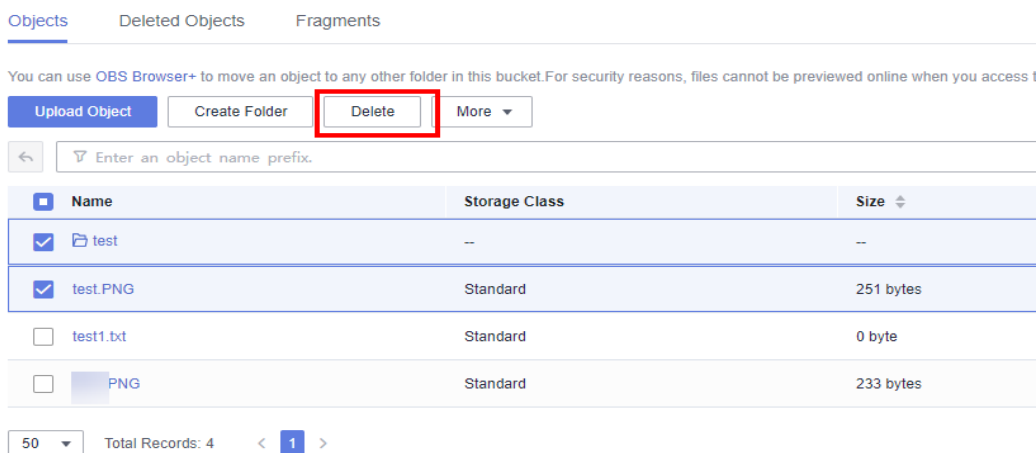


Procedure

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** Select the file or folder you want to delete and choose **More > Delete** on the right.

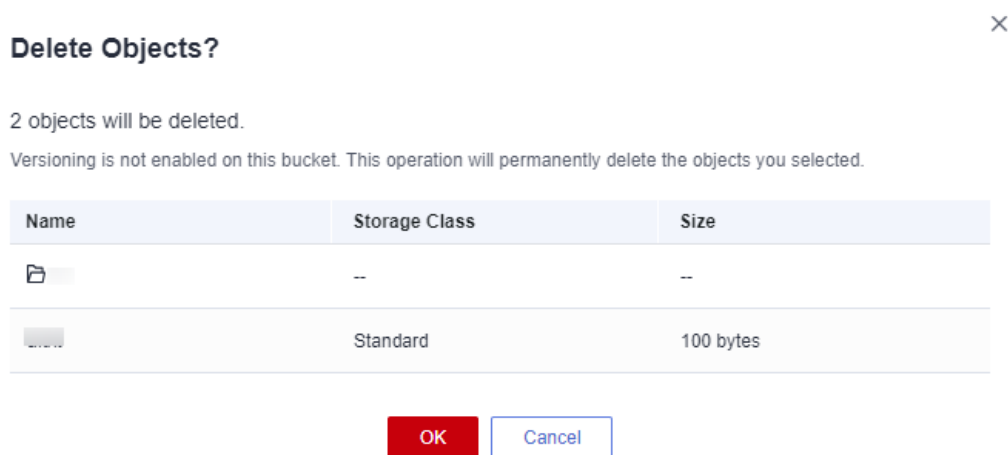
You can select multiple files or folders and click **Delete** above the object list to batch delete them.

Figure 5-18 Deleting a file or folder



Step 4 Click **OK** to confirm the deletion.

Figure 5-19 Deleting objects



CAUTION

If you delete an object from a bucket with versioning enabled, the object is not permanently deleted but retained in the **Deleted Objects** list. All versions of the object are still kept in the bucket and are billed for storage. If you need to permanently delete the object, see the following steps.

Step 5 If versioning is enabled for the bucket, delete the files or folders again from the **Deleted Objects** list to permanently delete them.

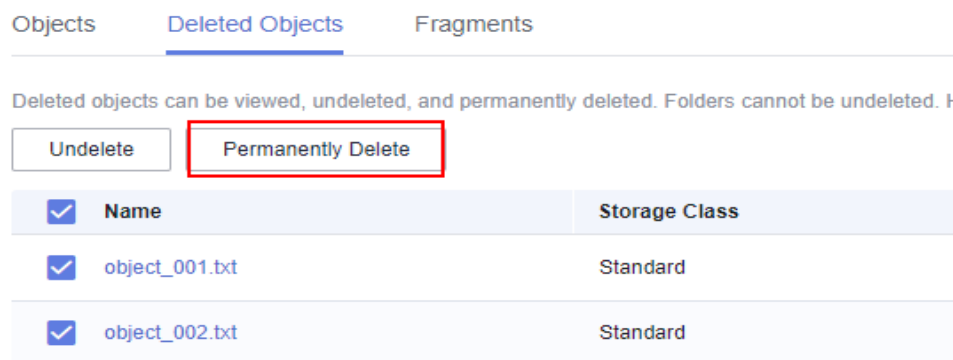
NOTE

In a bucket with WORM enabled, objects cannot be permanently deleted from the **Deleted Objects** list. You can permanently delete an object on its details page. For details, see [Related Operations](#) or [Configuring WORM Retention](#).

Likewise, folders cannot be permanently deleted from the **Deleted Objects** list either. To permanently delete a folder, you can only [configure a lifecycle rule](#).

1. Click **Deleted Objects**.
2. In the **Operation** column of the file or folder to be deleted, click **Permanently Delete**.
You can also select multiple files or folders and click **Permanently Delete** above the object list to batch delete them.

Figure 5-20 Deleting a file or folder permanently



----End

Related Operations

When versioning is enabled, files in the **Deleted Objects** list also have multiple versions. Note the following points when deleting different versions of files:

Figure 5-21 Versions of files in the **Deleted Objects** list

| Last Modified | Storage Class | Operation |
|----------------------------------------------------------------|---------------|-----------------------|
| Jun 07, 2022 10:15:40 GMT+08:00(Delete Marker)(Latest Version) | Standard | Delete |
| Jun 07, 2022 10:15:01 GMT+08:00 | Standard | Download Share Delete |
| Jun 07, 2022 09:50:12 GMT+08:00 | Standard | Download Share Delete |

- Deleting a version with the **Delete Marker** actually recovers this version instead of permanently deleting it. For details, see [Undeleting an Object](#).
- Deleting a version without the **Delete Marker** permanently deletes this version. This version will not be recovered even if the object is recovered later.

5.5.2 Undeleting an Object

Scenarios

If a bucket has **versioning** enabled, you can recover a deleted object by undeleting it.

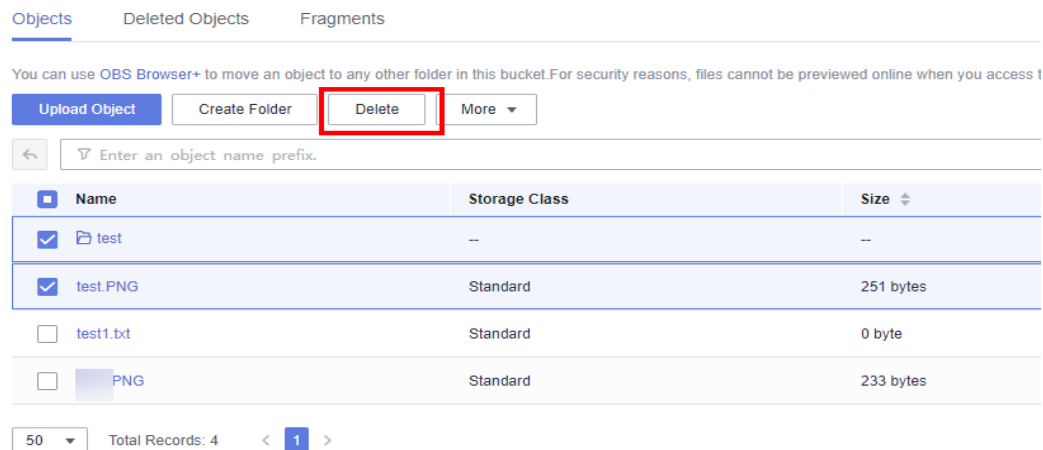
Background Information

Object Deletion with Versioning Enabled

When versioning is enabled for a bucket, OBS works slightly different when deleting different objects.

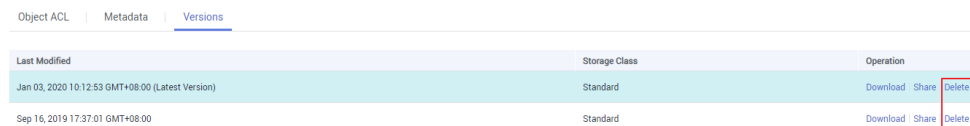
- Deleting a file or folder: The file or folder is not permanently deleted, but is retained in the **Deleted Objects** list and marked with the **Delete Marker**.

Figure 5-22 Deleting a file or folder



- To permanently delete the file or folder, delete it again from the **Deleted Objects** list. For details, see [Deleting an Object or Folder](#).
- To recover the deleted file, undelete it from the **Deleted Objects** list. For details, see [Procedure](#).
- Deleting an object version: The version will be permanently deleted and cannot be recovered. If the deleted version is the latest one, the next latest version becomes the latest version.

Figure 5-23 Deleting a version of an object



Object Recovery with Versioning Enabled

When a bucket has the versioning function enabled, deleting a file from the **Objects** list does not permanently delete it. The deleted file will be retained with the **Delete Marker** in the **Deleted Objects** list. You can recover the deleted file using the **Undelete** operation.

Note the following points when you undelete objects:

1. Only files can be undeleted but not folders.
After you undelete a deleted file, the file is recovered and will appear in the **Objects** list. Then you can perform basic operations on the file as you normally do on other objects. If the file was stored in a folder before the deletion, it will be recovered to its original path after you undelete it.
2. Deleted files in the **Deleted Objects** also keep multiple versions. When deleting different versions of files, note the following points:
 - If you delete a version with the **Delete Marker**, it actually recovers this version instead of permanently deleting it. For details, see [Related Operations](#).

- If you delete a version without the **Delete Marker**, that version is permanently deleted. This version will not be recovered, even if the object is recovered later.

Figure 5-24 Versions of files in the **Deleted Objects** list

| Last Modified | Storage Class | Operation |
|----------------------------------------------------------------|------------------------------------------|-----------------------|
| Jun 07, 2022 10:15:40 GMT+08:00(Delete Marker)(Latest Version) | Object version with the delete marker | Delete |
| Jun 07, 2022 10:15:01 GMT+08:00 | Standard | Download Share Delete |
| Jun 07, 2022 09:50:12 GMT+08:00 | Object version without the delete marker | Standard |

3. A deleted object must have at least one version without the **Delete Marker** in the **Deleted Objects** list. Otherwise, the object cannot be undeleted.

Prerequisites

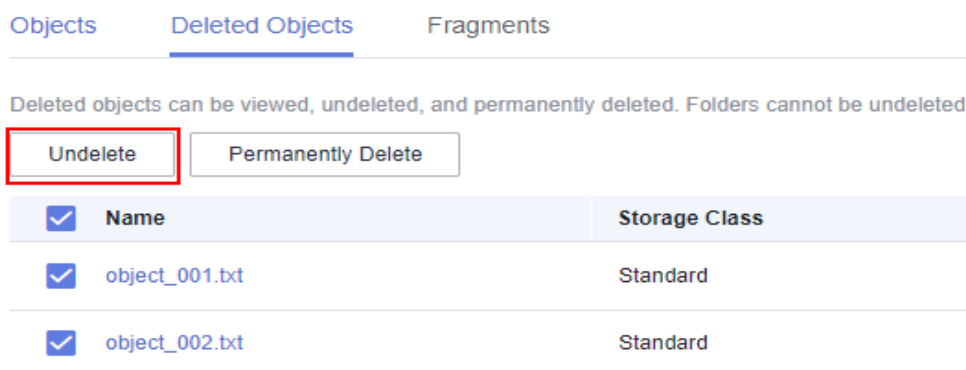
- Versioning has been enabled for the bucket. For details, see [Configuring Versioning](#).
- The file to be recovered is in the **Deleted Objects** list, and has at least one version without the **Delete Marker**.

Procedure

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** Click **Deleted Objects**.
- Step 4** In the row of the deleted object that you want to recover, click **Undelete** on the right.

You can select multiple files and click **Undelete** above the object list to batch recover them.

Figure 5-25 Undeleting a file



----End

Related Operations

Recover a file by deleting its version with the Delete Marker:

- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** Click **Deleted Objects**.
- Step 4** Click the deleted file that you want to recover. The file information is displayed.
- Step 5** On the **Versions** tab page, view all versions of the file.

Figure 5-26 Versions of files in the **Deleted Objects** list

| Last Modified | Storage Class | Operation |
|----------------------------------------------------------------|------------------------------------------------------|---------------------------|
| Jun 07, 2022 10:15:40 GMT+08:00(Delete Marker)(Latest Version) | Object version with the delete marker | Delete |
| Jun 07, 2022 10:15:01 GMT+08:00 | Standard | Download Share Delete |
| Jun 07, 2022 09:50:12 GMT+08:00 | Object version without the delete marker Standard | Download Share Delete |

- If you delete a version with the **Delete Marker**, the file will be recovered and retained in the **Objects** list.
- If you delete a version without the **Delete Marker**, that version will be permanently deleted.

----End

5.5.3 Managing Fragments

Background Information

Data can be uploaded to OBS using multipart uploads. There will be fragments generated, if a multipart upload fails because of the following causes (included but not limited to):

- The network is in poor conditions, and the connection to the OBS server is interrupted frequently.
- The upload task is manually suspended.
- The device is faulty.
- The device is powered off suddenly.

On OBS Console, storage used by fragments is charged. Clear fragments when they are not needed. If a file upload task fails, upload the file again.

NOTICE

Generated fragments take up storage space that is billable.

Constraints

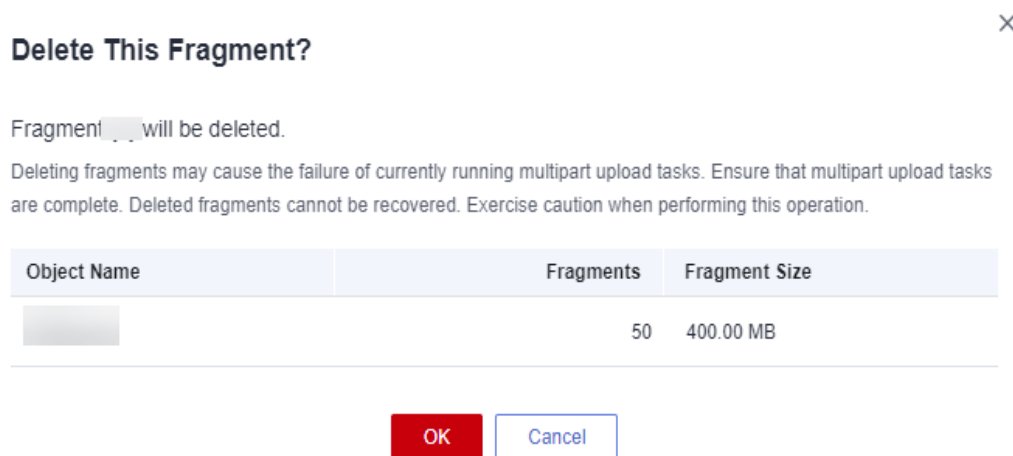
OBS Console currently does not support the deletion of all fragments in a batch. You can use OBS Browser+ to delete all fragments at a time. For details, see [Managing Fragments](#).

Procedure

- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** Click **Fragments**, select the fragment that you want to delete, and click **Delete** on the right.

You can also select multiple fragments and click **Delete** above the fragment list to batch delete them.
- Step 4** Click **OK** to confirm the deletion.

Figure 5-27 Deleting a fragment



----End

6 Permissions Control

6.1 Configuring IAM Permissions

6.1.1 Creating an IAM User and Granting OBS Permissions

You can use [IAM](#) for fine-grained access control over your OBS resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing OBS resources.
- Manage permissions on a principle of least permissions (PoLP) basis.
- Entrust a Huawei Cloud account or cloud service to perform efficient O&M on your OBS resources.

If your Huawei Cloud account does not require individual IAM users, skip this chapter.

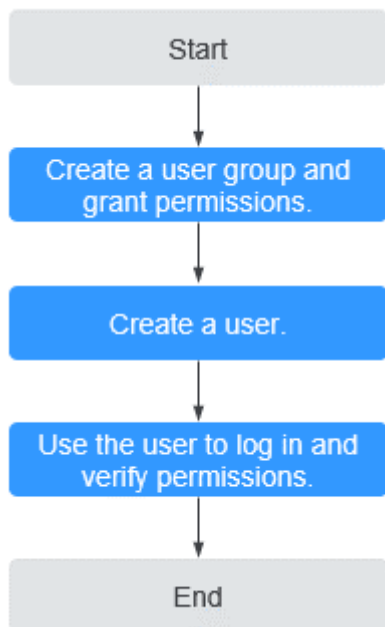
[Figure 6-1](#) shows the procedure for granting permissions.

Prerequisites

You have learned about the [OBS permissions](#) that can be assigned to a user group.

Process

Figure 6-1 Process of granting an IAM user the OBS permissions



The below example describes how to grant an IAM user the **Tenant Guest** permission for OBS.

1. **Create a user group and assign permissions.**
Create a user group on the IAM console, and assign the group the **Tenant Guest** permission.
2. **Create an IAM user and add it to the user group.**
Create a user on the IAM console and add the user to the group created in 1.
3. **Log in** and verify the permission granting.
Log in to OBS Console using the newly created user, and verify that the assigned permission has taken effect:
 - Choose **Object Storage Service** from the service list to go to the OBS homepage. If the list of buckets is displayed and you can view the basic information about any bucket, but you cannot create or delete buckets or perform any other operations, the granted **Tenant Guest** permission has already taken effect.
 - Go to an OBS bucket. If the list of objects is displayed and you can download objects, but you cannot upload or delete objects or perform any other operations, the **Tenant Guest** permission granted has already taken effect.

6.1.2 OBS Custom Policies

Custom policies can be created to supplement the system-defined policies of OBS. For the actions supported for custom policies, see [Bucket-Related Actions](#) and [Object-Related Actions](#).

You can create custom policies in either of the following two ways:

- Visual editor: Select cloud services, actions, resources, and request conditions without the need to know policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see [Creating a Custom Policy](#). The following provides examples of common OBS custom policies.

Example Custom Policies

- Example 1: Grant users all OBS permissions.

This policy allows users to perform any operation on OBS.

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

- Example 2: Grant users all OBS Console permissions.

This policy allows users to perform all operations on OBS Console.

When a user logs in to OBS Console, the user may access resources of other services such as audit information in CTS, acceleration domain names in CDN, and keys in KMS. Therefore, in addition to the OBS permissions in example 1, you also need to configure the access permissions to other services. CDN is a global service, while CTS and KMS are regional ones. You need to configure the **Tenant Guest** permission for the global project and regional projects based on the services and regions that you use.

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

- Example 3: Grant users the read-only permission for all directories in a bucket.

This policy allows users to list and download all objects in 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"
      ]
    }
  ]
}
```

```
]
}
```

- Example 4: Grant users the read-only permission for a specified directory in a bucket.

This policy allows users to download objects in only the **my-project/** directory of bucket **obs-example**. Objects in other directories can be listed but cannot be downloaded.

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

- Example 5: Grant users the read/write permissions for a specified directory in a bucket.

This policy allows users to list, download, upload, and delete objects in the **my-project** directory of 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"
      ]
    }
  ]
}
```

- Example 6: Grant users all permissions for a bucket.

This policy allows users to perform any operation on bucket **obs-example**.

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

- Example 7: Grant users the permission to deny object upload.
A deny policy must be used together with other policies. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

If you grant the system policy OBS OperateAccess to a user but do not want the user to have the object upload permission (which is also a permission allowed by OBS OperateAccess), you can create a custom policy besides the OBS OperateAccess policy, to deny the user's upload permission. According to the authorization principle, the policy with the deny statement takes precedence, so that the user can perform all operations allowed by OBS OperateAccess, except uploading objects. The following is an example of a deny policy:

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

6.1.3 OBS Resources

A resource is an object that exists within a service. OBS resources include buckets and objects. You can select these resources by specifying their paths.

Table 6-1 OBS resources and their paths

| Resource Type | Resource Name | Path |
|---------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Buckets | Bucket | <p>[Format] obs:**:bucket:<i>Bucket name</i></p> <p>[Notes] IAM automatically generates the prefix obs:**:bucket: for bucket resource paths. By adding <i>Bucket name</i> to the end of the generated prefix, you can define a specific path. An asterisk * is allowed to indicate any bucket. An example is given as follows: obs:**:bucket:*</p> |

| Resource Type | Resource Name | Path |
|---------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Objects | Object | [Format] obs:*:*:object:Bucket name/Object name [Notes] IAM automatically generates the prefix obs:*:*:object: for object resource paths. By adding <i>Bucket name/Object name</i> to the end of the generated prefix, you can define a specific path. An asterisk * is allowed to any object in the bucket. An example is given as follows: obs:*:*:object:my-bucket/my-object/* (indicating any object in the my-object directory of bucket my-bucket) |

6.1.4 OBS Request Conditions

Request conditions are useful in determining when a custom policy is in effect. A request condition consists of a condition key and an operator. Condition keys are either global or service-level and are used in the condition elements of a policy statement. **Global condition keys** (starting with **g:**) are available for operations of all services, while service-level condition keys (starting with a service name acronym like **obs:**) are available only for operations of a specific service. An operator is used together with a condition key to form a complete condition statement.

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.

The condition keys and operators supported by OBS are the same as those in the bucket policy. When configuring condition keys in IAM, start them with **obs:**. For details, see [Policy Format](#).

6.2 Configuring a Bucket Policy

6.2.1 Creating a Bucket Policy with a Template

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

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the navigation pane, choose **Permissions > Bucket Policies**.

Step 4 Click **Create**.

Step 5 Choose a policy template. For details about the parameters, see [Bucket Policies](#).

Figure 6-2 Choosing the Public Read template

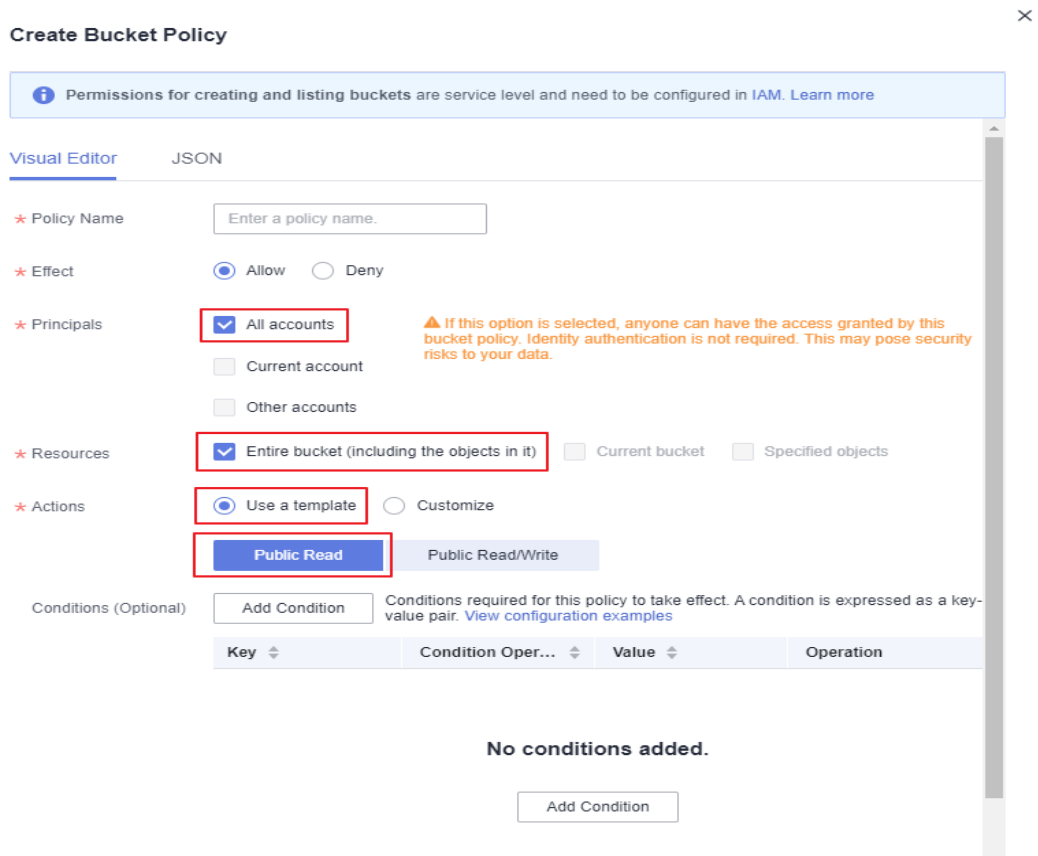


Figure 6-3 Choosing the Public Read/Write template

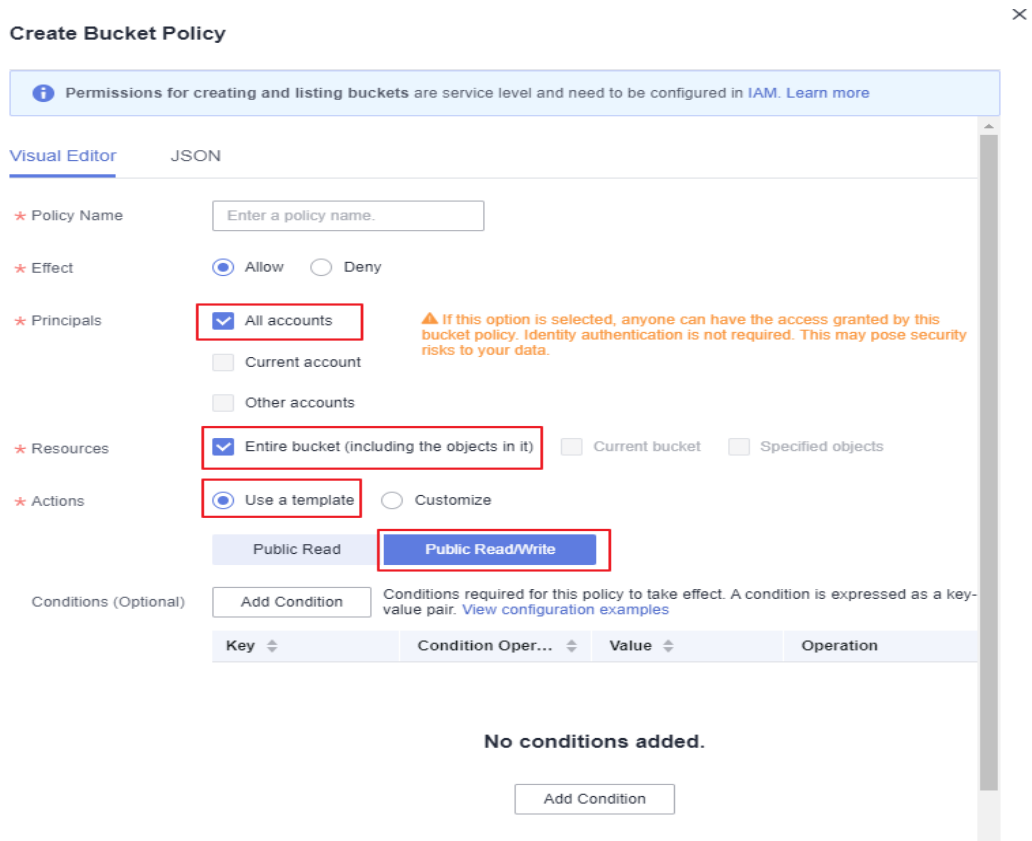


Figure 6-4 Choosing the Bucket Read-Only template

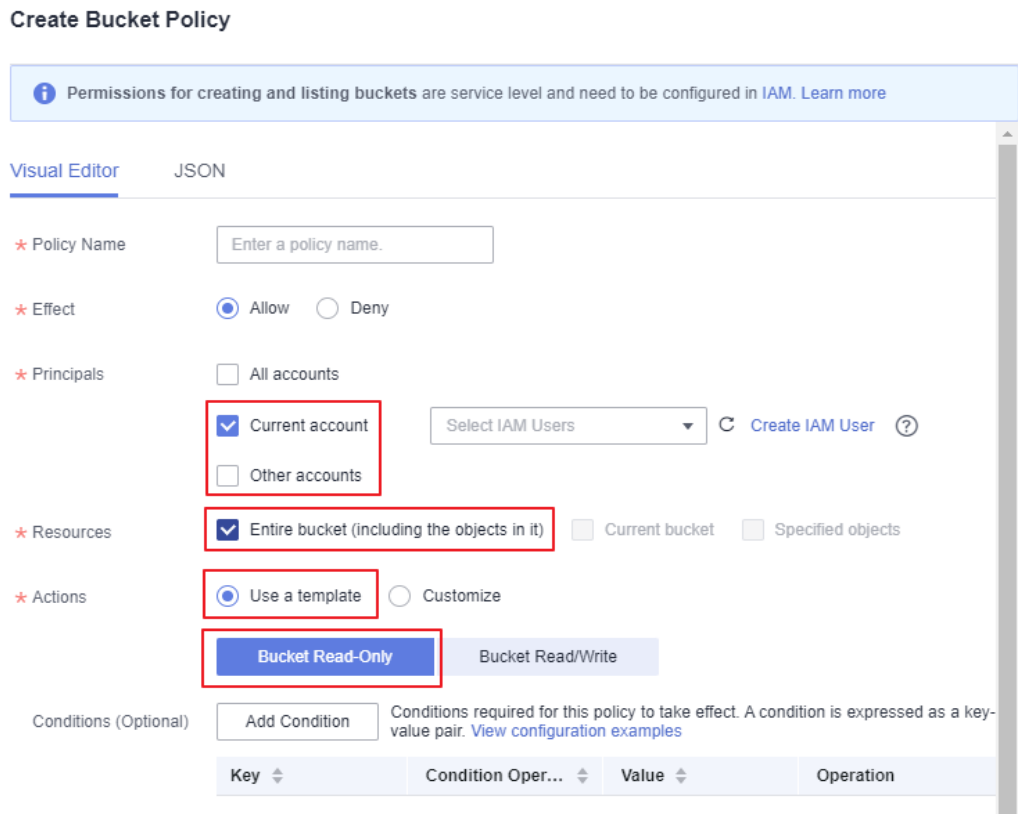


Figure 6-5 Choosing the Bucket Read/Write template

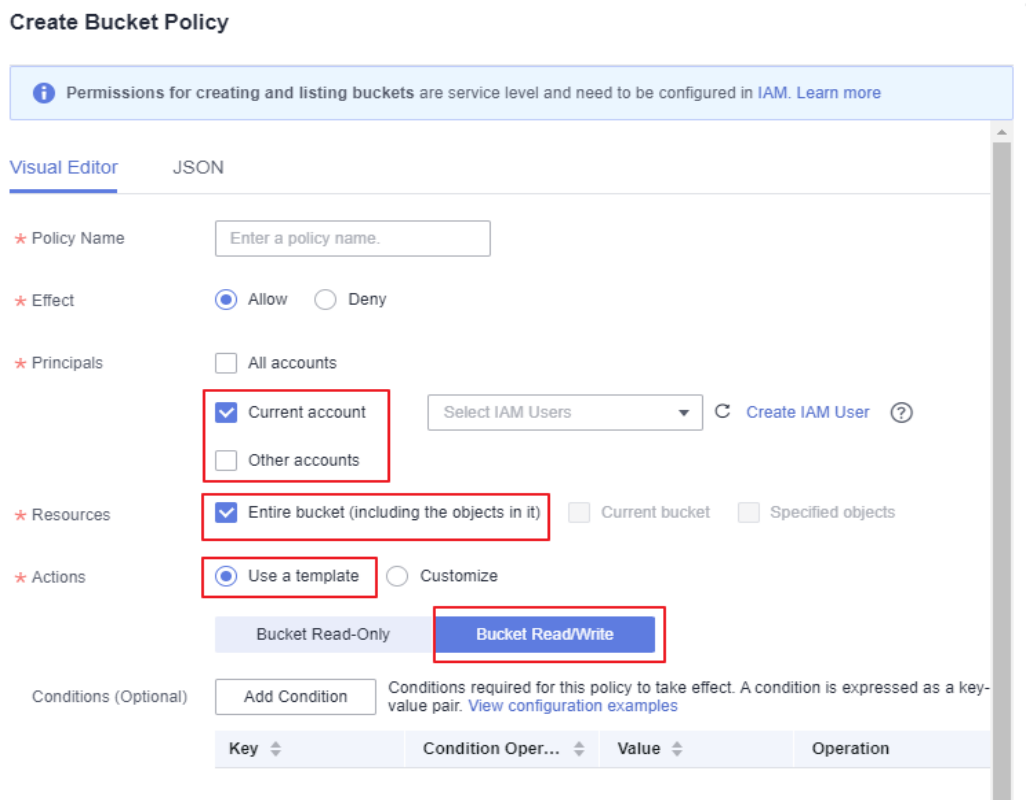


Figure 6-6 Choosing the Directory Read-Only template

Create Bucket Policy

Permissions for creating and listing buckets are service level and need to be configured in IAM. [Learn more](#)

Visual Editor JSON

* Policy Name

* Effect Allow Deny

* Principals

- All accounts ▲ If this option is selected, anyone can have the access granted by this bucket policy. Identity authentication is not required. This may pose security risks to your data.
- Current account
- Other accounts

* Resources

- Entire bucket (including the objects in it)
- Current bucket
- Specified objects

Bucket selected:

Format: Folder name/Object name, for example, testdir/a.txt. * indicates all objects.

[Add](#)

* Actions

- Use a template
- Customize

- Directory Read-Only**
- Directory Read/Write

Conditions (Optional) Conditions required for this policy to take effect. A condition is expressed as a key-value pair. [View configuration examples](#)

| Key | Condition Oper... | Value | Operation |
|-----|-------------------|-------|-----------|
|-----|-------------------|-------|-----------|

Figure 6-7 Choosing the Directory Read/Write template

Create Bucket Policy

Permissions for creating and listing buckets are service level and need to be configured in IAM. [Learn more](#)

Visual Editor JSON

* Policy Name

* Effect Allow Deny

* Principals

- All accounts ▲ If this option is selected, anyone can have the access granted by this bucket policy. Identity authentication is not required. This may pose security risks to your data.
- Current account
- Other accounts

* Resources

- Entire bucket (including the objects in it)
- Current bucket
- Specified objects

Bucket selected:

;

Format: Folder name/Object name, for example, testdir/a.txt. * indicates all objects.

* Actions

- Use a template
- Customize

Conditions (Optional) Conditions required for this policy to take effect. A condition is expressed as a key-value pair. [View configuration examples](#)

| Key | Condition Oper... | Value | Operation |
|-----|-------------------|-------|-----------|
|-----|-------------------|-------|-----------|

Figure 6-8 Choosing the Object Read-Only template

Create Bucket Policy

Permissions for creating and listing buckets are service level and need to be configured in IAM. [Learn more](#)

Visual Editor JSON

* Policy Name

* Effect Allow Deny

* Principals

- All accounts **⚠ If this option is selected, anyone can have the access granted by this bucket policy. Identity authentication is not required. This may pose security risks to your data.**
- Current account
- Other accounts

* Resources

Entire bucket (including the objects in it) Current bucket Specified objects

Format: Folder name/Object name, for example, testdir/a.txt. * indicates all objects.

* Actions

Use a template Customize

Conditions (Optional) Conditions required for this policy to take effect. A condition is expressed as a key-value pair. [View configuration examples](#)

| Key | Condition Oper... | Value | Operation |
|-----|-------------------|-------|-----------|
|-----|-------------------|-------|-----------|

Figure 6-9 Choosing the Object Read/Write template

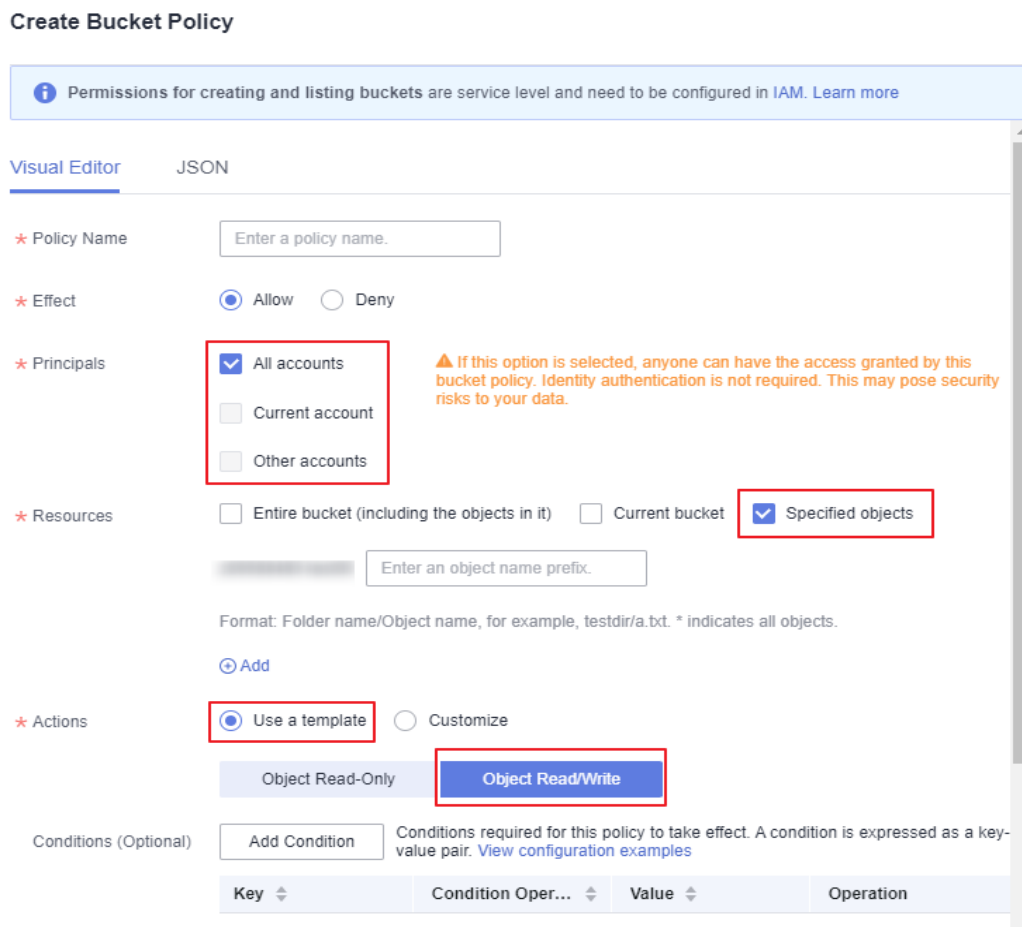


Table 6-2 Bucket policy templates

| Principal | Resource | Template | Actions Allowed | Advanced Settings |
|--------------|---------------------------------------------|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| All accounts | Entire bucket (including the objects in it) | Public Read See Figure 6-2 . | <p>Allows anonymous users to perform the following actions on a bucket and the objects in it:</p> <ul style="list-style-type: none"> HeadBucket (to check whether the bucket exists and obtain the bucket metadata) GetBucketLocation (to get the bucket location) 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) | Excluding the specified actions is not allowed. |

| Principal | Resource | Template | Actions Allowed | Advanced Settings |
|-----------|----------|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| | | Public Read/Write See Figure 6-3 . | <p>Allows anonymous users to perform the following actions on a bucket and the objects in it:</p> <ul style="list-style-type: none"> ListBucket (to list objects in the bucket and obtain the bucket metadata) ListBucketVersions (to list object versions in the bucket) HeadBucket (to check whether the bucket exists and obtain the bucket metadata) GetBucketLocation (to get the bucket location) 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) ListBucketMultipartUploads (to list multipart uploads) 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) | Excluding the specified actions is not allowed. |

| Principal | Resource | Template | Actions Allowed | Advanced Settings |
|-----------------------------------------------------------|---------------------------------------------|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| Current account/ Other accounts/ Delegated accounts | Entire bucket (including the objects in it) | Bucket Read-Only See Figure 6-4 . | Allows specified accounts to perform the following actions on a bucket and the objects in it: Get* (all GET actions) List* (all LIST actions) HeadBucket (to check whether the bucket exists and obtain the bucket metadata) | Excluding the specified actions is not allowed. |
| | | Bucket Read/Write See Figure 6-5 . | Allows specified accounts to perform all actions excluding the following ones on a bucket and the objects in it: DeleteBucket (to delete the bucket) PutBucketPolicy (to configure a bucket policy) PutBucketAcl (to configure the bucket ACL) | The specified actions are excluded. |

| Principal | Resource | Template | Actions Allowed | Advanced Settings |
|----------------------------------------------------------------------------|------------------------------------|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| All accounts/ Current account/ Other accounts/ Delegated accounts | Current bucket + Specified objects | Directory Read-Only See Figure 6-6 . | <p>Allows all accounts or specified accounts to perform the following actions on the current bucket and the specified resources in it:</p> <p>GetObject (to obtain object content and metadata)</p> <p>GetObjectVersion (to obtain the content and metadata of a specified object version)</p> <p>GetObjectVersionAcl (to obtain the ACL of a specified object version)</p> <p>GetObjectAcl (to obtain the object ACL)</p> <p>RestoreObject (to restore objects from Archive storage)</p> <p>ListBucket (to list objects in the bucket and obtain the bucket metadata)</p> <p>ListBucketVersions (to list object versions in the bucket)</p> <p>HeadBucket (to check whether the bucket exists and obtain the bucket metadata)</p> <p>GetBucketLocation (to get the bucket location)</p> <p>NOTE If you apply the policy to All accounts, ListBucket and ListBucketVersions are not included in the template.</p> | Excluding the specified actions is not allowed. |

| Principal | Resource | Template | Actions Allowed | Advanced Settings |
|-----------|----------|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| | | Directory Read/Write See Figure 6-7 . | <p>Allows all accounts or specified accounts to perform the following actions on the current bucket and the specified resources in it:</p> <p>PutObject (to upload objects using PUT and POST, upload parts, initiate multipart uploads, and assemble parts)</p> <p>GetObject (to obtain object content and metadata)</p> <p>GetObjectVersion (to obtain the content and metadata of a specified object version)</p> <p>ModifyObjectMetaData (to modify object metadata)</p> <p>ListBucketMultipartUploads (to list multipart uploads)</p> <p>ListMultipartUploadParts (to list uploaded parts)</p> <p>AbortMultipartUpload (to abort multipart uploads)</p> <p>GetObjectVersionAcl (to obtain the ACL of a specified object version)</p> <p>GetObjectAcl (to obtain the object ACL)</p> <p>PutObjectAcl (to configure the object ACL)</p> <p>RestoreObject (to restore objects from Archive storage)</p> <p>ListBucket (to list objects in the bucket and obtain the bucket metadata)</p> <p>ListBucketVersions (to list object versions in the bucket)</p> <p>HeadBucket (to check whether the bucket exists and obtain the bucket metadata)</p> <p>GetBucketLocation (to get the bucket location)</p> | Excluding the specified actions is not allowed. |

| Principal | Resource | Template | Actions Allowed | Advanced Settings |
|----------------------------------------------------------------------------|-------------------|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| All accounts/ Current account/ Other accounts/ Delegated accounts | Specified objects | Object Read-Only See Figure 6-8 . | <p>Allows all accounts or specified accounts to perform the following actions on specified resources in the bucket:</p> <p>GetObject (to obtain object content and metadata)</p> <p>GetObjectVersion (to obtain the content and metadata of a specified object version)</p> <p>GetObjectVersionAcl (to obtain the ACL of a specified object version)</p> <p>GetObjectAcl (to obtain the object ACL)</p> <p>RestoreObject (to restore objects from Archive storage)</p> | Excluding the specified actions is not allowed. |
| | | Object Read/Write See Figure 6-9 . | <p>Allows all accounts or specified accounts to perform the following actions on specified resources in the bucket:</p> <p>PutObject (to upload objects using PUT and POST, upload parts, initiate multipart uploads, and assemble parts)</p> <p>GetObject (to obtain object content and metadata)</p> <p>GetObjectVersion (to obtain the content and metadata of a specified object version)</p> <p>ModifyObjectMetaData (to modify object metadata)</p> <p>ListMultipartUploadParts (to list uploaded parts)</p> <p>AbortMultipartUpload (to abort multipart uploads)</p> <p>GetObjectVersionAcl (to obtain the ACL of an object version)</p> <p>GetObjectAcl (to obtain the object ACL)</p> <p>PutObjectAcl (to configure the object ACL)</p> <p>RestoreObject (to restore objects from Archive storage)</p> | Excluding the specified actions is not allowed. |

Step 6 Complete the bucket policy configuration.

Some bucket policy templates require a configuration of principals or resources. You can also change the existing settings of a template, including the policy name, principals, resources, actions, and conditions. For details, see [Bucket Policy Parameters](#).

Step 7 Click **Create** in the lower right corner.

----End

6.2.2 Creating a Custom Bucket Policy (Visual Editor)

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

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the navigation pane, choose **Permissions > Bucket Policies**.

Step 4 Click **Create**.

Step 5 Configure a bucket policy.

Figure 6-10 Configuring a bucket policy

Create Bucket Policy X

ℹ Permissions for creating and listing buckets are service level and need to be configured in IAM. [Learn more](#)

Visual Editor JSON

* Policy Name

* Effect Allow Deny

* Principals All accounts ⚠ If this option is selected, anyone can have the access granted by this bucket policy. Identity authentication is not required. This may pose security risks to your data.
 Current account
 Other accounts

* Resources Entire bucket (including the objects in it) Current bucket Specified objects

* Actions Use a template **Customize**

Conditions (Optional) Conditions required for this policy to take effect. A condition is expressed as a key-value pair. [View configuration examples](#)

| Key | Condition Oper... | Value | Operation |
|----------------------|-------------------|-------|-----------|
| No conditions added. | | | |

Table 6-3 Parameters for configuring a custom bucket policy

| Parameter | | Description |
|----------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Method | | Visual editor or JSON. The visual editor is used here. For details about configurations in the JSON view, see Creating a Custom Bucket Policy (JSON View) . |
| Policy Name | | Enter a bucket policy name. |
| Policy content | Effect | <ul style="list-style-type: none"> Allow: The policy allows the matched requests. Deny: The policy denies the matched requests. |

| Parameter | | Description |
|-----------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Principals | <ul style="list-style-type: none"> ● All accounts: The bucket policy applies to anonymous users. ● Current account: Specify one or more IAM users under the current account. ● Other accounts: Specify one or more accounts. <p>NOTE The account ID and IAM user ID can be obtained from the My Credentials page.</p> <p>Accounts should be configured in the <i>Domain ID/IAM user ID</i> format, with each one on a separate line.</p> <p><i>Account ID/*</i> indicates that permission is granted to all IAM users under the account.</p> <ul style="list-style-type: none"> ● Delegated accounts: Delegated accounts can be added only after Other accounts is selected. <p>NOTE Delegated accounts should be configured in the <i>ID of a delegating account/Agency name</i> format. Multiple delegated accounts are allowed, with each one on a separate line.</p> |
| | Resources | <ul style="list-style-type: none"> ● Entire bucket (including the objects in it): The policy applies to the bucket and the objects in it. You can configure bucket and object actions in this policy. ● Current bucket: The policy applies to the current bucket. You can configure bucket actions in this policy. ● Specified objects: The policy applies to specified objects in the bucket. You can configure object actions in this policy. <p>NOTE</p> <ol style="list-style-type: none"> 1. Multiple resource paths can be specified. 2. A resource path should be configured in the <i>Folder name/Object name</i> format, for example, testdir/a.txt. To specify the testdir folder and all objects in it, enter testdir/*. 3. You can specify a specific object, an object set, or a directory. * indicates all objects in the bucket. To specify a specific object, enter the object name. To specify a set of objects, enter <i>Object name prefix*</i>, <i>*Object name suffix</i>, or *. For example, testdir/* indicates objects in the testdir folder, and testprefix* indicates objects whose prefix is testprefix. |

| Parameter | | Description |
|-----------|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Actions | <ul style="list-style-type: none"> ● Actions: Choose Customize. ● Select Actions: See Bucket Policy Parameters. <p>NOTE</p> <ol style="list-style-type: none"> 1. If you select Entire bucket (including the objects in it) for Resources, common actions, bucket actions, and object actions will be available for you to choose from. 2. If you select Current bucket for Resources, common actions and bucket actions will be available for you to choose from. 3. If you select Specified objects for Resources, common actions and object actions will be available for you to choose from. 4. If you select both Current bucket and Specified objects for Resources, common actions, bucket actions, and object actions will be available for you to choose from. |
| | Conditions (Optional) | <ul style="list-style-type: none"> ● Key: See Bucket Policy Parameters. ● Conditional Operator: See Bucket Policy Parameters. ● Value: The entered value is associated with the key. |
| | Advanced Settings > Exclude (Optional) | <ul style="list-style-type: none"> ● Specified principals: By selecting this option, the bucket policy applies to users except the specified ones. <p>NOTE If you do not select this option, the bucket policy applies to the specified users.</p> <ul style="list-style-type: none"> ● Specified resources: By selecting this option, the bucket policy applies to resources except the specified ones. <p>NOTE If you do not select this option, the bucket policy applies to the specified resources.</p> <ul style="list-style-type: none"> ● Specified actions: By selecting this option, the bucket policy applies to actions except the specified ones. <p>NOTE</p> <ol style="list-style-type: none"> 1. If you do not select this option, the bucket policy applies to the specified actions. 2. By default, Specified actions is selected for Exclude in the bucket read/write template only. The action exclusion setting in bucket policy templates cannot be modified. |

Step 6 Click **Create** in the lower right corner.

----End

6.2.3 Creating a Custom Bucket Policy (JSON View)

If you are familiar with the JSON syntax and OBS bucket policies, you can code a bucket policy in the JSON view. There is no limit on the number of bucket policies (statements) for a bucket, but the JSON descriptions of all bucket policies in a bucket cannot exceed 20 KB in total.

Procedure

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the navigation pane, choose **Permissions > Bucket Policies**.
- Step 4** In the upper right corner of the page, click **JSON** and then **Edit**.
- Step 5** Edit the bucket policy. Below gives a bucket policy example in 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"
    }
  ]
}
```

Table 6-4 Parameters for creating a bucket policy in JSON

| Parameter | Description |
|-----------|---------------------------------------------------------------------------------------------------|
| Action | Actions the bucket policy applies to. For details, see Bucket Policy Parameters . |
| Effect | Effect of the bucket policy. For details, see Bucket Policy Parameters . |

| Parameter | Description |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Principal | Users the bucket policy is applied to. You can obtain the user ID on the My Credentials page by logging in to the console as the user to be authorized. Principals should be configured as follows: <ul style="list-style-type: none">• domain/Account ID (indicating that the principal is an account)• domain/Account ID:user/User ID (indicating that the principal is a user under an account) |
| Condition | Conditions under which the bucket policy takes effect. For details, see Bucket Policy Parameters . |
| Resource | Resources the bucket policy is applied to. For details, see Bucket Policy Parameters . |

Step 6 Click **Create**.

----End

6.2.4 Replicating Bucket Policies

Scenarios

OBS allows you to replicate the existing bucket policies to a new bucket. When replicating policies, OBS automatically replaces the bucket name in the source bucket policies with the destination bucket name, for the policies to apply to the destination bucket.

Constraints

- The policies replicated from a source bucket will not overwrite existing policies in the destination bucket.
- The source policies with the same name as those in the destination bucket will not be replicated.
- Both source and destination buckets must be of the 3.0 version.

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

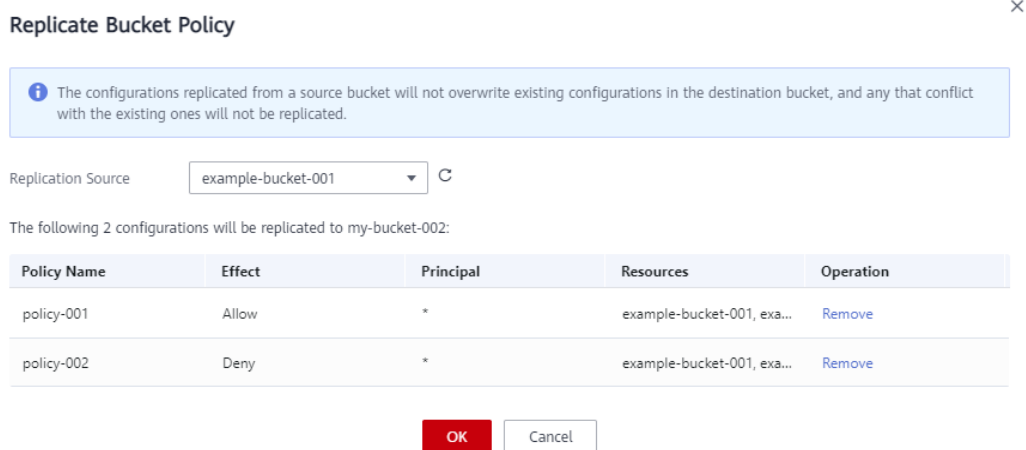
Step 3 In the navigation pane, choose **Permissions > Bucket Policies**.

Step 4 Click **Replicate**.

Step 5 Select a replication source, which is the bucket whose policies you want to replicate.

After you select a replication source, all bucket policies with different name from those in the destination bucket are displayed. You can remove any that are not required.

Figure 6-11 Replicating bucket policies



Step 6 Click **OK** to replicate the bucket policies to the destination bucket.

----End

6.3 Configuring an Object Policy

Object policies are applied to the objects in a bucket. With an object policy, you can configure conditions and actions for objects in a bucket.

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the row containing the object for which you want to configure a policy, choose **More > Configure Object Policy** in the **Operation** column. The **Configure Object Policy** page is displayed.

You can customize a policy or use a preset template to configure one as needed.

- **Using a preset template:** The system presets object policy templates for four typical scenarios. You can use the templates to quickly configure object policies. For details about each template, see [Bucket Policy Parameters](#).
- **Customizing a policy:** You can also customize an object policy based on your needs. A custom object policy consists of five basic elements: effect, principals, 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. For details about how to customize an object policy, see [Creating a Custom Bucket Policy \(Visual Editor\)](#). Different from customizing a bucket policy, to customize an object policy, you:

- a. Do not need to specify the resource.
- b. Can configure only object-related actions.

----End

6.4 Configuring a Bucket ACL

Prerequisites

You are the bucket owner or you have the permission to write the bucket ACL.

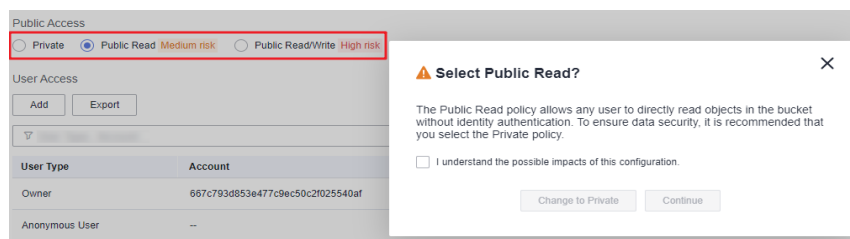
Procedure

- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the navigation pane, choose **Permissions > Bucket ACLs**.
- Step 4** On the **Bucket ACLs** page, choose a permission from **Private**, **Public Read**, and **Public Read/Write** to grant bucket ACL permission for anonymous users.

NOTE

1. After you change **Public Read** or **Public Read/Write** to **Private**, only the bucket owner or object owner has the access.
2. After you change **Private** to **Public Read**, anyone can read objects in the bucket. No identity authentication is required.
3. After you change **Private** to **Public Read/Write**, anyone can read, write, and delete objects in the bucket. No identity authentication is required.

Figure 6-12 Changing a public access permission



- Step 5** In the **Operation** column, click **Edit** to grant the owner, anonymous user, or log delivery user required ACL permissions for the bucket.
- Step 6** In the middle of the page, click **Export** to get the bucket ACL configuration. The file includes the user type, account, bucket access, and ACL access.
- Step 7** In the middle of the page, click **Add** to apply specific ACL permissions to an account.

Enter an account ID and specify ACL permissions for the account. You can obtain the account ID from the **My Credentials** page.

Click **OK**.

NOTE

To select **Object read** for **Object Permission**, you must select **Read** for **Access to Bucket**.

Figure 6-13 Granting permissions

Add Account Authorization ×

Account ?

⚠ Only an account ID is supported.

Access to Bucket Read Write

Object Permission Object read

Access to ACL Read Write

----End

Follow-up Procedure

After a specified account is granted the ACL permissions for a bucket, the authorized user can use the AK and SK to access that bucket by adding the bucket to OBS Browser+.

After certain permissions are granted to an anonymous user, the anonymous user can access the bucket without any authentication. The anonymous user can be either registered or non-registered. A registered anonymous user can use either of the methods above to access the bucket, while a non-registered anonymous user can access the bucket in any of the following ways:

- Access the bucket's domain name in a browser to view the objects in the bucket.
- Configure the bucket's domain name in a third-party system to directly connect to the bucket.

6.5 Configuring an Object ACL

Prerequisites

You are the object owner or you have the permission to write the object ACL.

An object owner is the account that uploads the object, but may not be the owner of the bucket that stores the object. 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, account **B**, instead of the bucket owner account **A**, is the

owner of the object. By default, account A is not allowed to access this object and cannot read or modify the object ACL.

Procedure

Step 1 In the navigation pane of **OBS Console**, choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

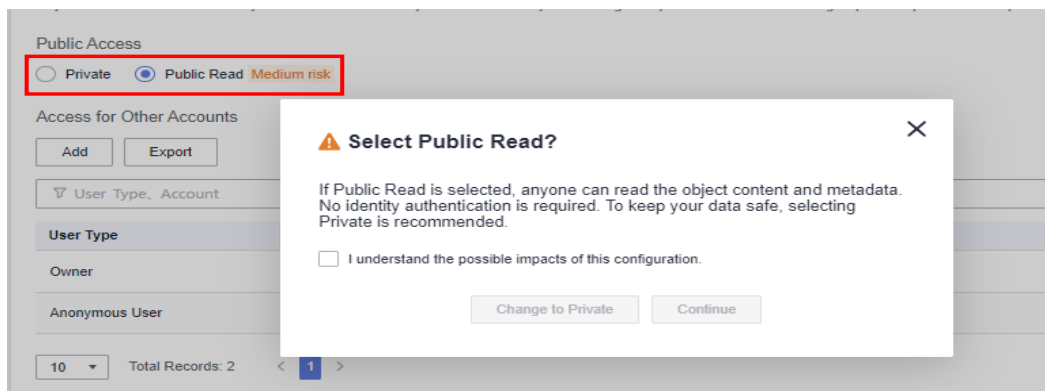
Step 3 Click a desired object.

Step 4 On the **Object ACL** page, choose a permission from **Private** and **Public Read** to grant object ACL permission for anonymous users.

NOTE

1. After you change **Public Read** to **Private**, only the bucket owner or object owner has the access.
2. After you change **Private** to **Public Read**, anyone can read the object content and metadata. No identity authentication is required.

Figure 6-14 Changing a public access permission



Step 5 Click **Edit** to grant the owner, anonymous user, or other accounts required permissions for the object.

NOTE

ACL permissions for encrypted objects cannot be granted to registered users or anonymous users.

Step 6 Click **Export** to get the object ACL configuration. The file includes the user type, account, object access, and ACL access.

Step 7 Click **Add** to apply specific ACL permissions to an account.

Enter an account ID and specify ACL permissions for the account. You can obtain the account ID from the **My Credentials** page.

Click **OK**.

Figure 6-15 Granting permissions

✕

Add Account Authorization

Account ?

▲ Only an account ID is supported.

Access to Object Read

Access to ACL Read Write

OK Cancel

----End

7 Data Management

7.1 Configuring a Lifecycle Rule

You can configure a lifecycle rule for a bucket or a set of objects to:

- Transition objects from Standard to Infrequent Access or Archive or Deep Archive.
- Transition objects from Infrequent Access to Archive or Deep Archive.
- Transition objects from Archive to Deep Archive.
- Expire objects and then delete them.

Lifecycle rules do not transition Deep Archive objects to other storage classes.

Lifecycle rules do not transition Archive objects to other storage classes.

Besides creating new lifecycle rules, you can replicate existing lifecycle rules from another bucket.

NOTE

A lifecycle rule can transition the storage class of WORM-protected object versions within the retention period, but cannot delete such object versions.

Creating a Lifecycle Rule

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the navigation pane, choose **Overview**.

Step 4 In the **Basic Configurations** area, click **Lifecycle Rules**. The **Lifecycle Rules** page is displayed.

Alternatively, you can choose **Basic Configurations** > **Lifecycle Rules** in the navigation pane.

Step 5 Click **Create**. A dialog box shown in [Figure 7-1](#) is displayed.

Figure 7-1 Creating a lifecycle rule

Step 6 Configure a lifecycle rule.

Basic Information:

- **Status:**
Select **Enable** to enable the lifecycle rule.
- **Rule Name:**
It identifies a lifecycle rule. A rule name can contain a maximum of 255 characters.
- **Prefix:** It is optional.
 - If this field is configured, objects with the specified prefix will be managed by the lifecycle rule. The prefix cannot start with a slash (/) or contain two consecutive slashes (//), and cannot contain the following special characters: \:*?"<>|
 - If this field is not configured, all objects in the bucket will be managed by the lifecycle rule.

NOTE

- If the specified prefix overlaps with the prefix of an existing lifecycle rule, OBS regards these two rules as one and forbids you to configure the one you are configuring. For example, if there is already a rule with prefix **abc** in OBS, you cannot configure another rule whose prefix starts with **abc**.
- If there is already a lifecycle rule based on an object prefix, you are not allowed to configure another rule that is applied to the entire bucket.

Current Version or Historical Version:

 NOTE

- **Current Version** and **Historical Version** are two concepts for versioning. If versioning is enabled for a bucket, uploading objects with the same name to the bucket creates different object versions. The last uploaded object is called the current version, while those previously uploaded are called historical versions. For more information, see [Versioning](#).
- You can configure either the **Current Version** or **Historical Version**, or both of them.
- **Transition to Infrequent Access After (Days)**: After this number of days since the last update, objects meeting specified conditions will be transitioned to Infrequent Access. This number must be at least 30.
- **Transition to Archive After (Days)**: After this number of days since the last update, objects meeting specified conditions will be transitioned to Archive. If you configure to transition objects first to Infrequent Access and then Archive, the objects must stay Infrequent Access at least 30 days before they can be transitioned to Archive. If transition to Archive is used, but transition to Infrequent Access is not, there is no limit on the number of days for transition.
- **Transition to Deep Archive After (Days)**: After this number of days since the last update, objects meeting specified conditions will be transitioned to Deep Archive. If you configure to transition objects first to Infrequent Access or Archive and then Deep Archive, the objects must stay Infrequent Access at least 30 days or stay Archive at least 90 days before they can be transitioned to Deep Archive. If only transition to Deep Archive is used, and transition to Infrequent Access or Archive is not, there is no limit on the number of days for transition.
- **Delete Objects After (Days)**: After this number of days since the last update, objects meeting certain conditions will be expired and then deleted. This number must be larger than that specified for any of the transition operations.
- **Delete Fragments After (Days)**: After this number of days since the fragment generation, OBS will automatically delete fragments in the bucket.

For example, on January 7, 2015, you saved the following files in OBS:

- log/test1.log
- log/test2.log
- doc/example.doc
- doc/good.txt

On January 10, 2015, you saved another four files:

- log/clientlog.log
- log/serverlog.log
- doc/work.doc
- doc/travel.txt

On January 10, 2015, you set the objects prefixed with **log** to expire one day later. You might encounter the following situations:

- Objects **log/test1.log** and **log/test2.log** uploaded on January 7, 2015 might be deleted after the last system scan. The deletion could happen on January 10, 2015 or January 11, 2015, depending on the time of the last system scan.
- Objects **log/clientlog.log** and **log/serverlog.log** uploaded on January 10, 2015 might be deleted on January 11, 2015 or January 12, 2015, depending

on whether they have been stored for over one day (since their last update) when the system scan happened.

One day, supposed you configure objects with the **log** prefix to be transitioned to Infrequent Access 30 days later, to Archive 60 days later, and then to be deleted 100 days later. OBS would perform these actions on **log/clientlog.log**, **log/serverlog.log**, **log/test1.log**, and **log/test2.log** as you defined.

 **NOTE**

In theory, it takes 24 hours at most to execute a lifecycle rule. Because OBS calculates the lifecycle of an object from the next 00:00 (UTC time) after the object is uploaded, there may be a delay in transitioning objects between storage classes and deleting expired objects. Generally, the delay does not exceed 48 hours. If you make changes to an existing lifecycle rule, the rule will take effect again.

Step 7 Click **OK** to complete the lifecycle rule configuration.

----End

Replicating Lifecycle Rules

Step 1 In the navigation pane of **OBS Console**, choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the navigation pane, choose **Overview**.

Step 4 In the **Basic Configurations** area, click **Lifecycle Rules**. The **Lifecycle Rules** page is displayed.

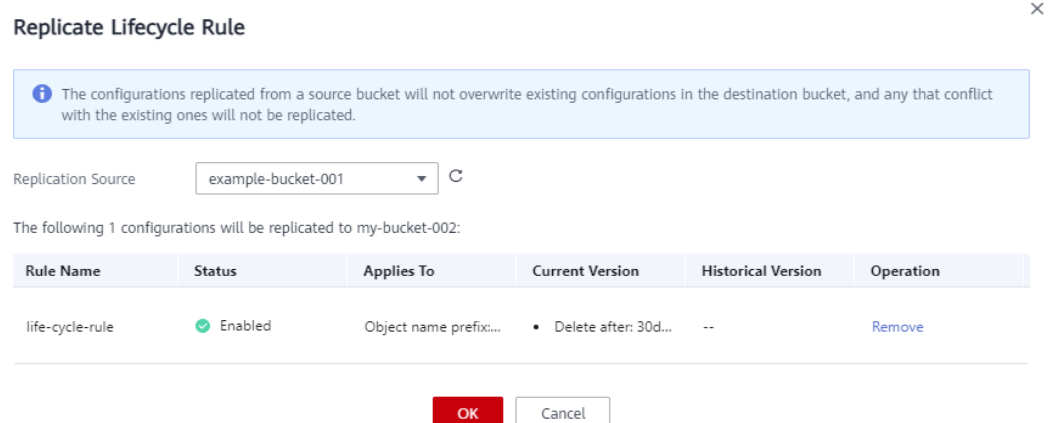
Alternatively, you can choose **Basic Configurations** > **Lifecycle Rules** in the navigation pane.

Step 5 Choose **More** > **Replicate**.

Step 6 Select a replication source, which is the bucket whose lifecycle rules you want to replicate.

 **NOTE**

- The lifecycle 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.
- Both source and destination buckets must be of the 3.0 version.
- You can remove the rules that you do not want to replicate.
- If the destination bucket does not have versioning enabled, rules related to versioning will not be replicated.

Figure 7-2 Replicating lifecycle rules

Step 7 Click **OK** to replicate the rules to the destination bucket.

----End

Follow-up Procedure

You can click **Enable**, **Edit**, or **Disable** in the **Operation** column of a lifecycle rule to enable, edit, or disable the rule.

If you want to delete more than one lifecycle rule at a time, select them and click **Delete** above the list.

7.2 Configuring Tags for a Bucket

When creating a bucket, you can add tags to it. For details, see [Creating a Bucket](#). You can also add tags to a bucket after it has been created. This section describes how to add tags to an existing bucket.

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

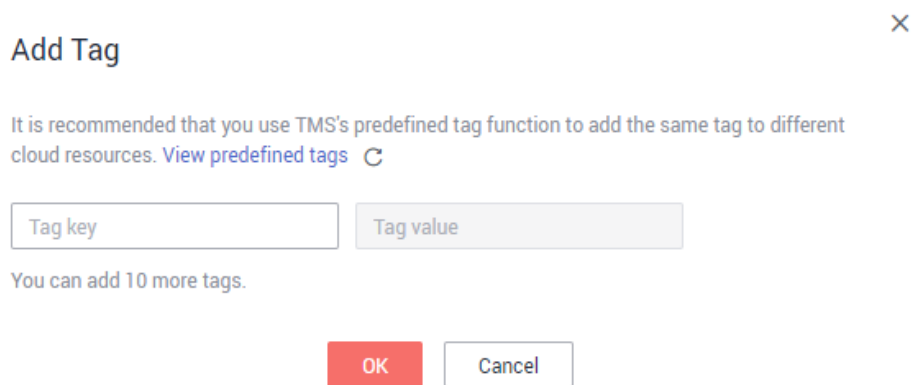
Step 3 In the navigation pane, choose **Overview**.

Step 4 In the **Basic Configurations** area, click **Tags**.

Alternatively, you can choose **Basic Configurations** > **Tagging** in the navigation pane.

Step 5 Click **Add Tag**. The **Add Tag** dialog box is displayed. See [Figure 7-3](#) for details.

Figure 7-3 Add Tag



Step 6 Set the key and value based on [Table 7-1](#).

Table 7-1 Parameter description

| Parameter | Description |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tag key | Key of a tag. Tag keys for the same bucket must be unique. You can customize tags or select the ones predefined on TMS. A tag key: <ul style="list-style-type: none"> • Must contain 1 to 36 characters and be case sensitive. • Cannot start or end with a space or contain the following characters: =*<>\, / |
| Tag value | Value of a tag. A tag value can be repetitive or left blank. A tag value: <ul style="list-style-type: none"> • Can contain 0 to 43 characters and must be case sensitive. • Cannot contain the following characters: =*<>\, / |

Step 7 Click **OK**.

It takes approximately 3 minutes for the tag to take effect.

----End

Related Operations

In the tag list, click **Edit** to change the tag value or click **Delete** to remove the tag.

7.3 Configuring a Bucket Inventory

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the navigation pane, click **Inventories**. The inventory list is displayed.

Step 4 Click **Create**. The **Create Inventory** dialog box is displayed.

Figure 7-4 Inventory settings

Step 5 Configure required parameters.

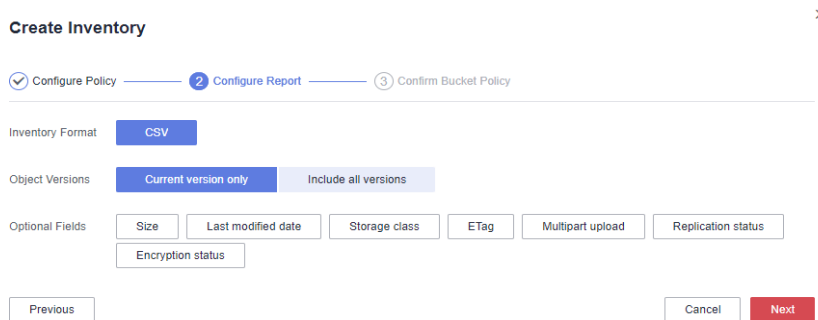
Table 7-2 Parameters for configuring a bucket inventory

| Parameter | Description |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inventory Name | Name of a bucket inventory |
| Filter | Filter of an inventory. You can enter an object name prefix for OBS to create an inventory for objects with the specified prefix. Currently, only a prefix can be used as a filter. If the filter is not specified, the inventory covers all objects in the bucket. If a bucket has multiple inventories, their filters cannot overlap with each other. |
| Save Inventory Files To | Select a bucket (destination bucket) for saving generated inventory files. This bucket must be in the same region as the source bucket. |
| Inventory File Name Prefix | Prefix of the inventory file path. An inventory file will be saved in the following path: <i>Inventory file name prefix/Source bucket name/Inventory name/Date and time/files/</i> . If this parameter is not specified, OBS automatically adds BucketInventory as the prefix to inventory file's path. |

| Parameter | Description |
|-----------|------------------------------------------------------------------------------------------------|
| Frequency | How frequently inventory files are generated. It can be set to Daily or Weekly . |
| Status | Inventory status. You can enable or disable the generation of inventories. |

Step 6 Click **Next** to go to the **Configure Report** page.

Figure 7-5 Configuring the report



Step 7 Configure the report.

Table 7-3 Report related parameters

| Parameter | Description |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inventory Format | Inventory files can only be saved in CSV format. |
| Object Versions | Object versions that you want to list in an inventory file. It can be set to Current version only or Include all versions . |
| Optional Fields | Object information fields that can be contained in an inventory file, including Size , Last modified date , Storage class , ETag , Multipart upload , Encryption status , and Replication status . For details about the fields, see Metadata in an Inventory File . |

Step 8 Click **Next** to confirm the bucket policy.

OBS then automatically creates a bucket policy on the destination bucket to grant OBS permission to write inventory files to the bucket.

Step 9 Click **OK**.

----End

7.4 Viewing Usage

On OBS Console, you can view the storage, traffic, and requests of a single bucket.

 **NOTE**

To view usage, you need to configure the `ces:metricData:list` policy in a regional project. For details, see [Cloud Eye Custom Policies](#).

Viewing Metrics

On the **Metrics** page, you can view the storage, traffic, and requests of a single bucket.

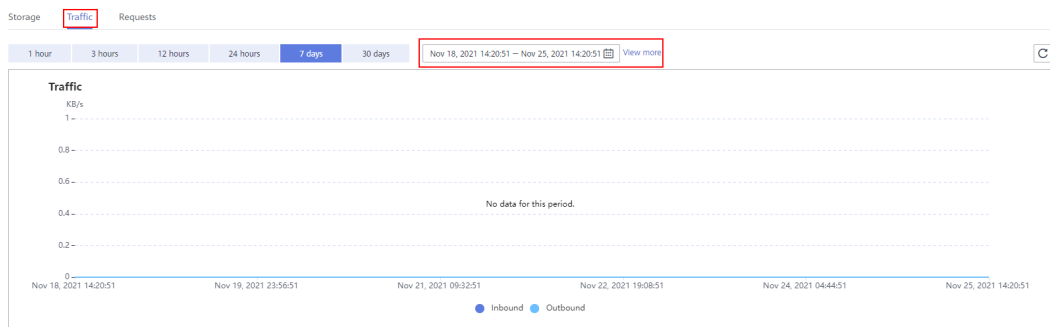
Step 1 In the navigation pane of **OBS Console**, choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the navigation pane, choose **Metrics**.

Step 4 Select a metric type and a period to view related statistics, as shown in **Figure 7-6**.

Figure 7-6 Viewing metrics



In the chart, you can:

- Choose one or more legends to display what you want to view.
- Move your mouse pointer over the statistical line to view the statistics of each item at a specific point in time.

----End

8 Data Access

8.1 Static Website Hosting

8.1.1 Configuring Static Website Hosting

You can configure static website hosting for a bucket and then use the bucket's domain name to access static websites hosted in the bucket.

The configuration of static website hosting takes two minutes at most to take effect.

 **NOTE**

In static website hosting scenarios, anonymous users must be granted access to hosted static website files. When they access the hosted files, there will be costs on outbound Internet traffic and requests.

Precautions

For security and compliance purposes, Huawei Cloud OBS prohibits the use of static website hosting based on the default OBS domain name ([a bucket domain name or static website domain name](#)). When you use such a domain name to access web pages in a browser, no content will be displayed. Instead, the content is downloaded as an attachment.

This restriction takes effect in different regions at the following two points in time:

January 1, 2022: CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, and CN South-Guangzhou

March 25, 2022: CN-Hong Kong, AP-Bangkok, AP-Singapore, AF-Johannesburg, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago

You can still use static website hosting with a user-defined domain name. This way, the content can still be previewed. For details, see [How Do I Preview Objects in OBS in a Browser Online?](#)

If you have enabled static website hosting for your OBS bucket, select the **Static website hosting** checkbox when adding a CDN domain name. In this way, the list of all files in the bucket will not be displayed when users access the bucket.

Prerequisites

Web page files required for static website hosting have been uploaded to the specified bucket.

The static website files hosted in the bucket are accessible to all users.

Static web page files in the Archive or Deep Archive storage class have been restored. For more information, see [Restoring an Object from Archive or Deep Archive Storage](#).

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 (Optional) If the static website files in the bucket are not accessible to everyone, perform this step. If they are already accessible to everyone, skip this step.

To grant required permissions, see [Granting All Accounts Read Permission for Specified Objects](#).

If the bucket contains only static website files, configure the **Object Read-Only** policy for the bucket, so that all files in it are publicly accessible.

1. Choose **Permissions > Bucket Policies**.
2. Click **Create**.
3. Configure bucket policy information.

Figure 8-1 Granting the Object Read-Only permission

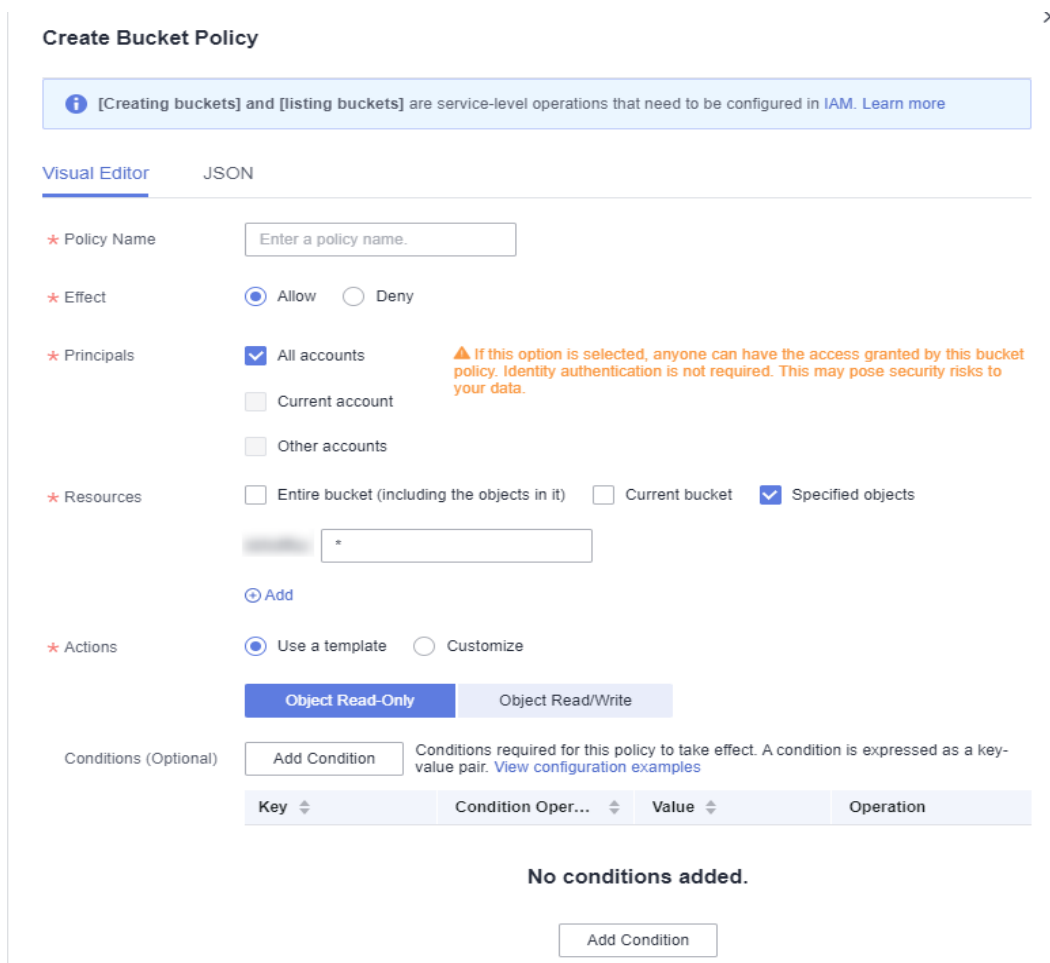


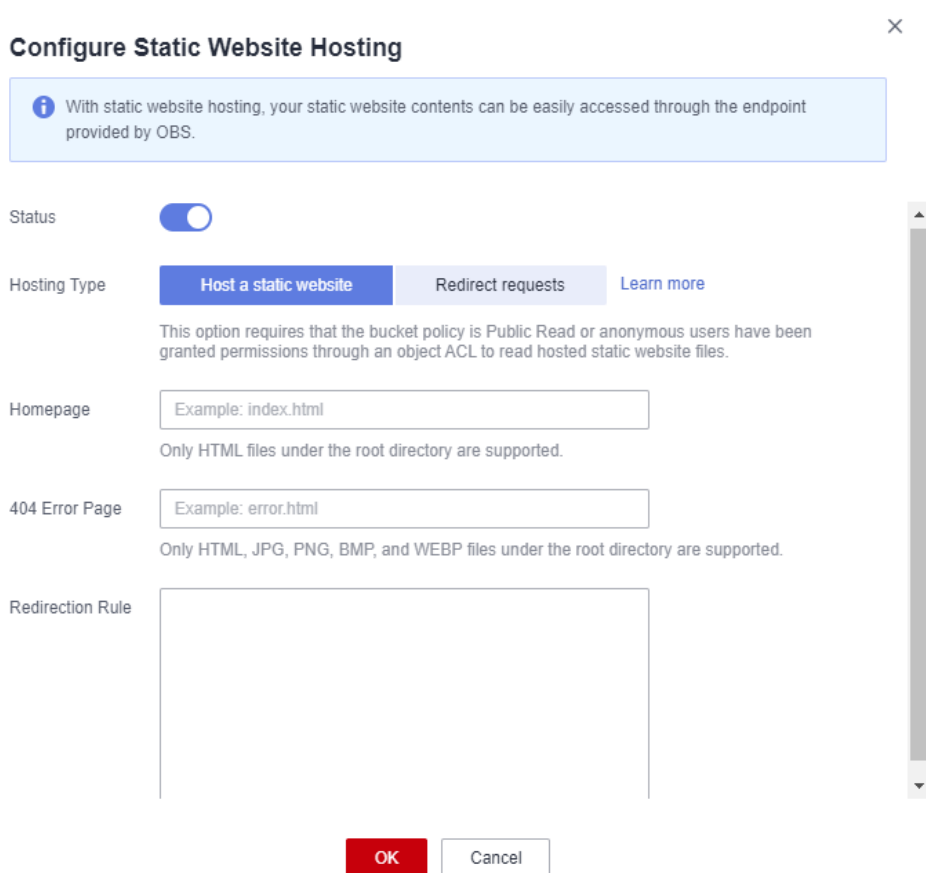
Table 8-1 Parameters for configuring a public read policy

| Parameter | | Description |
|----------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuration method | | Visual Editor and JSON are available. Choose Visual Editor here. For details, see Creating a Custom Bucket Policy (JSON View) . |
| Policy Name | | Enter a custom policy name. |
| Policy content | Effect | Select Allow . |
| | Principals | Select All accounts . |
| | Resources | <ul style="list-style-type: none"> - Select Specified objects. - Set the resource path to * (indicating all objects in the bucket). |
| | Actions | <ul style="list-style-type: none"> - Choose Use a template. - Select Object Read-Only. |

4. Click **Create**. The bucket policy is created.

- Step 4** In the navigation pane, choose **Overview**.
- Step 5** In the **Basic Configurations** area, click **Static Website Hosting**. The **Static Website Hosting** page is displayed.
- Alternatively, you can choose **Basic Configurations > Static Website Hosting** from the navigation pane on the left.
- Step 6** Click **Configure Static Website Hosting**. The **Configure Static Website Hosting** dialog box is displayed.
- Step 7** Enable **Status**.
- Step 8** Set the hosting type to the current bucket. For details, see [Figure 8-2](#).

Figure 8-2 Configuring static website hosting



- Step 9** Configure the homepage and 404 error page.
- Homepage:** specifies the default homepage of the static website. When OBS Console is used to configure static website hosting, only HTML web pages are supported. When APIs are used to configure static website hosting, OBS does not have any restriction but the **Content-Type** of objects must be specified. OBS only allows files such as **index.html** in the root directory of a bucket to function as the default homepage. Do not set the default homepage with a multi-level directory structure (for example, **/page/index.html**).

- 404 Error Page:** specifies the error page returned when an error occurs during static website access. When OBS Console is used to configure static website hosting, only HTML, JPG, PNG, BMP, and WebP files under the root directory are supported. When APIs are used to configure static website hosting, OBS does not have any restriction but the **Content-Type** of objects must be specified.

Step 10 Optional: In **Redirection Rules**, configure redirection rules. Requests that comply with the redirection rules are redirected to the specific host or page.

A redirection rule is compiled in the JSON or XML format. Each rule contains a **Condition** and a **Redirect**. The parameters are described in [Table 8-2](#).

Table 8-2 Parameter description

| Container | Key | Description |
|-----------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Condition | KeyPrefixEquals | Object name prefix on which the redirection rule takes effect. When a request is sent for accessing an object, the redirection rule takes effect if the object name prefix matches the value specified for this parameter. For example, to redirect the request for object ExamplePage.html , set the KeyPrefixEquals to ExamplePage.html . |
| | HttpErrorCodeReturnedEquals | HTTP error codes upon which the redirection rule takes effect. The specified redirection is applied only when the error code returned equals the value specified for this parameter. For example, if you want to redirect requests to NotFound.html when HTTP error code 404 is returned, set HttpErrorCodeReturnedEquals to 404 in Condition , and set ReplaceKeyWith to NotFound.html in Redirect . |
| Redirect | Protocol | Protocol used for redirecting requests. The value can be http or https . If this parameter is not specified, the default value http is used. |
| | HostName | Host name to which the redirection is pointed. If this parameter is not specified, the request is redirected to the host from which the original request is initiated. |

| Container | Key | Description |
|-----------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | ReplaceKeyPrefix- With | The object name prefix used in the redirection request. OBS replaces the value of KeyPrefixEquals with the value you specified here for ReplaceKeyPrefixWith . For example, to redirect requests for docs (objects in the docs directory) to documents (objects in the documents directory), set KeyPrefixEquals to docs under Condition and ReplaceKeyPrefix- With to documents under Redirect . This way, requests for object docs/a.html will be redirected to documents/a.html . |
| | ReplaceKeyWith | The object name used in the redirection request. OBS replaces the entire object name in the request with the value you specified here for ReplaceKeyWith . For example, to redirect requests for all objects in the docs directory to documents/error.html , set KeyPrefixEquals to docs under Condition and ReplaceKeyWith to documents/ error.html under Redirect . This way, requests for both objects docs/a.html and docs/b.html will be redirected to documents/error.html . |
| | HttpRedirectCode | HTTP status code returned to the redirection request. The default value is 301 , indicating that requests are permanently redirected to the location specified by Redirect . You can also set this parameter based on your service needs. |

Example of setting a redirection rule

- Example 1: All requests for objects prefixed with **folder1/** are automatically redirected to pages prefixed with **target.html** on host **www.example.com** using HTTPS.

```
[
  {
    "Condition": {
      "KeyPrefixEquals": "folder1/"
    },
    "Redirect": {
      "Protocol": "https",
      "HostName": "www.example.com",
      "ReplaceKeyPrefixWith": "target.html"
    }
  }
]
```

- Example 2: All requests for objects prefixed with **folder2/** are automatically redirected to objects prefixed with **folder/** in the same bucket.

```
[
  {
    "Condition": {
      "KeyPrefixEquals": "folder2/"
    },
    "Redirect": {
      "ReplaceKeyPrefixWith": "folder/"
    }
  }
]
```

- Example 3: All requests for objects prefixed with **folder.html** are automatically redirected to the **folderdeleted.html** object in the same bucket.

```
[
  {
    "Condition": {
      "KeyPrefixEquals": "folder.html"
    },
    "Redirect": {
      "ReplaceKeyWith": "folderdeleted.html"
    }
  }
]
```

- Example 4: If the HTTP status code 404 is returned, the request is automatically redirected to the page prefixed with **report-404/** on 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/"
    }
  }
]
```

Step 11 Click OK.

After the static website hosting is effective in OBS, you can access the static website by using the URL provided by OBS.

NOTE

In some conditions, you may need to clear the browser cache before the expected results are displayed.

----End

8.1.2 Configuring Redirection

You can redirect all requests for a bucket to another bucket or URL by configuring redirection rules.

Prerequisites

Web page files required for static website hosting have been uploaded to the specified bucket.

The static website files hosted in the bucket are accessible to all users.

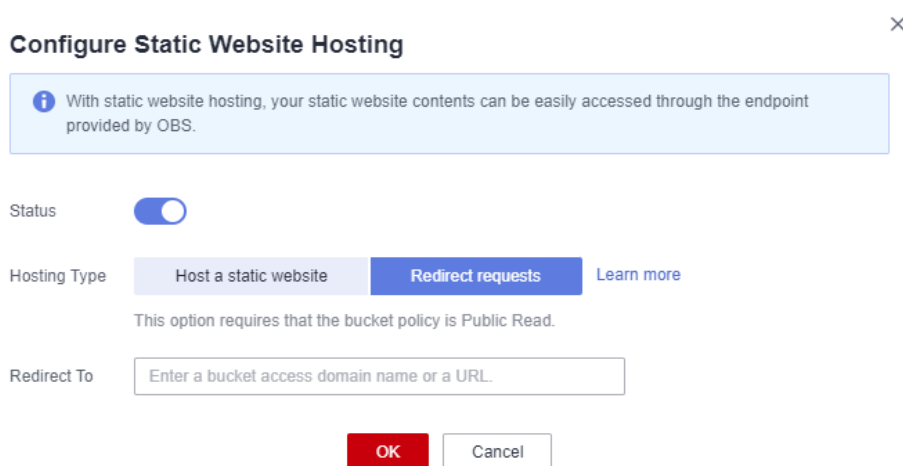
Static web page files in the Archive or Deep Archive storage class have been restored. For more information, see [Restoring an Object from Archive or Deep Archive Storage](#).

Procedure

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the navigation pane, choose **Overview**.
- Step 4** In the **Basic Configurations** area, click **Static Website Hosting**. The **Static Website Hosting** page is displayed.

Alternatively, you can choose **Basic Configurations > Static Website Hosting** from the navigation pane on the left.
- Step 5** Click **Configure Static Website Hosting**. The **Configure Static Website Hosting** dialog box is displayed.
- Step 6** Enable **Status**.
- Step 7** Set **Hosting Type** to **Redirect requests**, as shown in [Figure 8-3](#). In the text box of **Redirect To**, enter the bucket's access domain name or URL.

Figure 8-3 Configuring redirection



- Step 8** Click **OK**.
- Step 9** In the bucket list, click the bucket to which requests for the static website are redirected.
- Step 10 (Optional)** If the static website files in the bucket are not accessible to everyone, perform this step. If they are already accessible to everyone, skip this step.

To grant required permissions, see [Granting All Accounts Read Permission for Specified Objects](#).

If the bucket contains only static website files, configure the **Object Read-Only** policy for the bucket, so that all files in it are publicly accessible.

1. Choose **Permissions > Bucket Policies**.
2. Click **Create**.
3. Configure bucket policy information.

Figure 8-4 Granting the Object Read-Only permission

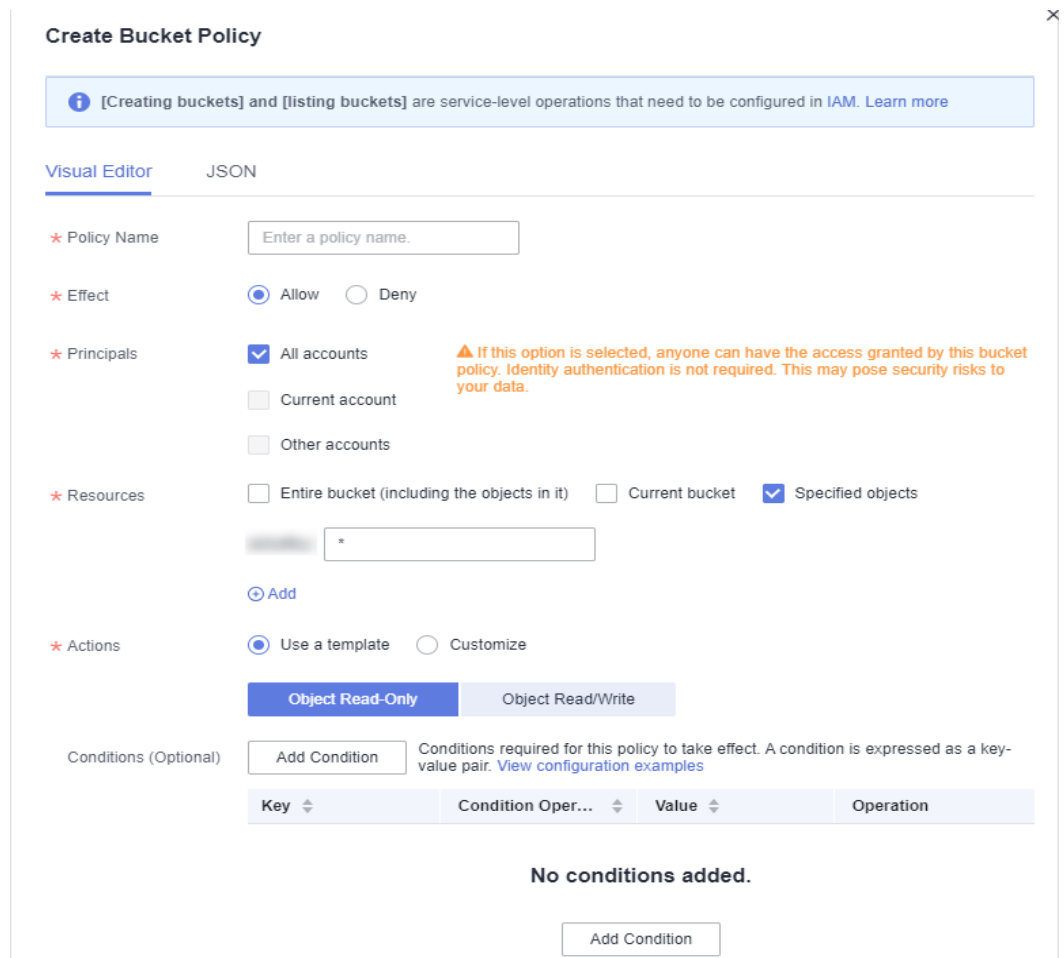


Table 8-3 Parameters for configuring a public read policy

| Parameter | | Description |
|----------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuration method | | Visual Editor and JSON are available. Choose Visual Editor here. For details, see Creating a Custom Bucket Policy (JSON View) . |
| Policy Name | | Enter a custom policy name. |
| Policy content | Effect | Select Allow . |
| | Principals | Select All accounts . |

| Parameter | | Description |
|-----------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Resources | <ul style="list-style-type: none">- Select Specified objects.- Set the resource path to * (indicating all objects in the bucket). |
| | Actions | <ul style="list-style-type: none">- Choose Use a template.- Select Object Read-Only. |

4. Click **Create**. The bucket policy is created.

Step 11 Verification: Input the access domain name of the bucket in the web browser and press **Enter**. The bucket or URL to which requests are redirected will be displayed.

 **NOTE**

In some conditions, you may need to clear the browser cache before the expected results are displayed.

----End

8.2 Configuring a Back-to-Source Rule

Scenarios

See [Back to Source](#).

You can create back-to-source rules or replicate existing back-to-source rules from another bucket.

Constraints

See [Back to Source](#).

Creating a Mirroring Back-to-Source Rule

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the navigation pane, choose **Back to Source**. The back-to-source rule list is displayed.

Step 4 Click **Create**.

Figure 8-5 Creating a mirroring back-to-source rule

Step 5 Configure a mirroring back-to-source rule by referring to the parameters listed in [Table 8-4](#).

Table 8-4 Parameters in a mirroring back-to-source rule

| Parameter | Description |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resource Type | Type of the resources at the source site (origin server). <ul style="list-style-type: none"> • Public: The origin server data comes from public object storage. • Private: The origin server data comes from private object storage of some cloud vendors. |
| Back-to-Source Condition | <p>Conditions that trigger the back-to-source rule.</p> <p>A mirroring back-to-source rule is triggered when the following conditions are met: The requested object starts with the specified file name prefix, and an HTTP status code 404 is returned because the object is not found in the bucket.</p> <p>The specified file name prefix:</p> <ul style="list-style-type: none"> • Cannot exceed 1,023 characters. • Cannot contain or overlap with any other file name prefix specified for an existing rule. • Can be left blank, which means that the rule applies to all files that do not meet the conditions of other back-to-source rules configured for the bucket. A bucket can have only one back-to-source rule that does not have a file name prefix specified. <p>For example, if the file name prefix is set to 123/, the rule is triggered when the 123/456.txt file is requested but not available in the bucket.</p> |

| Parameter | Description |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add Prefix or Suffix | <p>When OBS requests data from the source site, the prefix or suffix is added in front of or after the name of the requested object. However, the object returned to OBS and the client keeps its original name without the added prefix or suffix.</p> <p>Example: A client requests abc.txt from OBS, which triggers the back-to-source rule. If the specified prefix is 123, OBS then retrieves 123abc.txt from the source site. However, the object is still downloaded as abc.txt to OBS and then returned to the client.</p> |
| Replace Prefix With | <p>OBS uses the specified prefix to replace the file name prefix set in the back-to-source condition when it requests data from the source site. However, the object returned to the client keeps the original prefix in its name.</p> <p>Example: The file name prefix is set to 123 as the back-to-source condition and the replacement prefix is set to abc. When the client requests 123456.txt, the back-to-source rule is triggered. Then OBS requests abc456.txt from the source site. However, the obtained object is still saved as 123456.txt in OBS and returned to the client.</p> |
| Source URL | <p>Source site address. You can set active sites and standby sites.</p> <p>The active site address is preferentially used during the back-to-source process. If multiple active site addresses are configured, all active sites are accessed in polling mode. If two or more active site addresses are configured, when the first request to an active address fails and the retry conditions are met, the request will retry another active site address. Configure at least one active site. Up to five active sites are supported. If you fail to retrieve content from all active sites, the request will try standby sites.</p> <p>Format: <i>http(https)://source domain name/static path</i></p> <ul style="list-style-type: none"> • The source domain name is the domain name of the source site. <ul style="list-style-type: none"> - If the source site is a bucket that can be accessed over HTTP, the address is the bucket domain name. - If the source site is a private bucket provided by other cloud vendors, the address is the region domain name. At present, only private buckets of some cloud vendors are supported. • The static path indicates the directory that stores the target file. For example, if the static path is 123/, the target file is in the 123/ directory. |

| Parameter | Description |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Retry Condition | Condition when a retry is triggered. 4XX and a specific error code starting with 4 cannot be configured together. This rule works the same for 5XX and an error code starting with 5 . A maximum of 20 error codes can be configured. |
| Carry Request String | When this function is enabled, query parameters in the request URL are passed to the source site. |
| Redirect Request | When this function is enabled, the request will follow the 3xx redirection response, if redirection is configured for the source site, to fetch the requested resource and save the resource to OBS. A request can follow a maximum of 10 redirections. |
| Redirect without Referer | With this function enabled, if redirection has been configured for the origin server, the Referer header in the request will be filtered out during redirecting. |
| HTTP Header Pass Rule | You can specify the HTTP header parameters that can be passed to the source site when a request sent to OBS triggers the mirroring back-to-source rule. References provides a configuration example and lists the HTTP headers that are not supported. <ul style="list-style-type: none">• Pass all parameters/Pass specified parameters: Set the HTTP header parameters that can be passed.• Do not pass specified parameters: Set the HTTP header parameters that cannot be passed. In this case, OBS does not pass the specified headers to the source site. If a header is specified for both the pass and do-not-pass categories, it is deemed as a do-not-pass parameter.• Configure custom parameters: You can set a custom value for a specified header. If a client request carries this header, OBS changes the header value to the custom value before passing it to the source site. |
| IAM Agency | An IAM agency is required to delegate OBS to obtain data from the source site. The agency must grant OBS the Tenant Administrator permission, with an unlimited validity period. If no appropriate IAM agency is available, create one by referring to Creating an IAM Agency . |

Step 6 Click **OK**.

----End

Replicating Mirroring Back-to-Source Rules

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the navigation pane, choose **Back to Source**. The back-to-source rule list is displayed.

Step 4 Click **Replicate**.


Step 5 Select a replication source, which is bucket whose back-to-source rules you want to replicate.

 **NOTE**

- The back-to-source 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.
- Both source and destination buckets must be of the 3.0 version.
- Before replicating the back-to-source rules, you can change their source URL. For details about the source URL configuration, see [Table 8-4](#).
- You can remove the rules that you do not want to replicate.
- There can be five back-to-source rules at most in a bucket. If the number of rules you will replicate plus the number of existing rules in the destination bucket exceeds five, the replication will fail. Before replicating the rules, delete some if necessary.

Figure 8-6 Replicating back-to-source rules

Replicate Back-to-Source Rule ×

 The configurations replicated from a source bucket will not overwrite existing configurations in the destination bucket, and any that conflict with the existing ones will not be replicated.

Replication Source ↕

The following 1 configurations will be replicated to my-bucket-002:

| Back to the Source By | Back-to-Source Condition | Source URL | Operation |
|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|------------------------|
| <ul style="list-style-type: none">• Back to the Source By: ...• Resource Type: Public | <ul style="list-style-type: none">• HTTP status code: 404• File Name Prefix: 123/ | Active Site <input type="text" value="http"/> <input type="text" value="://example.com"/> | Remove |

Step 6 Click **OK** to replicate the rules to the destination bucket.

----End

References

Example for configuring an HTTP header pass rule:

Assume that the parameters are set as shown in [Figure 8-7](#).

Figure 8-7 Configuring an HTTP header pass rule

HTTP Header Pass Rule

Pass all parameters

Pass specified parameters

aaa Add

You can add 9 more parameters.

Do not pass specified parameters

bbb Add

You can add 9 more parameters.

Configure custom parameters

ccc : 111 Add

You can add 9 more parameters.

Based on the preceding configuration, if the header of the request sent to OBS is as follows:

```
GET /ObjectName HTTP/1.1
Host: bucketname.obs.region.myhuaweicloud.com
aaa:aaa
bbb:bbb
ccc:ccc
```

OBS sends the following request to the source site when the back-to-source rule is triggered:

```
GET /ObjectName HTTP/1.1
Host: source.com
aaa:aaa
ccc:111
```

Notes for passing HTTP headers during back to source

- HTTP headers that can be passed from a source site to a client:
 - Content-Type
 - Content-Language
 - Content-Encoding
 - Content-Disposition
 - Cache-Control
 - Expires
- HTTP headers that cannot be passed from a client to a source site:
 - a. HTTP headers starting with the prefix below:
 - x-obs-
 - b. All standard HTTP headers, including:
 - Content-Length
 - Authorization2
 - Authorization

- Range
- Date

8.3 Configuring a User-Defined Domain Name

Prerequisites

As required by the MIIT, you must complete the ICP filing, if the bucket which your domain name is bound to is in any of the following regions:

CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, and CN South-Guangzhou

You have created a bucket and uploaded your website file to it.

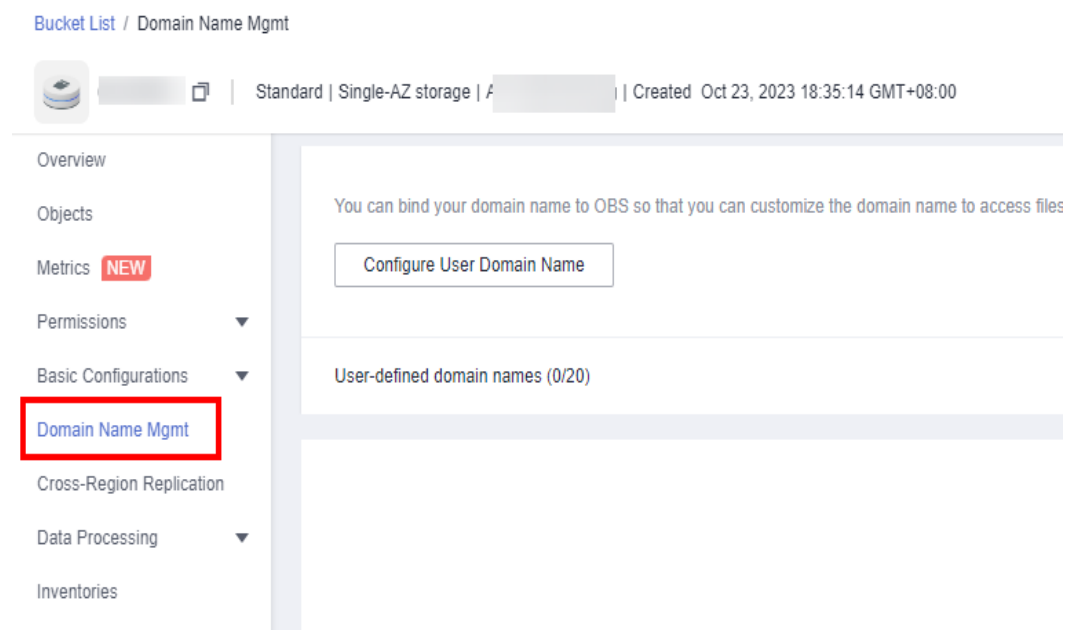
NOTE

If an acceleration domain name is also needed, to prevent objects in OBS buckets from being directly downloaded upon access, you need to perform other required operations after the custom domain name and the acceleration domain name have been configured. For details, see [With CDN Acceleration Enabled, Why Are the Objects in My OBS Bucket Directly Downloaded When I Access Them?](#)

Procedure

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the navigation pane, choose **Domain Name Mgmt**.

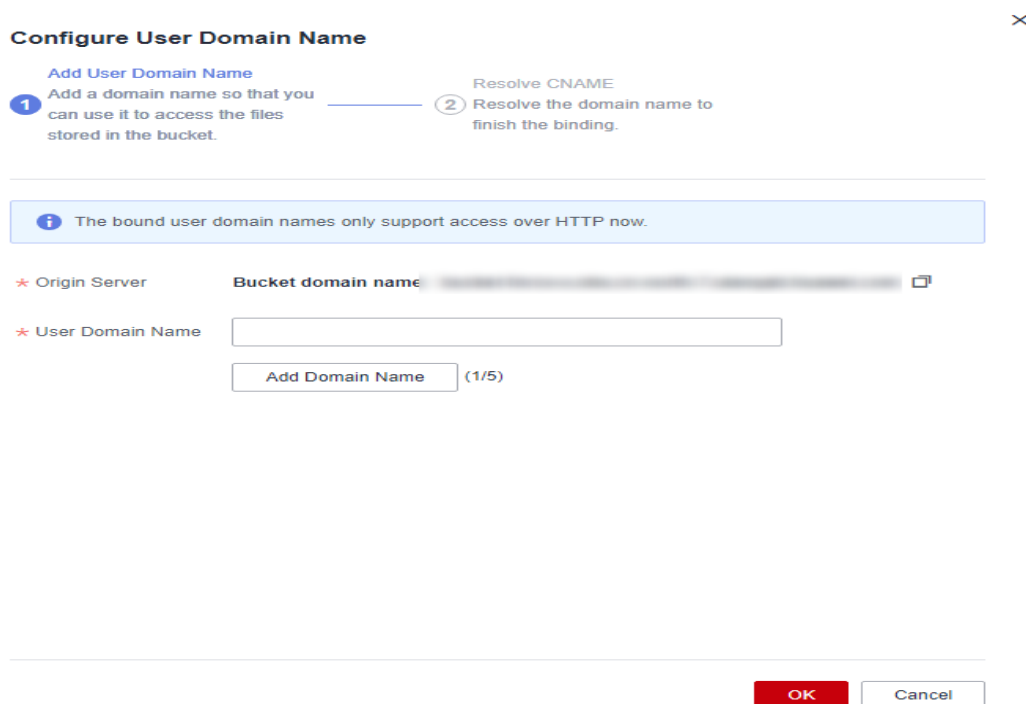
Figure 8-8 Domain name management page



Step 4 Click **Configure User Domain Name** in the upper part of the page. Alternatively, click **Configure User Domain Name** in the lower card area of the page when no user-defined domain names are available. In the displayed dialog box, enter the domain name to configure, as shown in [Figure 8-9](#). If you want to choose one of the existing Huawei Cloud domain names from the drop-down list on OBS Console, you must have the **Domains:domains:getDetails** permission. You can contact the administrator to use IAM to grant you this permission. If you do not have this permission, you can only manually type a domain name.

The suffix of a user-defined domain name can contain 2 to 6 uppercase or lowercase letters.

Figure 8-9 Configuring a user domain name



Step 5 Click **OK**.

Step 6 Based on the tips, click **Resolve** or manually add a CNAME record set. Then, click **OK**.

NOTE

Clicking **Resolve** will automatically add CNAME record sets for Huawei Cloud domain names. To resolve those domain names not registered with Huawei Cloud, you need to configure resolution rules by yourself.

Step 7 Configure a CNAME record on the DNS, and map the user-defined domain name (for example, **example.com**) to the domain name of the bucket.

The CNAME configuration varies depending on DNS providers. If you are using a DNS provider rather than Huawei Cloud, configure CNAME records by referring to [Configuring a CNAME Record](#).

If your DNS service is provided by Huawei Cloud, perform the following steps to configure a CNAME record:

1. Log in to the Huawei Cloud console. On the homepage, choose **Networking** > **Domain Name Service**. The DNS console is displayed.
2. In the navigation pane, choose **Public Zones**. The domain name list page is displayed.
3. Click the domain name which you want to add a record set to.
4. Choose the **Record Sets** tab and click **Add Record Set**.
5. Configure the parameters based on [Table 8-5](#). Retain the default values for those not listed in the table below.

Table 8-5 Parameters for adding a record set

| Parameter | Description | Example Value |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Prefix of the domain name | www |
| Type | Type of the record set, which should be a CNAME-Canonical name here. | CNAME – Map one domain to another |
| Line | Resolution line. The DNS server will return the IP address of the specified line, depending on where the visitor comes from. You must add a Default line to ensure that the website is accessible to anyone. | Default |
| TTL (s) | Cache duration of the record set, in seconds | The default interval is 5 min (300 seconds). |
| Value | Domain name to be pointed to | <ul style="list-style-type: none">– If CDN acceleration is not used, set this parameter to the bucket domain name.– If CDN acceleration is used, set this parameter to the CNAME record allocated by CDN. |

6. Click **OK**.
7. Check whether the CNAME configuration takes effect.
Open the Windows command line interface and run the following command:

```
nslookup -qt=cname User-defined domain name bound to the bucket
```

 - Without CDN acceleration: If the output is the bucket domain name, the CNAME configuration has taken effect.

- With CDN acceleration: If the output is the CNAME record allocated by CDN, the CNAME configuration has taken effect.

----End

9 Data Security

9.1 Configuring Server-Side Encryption

9.1.1 Configuring Bucket Default Encryption

OBS allows you to configure default encryption for a bucket. After the default encryption is enabled for the bucket, objects uploaded to this bucket are automatically encrypted using the specified key, making data storage more secure.

You can enable the default encryption (by choosing SSE-KMS or SSE-OBS) when creating a bucket (see [Creating a Bucket](#)), or enable or disable default encryption after the bucket is created.

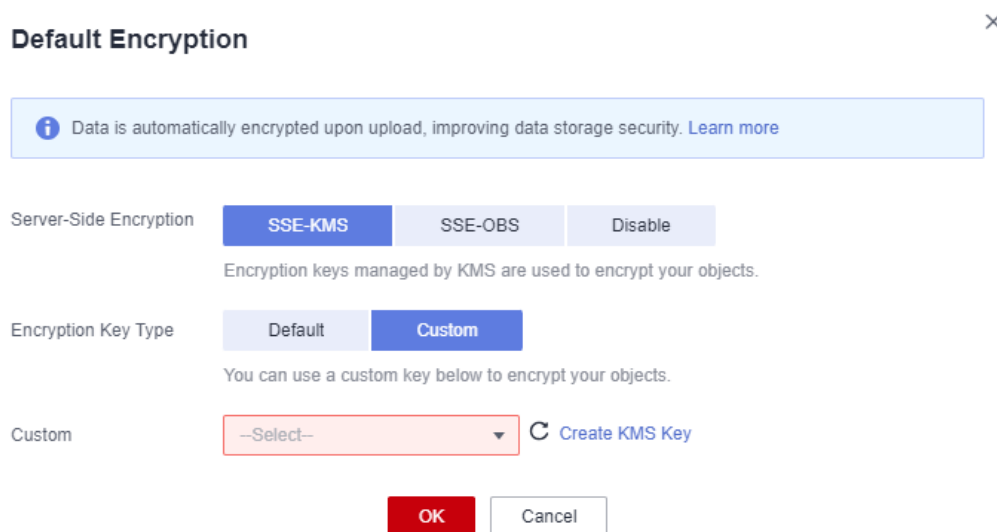
OBS only encrypts the objects uploaded after the default encryption is enabled for the bucket, and does not encrypt those uploaded before. After you disable a bucket's default encryption, the encryption status of existing objects keeps unchanged, and you can separately encrypt objects when uploading them to the bucket.

Enabling Default Encryption for a Bucket

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the navigation pane, choose **Overview**.
- Step 4** In the **Basic Configurations** area, click **Default Encryption**. The **Default Encryption** dialog box is displayed.
- Step 5** Choose **SSE-KMS** or **SSE-OBS**.

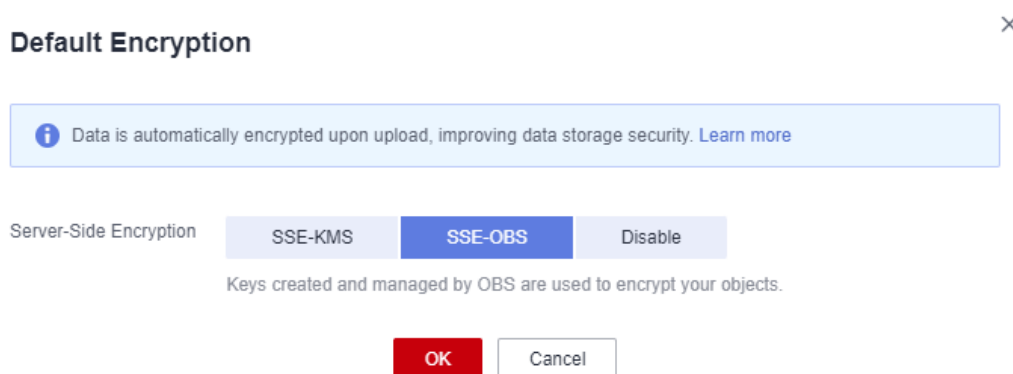
If you choose **SSE-KMS** for encryption, you must specify an encryption key type (**Default** or **Custom**). If **Default** is used, the default key of the current region will be used to encrypt your objects. If there is no such a default key, OBS creates one the first time you upload an object. If **Custom** is used, you can choose a custom key you created on the KMS console to encrypt your objects.

Figure 9-1 Choosing SSE-KMS for a bucket



When **SSE-OBS** is chosen, the keys created and managed by OBS are used for encryption.

Figure 9-2 Choosing SSE-OBS for a bucket



Step 6 Click **OK**.

----End

Disabling Default Encryption for a Bucket

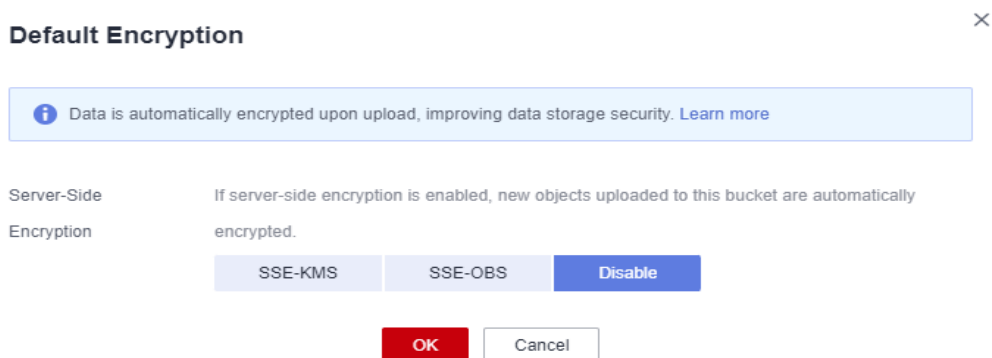
Step 1 In the navigation pane of **OBS Console**, choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the navigation pane, choose **Overview**.

Step 4 In the **Basic Configurations** area, click **Default Encryption**. The **Default Encryption** dialog box is displayed.

Step 5 Select **Disable**.

Figure 9-3 Disabling encryption for a bucket

Step 6 Click **OK**.

----End

9.1.2 Uploading an Object in Server-Side Encryption Mode

OBS allows you to encrypt objects with server-side encryption so that the objects can be securely stored in OBS.

In a bucket with server-side encryption disabled, objects uploaded to it are not encrypted by default, but you can configure server-side encryption for the objects when uploading them. In a bucket with server-side encryption enabled, objects uploaded to it can inherit the encryption settings of the bucket, and you can also separately configure encryption for the objects.

Constraints

- The object encryption status cannot be changed.
- A key in use cannot be deleted. Otherwise, the object encrypted with this key cannot be downloaded.
- If an object is server-side encrypted and does not have any IAM agency, other accounts and users cannot access the object even if they can read this object.

Prerequisites

In the region where OBS is deployed, the **KMS Administrator** permission has been added to the user group. For details about how to add the permission, see [Assigning Permissions to an IAM User](#). If the current account or user is the grantee, it also requires the **KMS Administrator** permission.

For details about DEW pricing, see the [Product Pricing Details](#).

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 Click **Upload Object**. The **Upload Object** dialog box is displayed.

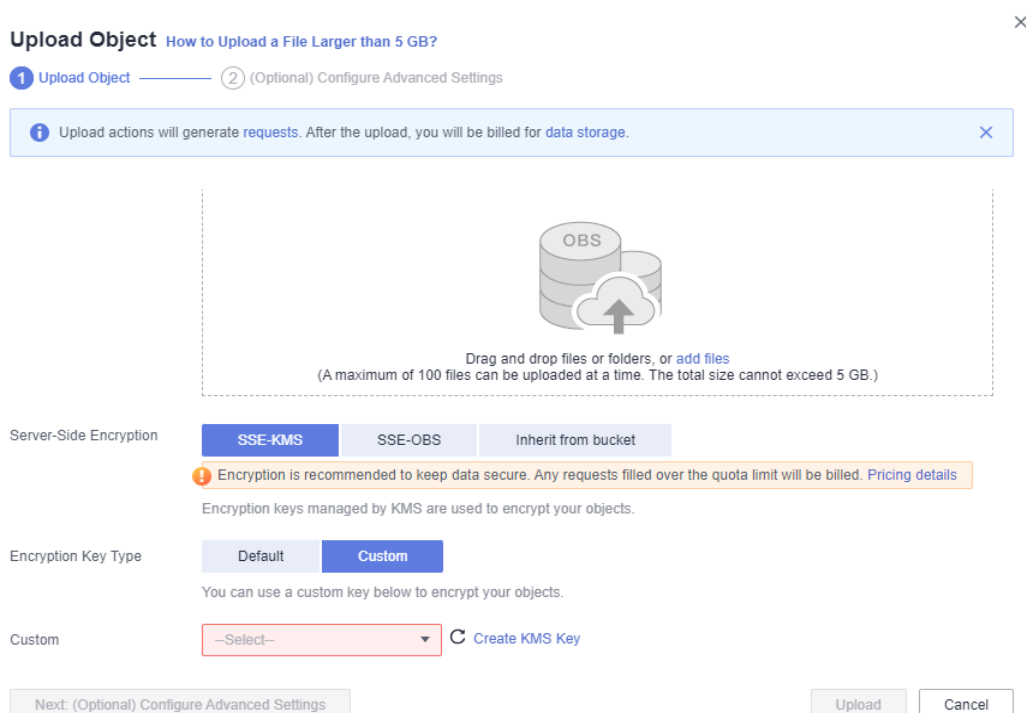
Step 4 Add the files to be uploaded.

Step 5 Select **SSE-KMS** or **SSE-OBS**.

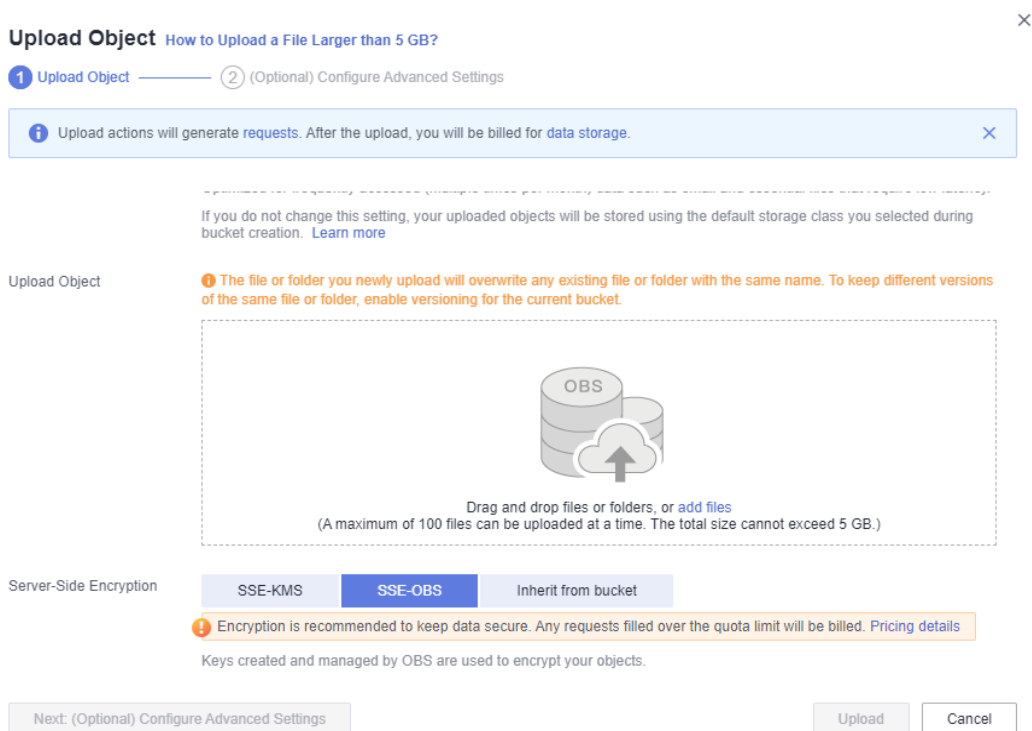
If you choose **SSE-KMS** for encryption, you must specify an encryption key type (**Default** or **Custom**). If **Default** is used, the default key of the current region will be used to encrypt your objects. If there is no such a default key, OBS creates one the first time you upload an object. If **Custom** is used, you can choose a custom key you created on the KMS console to encrypt your objects.

For details, see [Creating a Key](#).

Figure 9-4 Choosing **SSE-KMS** for server-side encryption



When **SSE-OBS** is chosen, the keys created and managed by OBS are used for encryption.

Figure 9-5 Choosing SSE-OBS for server-side encryption**Step 6** Click **Upload**.

After the object is uploaded, you can view its encryption status on its details page.

----End

9.2 Configuring WORM Retention

You can configure WORM retention policies when creating a bucket (see [Creating a Bucket](#)) or after a bucket is created. The following describes how to configure WORM retention after you create a bucket with WORM enabled.

Prerequisites

You have enabled WORM for the bucket when you create it.

Configuring WORM for a Bucket

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the navigation pane, choose **Overview**.

Step 4 In the **Basic Configurations** area, click **WORM Retention**. The **Configure WORM Retention** dialog box is displayed.

Step 5 Choose **Configure** and specify a default retention period. The default retention mode is **Compliance**.

NOTE

- Only the compliance retention mode is currently supported. In this mode, no users can delete protected object versions or change their retention mode during the specified retention period.
- During the specified default retention period, OBS prevents WORM-protected object versions from being deleted. You can configure a retention period in either days (from 1 to 36500) or years (from 1 to 100). The upper limit is 100 years.
- When you upload an object to a WORM-protected bucket, you can configure the object to inherit the WORM retention from the bucket under advanced settings. If both a bucket-level and object-level WORM retention policy are applied to an object, the object-level retention policy will be used.

Figure 9-6 Configuring a WORM retention policy

Configure WORM Retention ×

Default Retention

Protects object versions newly uploaded to the current bucket from being deleted during the retention period.

Default Retention Mode

No users can delete protected object versions or change their retention mode during the retention period.

Default Retention Period

During the specified period, OBS prevents WORM-protected object versions from being deleted.

Step 6 Click **OK**.

----End

Skipping the WORM Retention Configuration

Step 1 In the navigation pane of **OBS Console**, choose **Object Storage**.

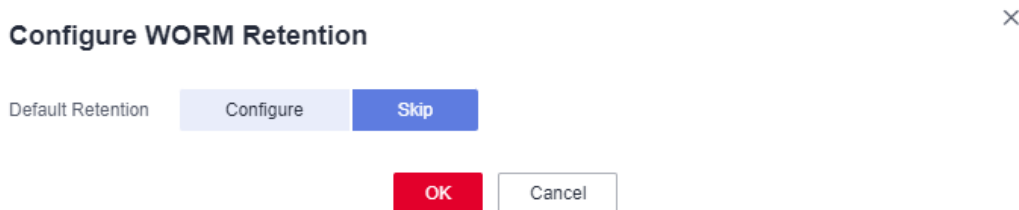
Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the navigation pane, choose **Overview**.

Step 4 In the **Basic Configurations** area, click **WORM Retention**. The **Configure WORM Retention** dialog box is displayed.

Step 5 Choose **Skip**.

Figure 9-7 Skipping the WORM retention configuration



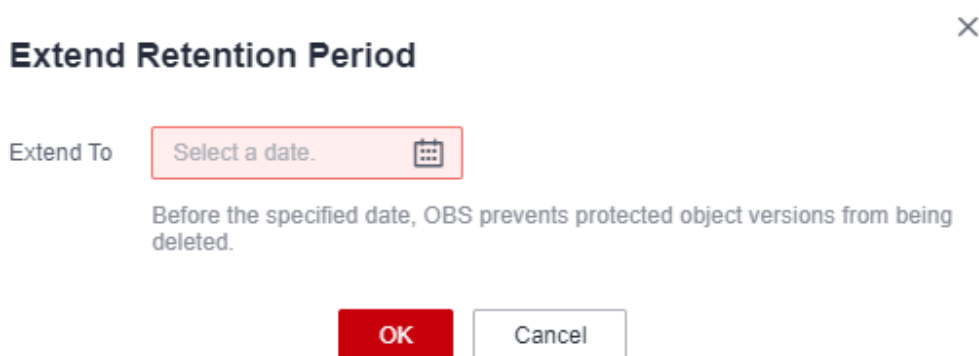
----End

Extending the Retention Period

After WORM is configured for an object, you can go to the object details page and extend the retention period of an object version on the **Versions** page. Before the specified date, OBS prevents protected object versions from being deleted.

- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the object list, click the object you want to go to the object details page.
- Step 4** On the **Versions** tab page, view all versions of the object.
- Step 5** Locate the object version for which you want to extend the retention period, choose **More > Extend Retention Period**, and select a date.

Figure 9-8 Extending the retention period



NOTE

A retention period can only be extended, but not shortened.

Assume that an object version was configured to be protected until March 30, 2023. If you want to extend the retention period on March 1, 2023, you can extend it to March 31, 2023 or a later date. If you extend the retention period on April 1, 2023, you can extend it to the current day (April 1, 2023) or a later date. If the current day is used, the object version will no longer be protected by WORM after 24:00 on that day.

----End

Manually and Permanently Deleting Objects from a WORM-Enabled Bucket

In the **Deleted Objects** list, objects cannot be permanently deleted from a WORM-enabled bucket. In a WORM-enabled bucket, if an object has no retention policy configured or its retention policy has expired, you can delete a desired object version on the object's **Versions** tab page. If an object version is within the retention period, it cannot be deleted.

- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the object list, click the object you want to go to the object details page.
- Step 4** On the **Versions** tab page, view all versions of the object.
- Step 5** Find the object's current version and choose **More > Extend Retention Period** to check its retention status.

NOTE

If the object version is within the retention period, you will see a message indicating the remaining retention days.

If the retention for the object version has expired, you will see a message indicating the retention expiration days.

If the object version has no retention policy configured, you will not see a message indicating the retention status.

Figure 9-9 Object version within the WORM retention period

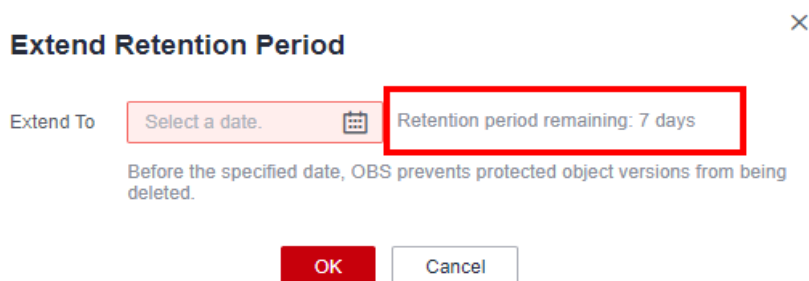


Figure 9-10 Object version whose WORM retention has expired

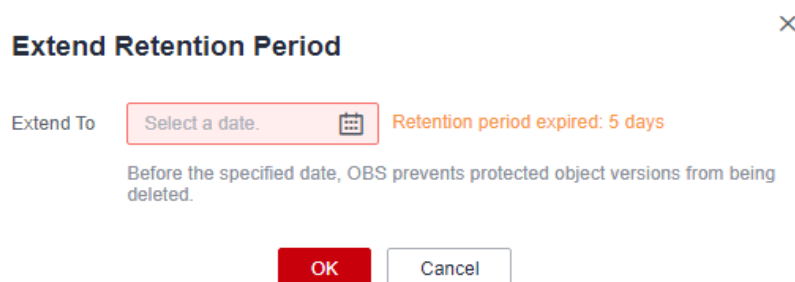
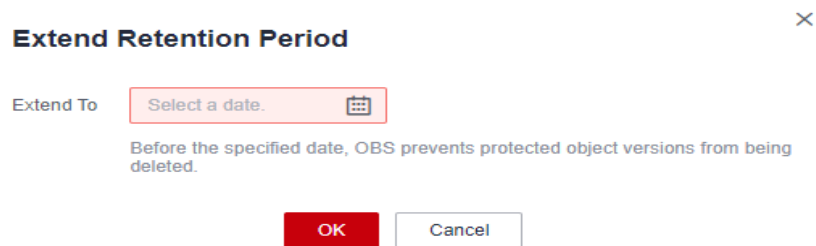


Figure 9-11 Object version with no WORM retention policy



- Step 6** Confirm that the current object version is out of the retention period or has no retention policy configured, and choose **More > Delete**.
- Step 7** Verify that the object is no longer displayed in the **Deleted Objects** list after all object versions are deleted.

----End

Using a Lifecycle Rule to Delete Objects from a WORM-Enabled Bucket

You can configure a lifecycle rule to let OBS automatically expire and delete objects in a WORM enabled bucket. To realize this, the objects must have no retention policies configured or their retention policies have expired. If the objects are within their retention period, they cannot be deleted.

NOTE

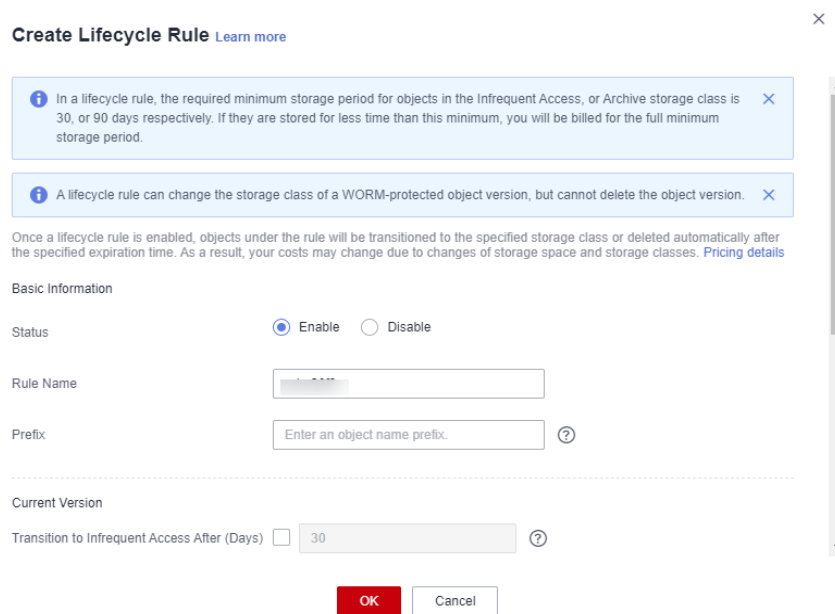
In a WORM-enabled bucket, folders cannot be permanently deleted from the **Deleted Objects** list. To permanently delete a folder, you can only configure a lifecycle rule.

- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the navigation pane, choose **Overview**.
- Step 4** In the **Basic Configurations** area, click **Lifecycle Rules**. The **Lifecycle Rules** page is displayed.

Alternatively, you can choose **Basic Configurations > Lifecycle Rules** in the navigation pane.

- Step 5** Click **Create**.

Figure 9-12 Creating a lifecycle rule



Step 6 Configure a lifecycle rule.

Configure parameters under **Basic Information**:

- **Status:** Select **Enable** to enable this lifecycle rule after the configuration.
- **Rule Name:** It identifies a lifecycle rule. The rule name must be no longer than 255 characters.
- **Prefix:** It is optional.
 - If this field is configured, objects with the specified prefix will be managed by the lifecycle rule. The prefix cannot start with a slash (/) or contain two consecutive slashes (//), and cannot contain the following special characters: \:*?'"<>|
 - If this field is not configured, all objects in the bucket will be managed by the lifecycle rule.

Configure parameters under **Current Version** or **Historical Version**:

Delete Objects After (Days): After this number of days since the last update, OBS will expire and then delete the objects meeting the specified conditions. The days set here must be larger than any of the days configured for the transition actions.

Suppose that you last updated the following files in OBS on November 7, 2023:

- **log/notConfigured-1.log** (This file has no WORM retention policy configured.)
- **log/expired-1.log** (The WORM retention policy configured for this file has expired.)
- **doc/withinRetention-1.doc** (The WORM retention policy configured for this file expires on November 30, 2023.)

Then on November 10, 2023, you last updated the following files:

- **log/notConfigured-2.log** (This file has no WORM retention policy configured.)

- **log/expired-2.log** (The WORM retention policy configured for this file has expired.)
- **doc/withinRetention-2.doc** (The WORM retention policy configured for this file expires on November 30, 2023.)

On November 10, 2023, you set the objects prefixed with **log** to expire one day later. You might encounter the following situations:

- Objects **log/notConfigured-1.log** and **log/expired-1.log** last updated on November 7, 2023 might be deleted after the last system scan. The deletion could happen on November 10, 2023 or November 11, 2023, depending on the time of the last system scan. **doc/withinRetention-1.doc** will not be deleted.
- Objects **log/notConfigured-2.log** and **log/expired-2.log** last uploaded on November 10, 2023 might be deleted on November 11, 2023 or November 12, 2023, depending on whether they have been stored for over one day (since their last update) when the system scan happened. **doc/withinRetention-2.doc** will not be deleted.

 NOTE

For more information about how to configure lifecycle rules, see [Configuring a Lifecycle Rule](#).

Step 7 Click **OK**.

----End

Related Operations

When uploading an object, configure a retention policy for the object. For details, see [Uploading an Object](#).

To normally delete objects from a WORM-enabled bucket, see [Deleting an Object or Folder](#).

9.3 Configuring CORS

This section describes how to use CORS in HTML5 to implement cross-origin access.

You can create CORS rules or replicate existing CORS rules from another bucket.

Prerequisites

Static website hosting has been configured. For details, see [Configuring Static Website Hosting](#).

Creating a CORS Rule

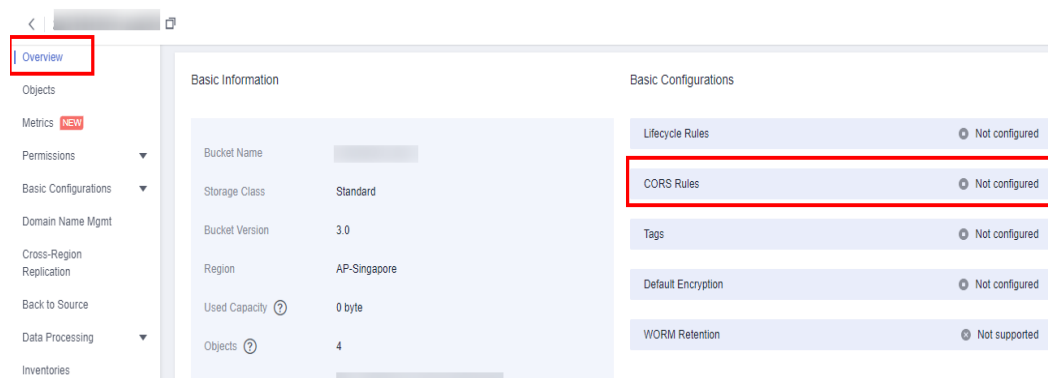
Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the navigation pane, choose **Overview**.

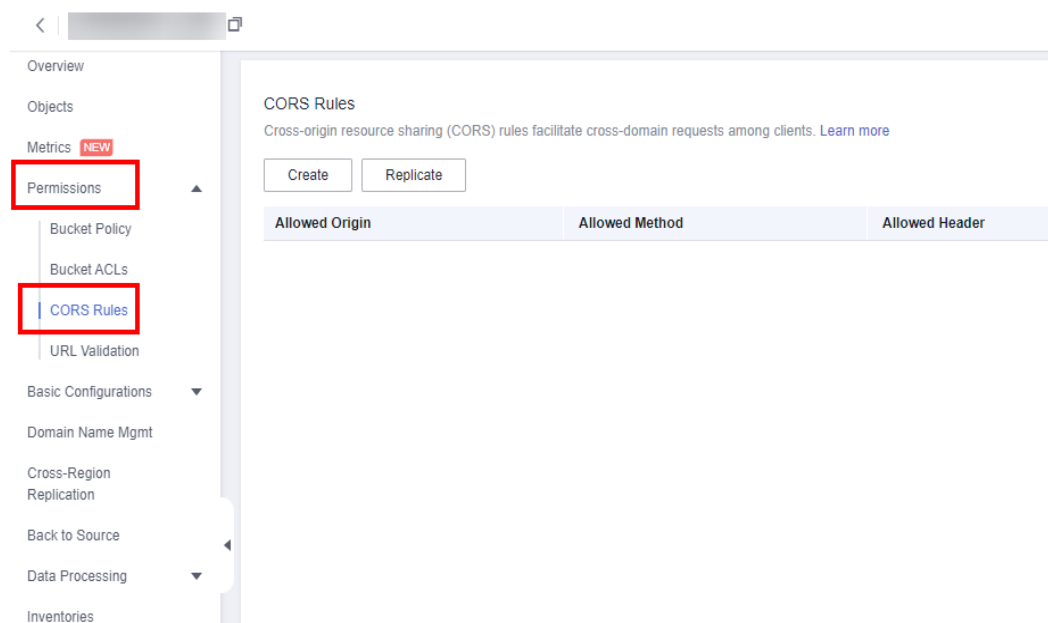
Step 4 In the **Basic Configurations** area, click **CORS Rules**. The **CORS Rules** page is displayed.

Figure 9-13 Overview > Basic Configurations > CORS Rules



Alternatively, you can choose **Permissions** > **CORS Rules** in the navigation pane.

Figure 9-14 Permissions > CORS Rules



Step 5 Click **Create**. The **Create CORS Rule** dialog box is displayed. See [Figure 9-15](#) for details.

NOTE

A bucket can have a maximum of 100 CORS rules configured.

Figure 9-15 Creating a CORS rule

Create CORS Rule [Learn more](#) ×

★ Allowed Origin ?
0/1,024

★ Allowed Method

Allowed Header ?
0/1,024

Exposed Header ?
0/1,024

Cache Duration (s)

Step 6 In the **CORS Rule** dialog box, configure **Allowed Origin**, **Allowed Method**, **Allowed Header**, **Exposed Header**, and **Cache Duration (s)**.

NOTE

If CDN acceleration is enabled for the bucket, HTTP headers must be configured on CDN. For details, see [HTTP Header Settings](#).

Table 9-1 Parameters in CORS rules

| Parameter | Description |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Allowed Origin | <p>Mandatory</p> <p>Specifies the origins from which requests can access the bucket.</p> <p>Multiple matching rules are allowed. One rule occupies one line, and allows one wildcard character (*) at most. An example is given as follows:</p> <pre>http://rds.example.com https://*.vbs.example.com</pre> |
| Allowed Method | <p>Mandatory</p> <p>Specifies the allowed request methods for buckets and objects.</p> <p>The methods include Get, Post, Put, Delete, and Head.</p> |

| Parameter | Description |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Allowed Header | Optional Specifies the allowed headers in cross-origin requests. Only CORS requests matching the allowed headers are valid. You can enter multiple allowed headers (one per line) and each line can contain one wildcard character (*) at most. Spaces and special characters including & and < are not allowed. |
| Exposed Header | Optional Specifies the exposed headers in CORS responses, providing additional information for clients. By default, a browser can access only headers Content-Length and Content-Type . If the browser wants to access other headers, you need to configure those headers in this parameter. You can enter multiple exposed headers (one per line). Spaces and special characters including * and < are not allowed. |
| Cache Duration (s) | Mandatory Specifies the duration that your browser can cache CORS responses, expressed in seconds. The default value is 100 . |

Step 7 Click **OK**.

Message "The CORS rule created successfully." is displayed. The CORS configuration takes effect within two minutes.

After CORS is successfully configured, only the addresses specified for **Allowed Origin** can access the bucket using the methods specified for **Allowed Method**. For example, you can configure CORS parameters for bucket **testbucket** as follows:

- **Allowed Origin:** **https://www.example.com**
- **Allowed Method:** **GET**
- **Allowed Header:** *****
- **Exposed Header:** *****
- **Cache Duration (s):** **100**

By doing so, OBS only allows GET requests from **https://www.example.com** to access bucket **testbucket**, without restrictions on request headers. The client can cache CORS responses for 100 seconds.

----End

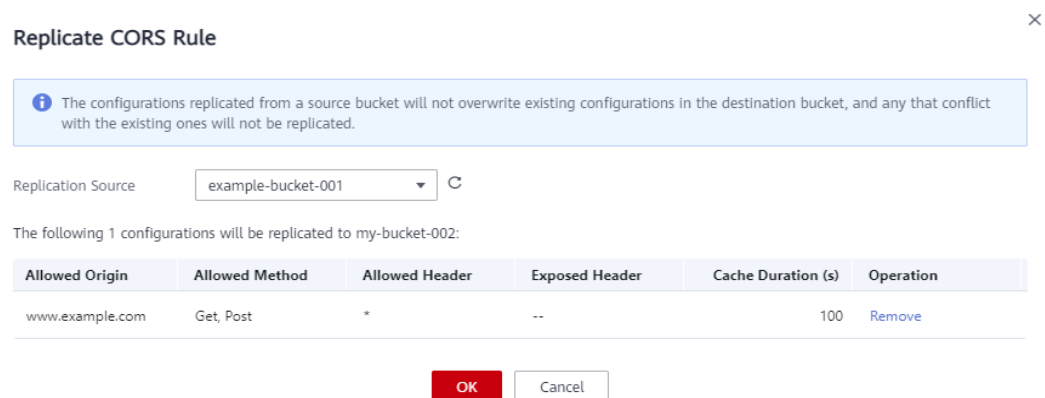
Replicating CORS Rules

- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the navigation pane, choose **Overview**.
- Step 4** In the **Basic Configurations** area, click **CORS Rules**. The **CORS Rules** page is displayed.
- Alternatively, you can choose **Permissions** > **CORS Rules** in the navigation pane.
- Step 5** Click **Replicate**.
- Step 6** Select a replication source, which is the bucket whose CORS rules you want to replicate.

NOTE

- The CORS 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.
- Both source and destination buckets must be of the 3.0 version.
- You can remove the rules that you do not want to replicate.
- There can be 100 CORS rules at most in a bucket. If the number of rules you will replicate plus the number of existing rules in the destination bucket exceeds 100, the replication will fail. Before replicating the rules, delete some if necessary.

Figure 9-16 Replicating CORS rules



- Step 7** Click **OK** to replicate the CORS rules to the destination bucket.

----End

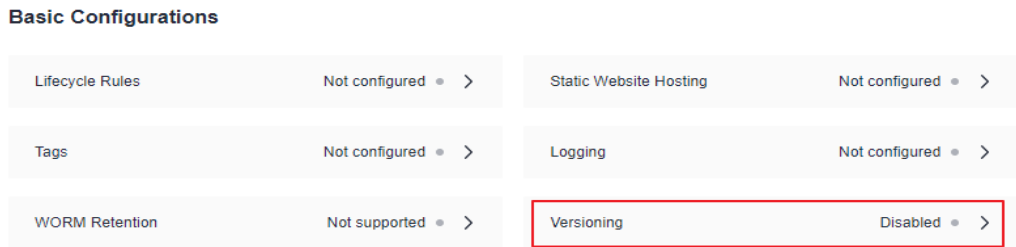
9.4 Configuring Versioning

Procedure

- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the navigation pane, choose **Overview**.

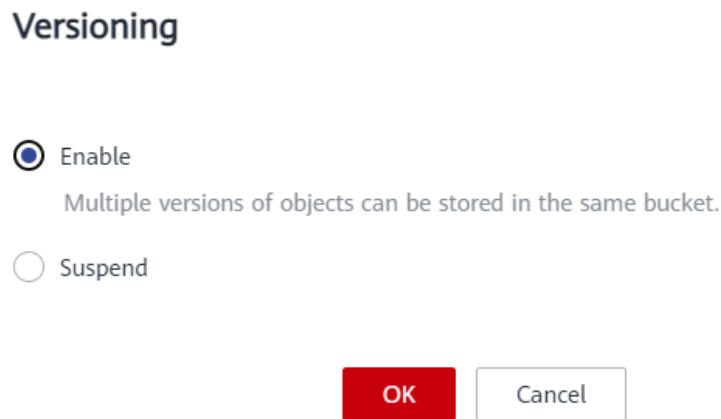
Step 4 In the **Basic Configurations** area, click **Versioning**.

Figure 9-17 Editing versioning status



Step 5 Select **Enable**. For details, see [Figure 9-18](#).

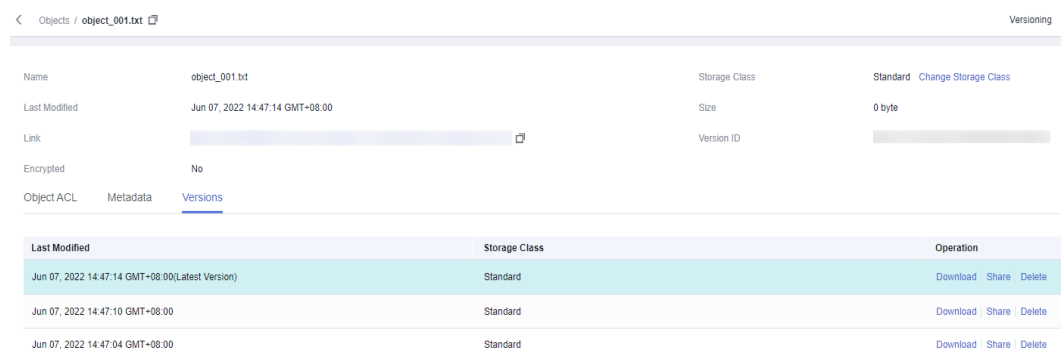
Figure 9-18 Configuring versioning



Step 6 Click **OK** to enable versioning for the bucket.

Step 7 Click an object to go to the object details page. On the **Versions** tab page, view all versions of the object.

Figure 9-19 Viewing object versions



----End

Related Operations

After versioning is configured for a bucket, you can go to the object details page, click the **Versions** tab, and then delete, share, and download object versions, and extend the retention period of an object version.

Step 1 In the navigation pane of **OBS Console**, choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the object list, click the object you want to go to the object details page.

Step 4 On the **Versions** tab page, view all versions of the object.

Step 5 Perform the following operations on object versions:

1. Download a desired version of the object by clicking **Download** in the **Operation** column.

 **NOTE**

If the version you want to download is in the Archive or Deep Archive storage class, restore it first.

2. Share a version of the object by clicking **Share** in the **Operation** column.
3. Delete a version of the object by clicking **Delete** or **More > Delete** in the **Operation** column. If you delete the latest version, the most recent version will become the latest version.

 **NOTE**

In a WORM-enabled bucket, if an object has no retention policy configured or its retention policy has expired, you can delete a desired object version on the object's **Versions** tab page. If an object version is within the retention period, it cannot be deleted.

4. Locate the object version for which you want to extend the retention period, choose **More > Extend Retention Period**, and select a date. A retention period can only be extended, but not shortened.

----End

9.5 Configuring Cross-Region Replication

To replicate objects from a source bucket to a destination bucket in a different region, you can configure a single cross-region replication rule that is applied to all objects in the bucket, or you can configure multiple rules that are applied to a set of objects by specifying a prefix.

 **NOTE**

A cross-region replication rule may not take effect immediately upon its configuration. Accordingly, the objects that this rule is applied to may not be replicated immediately after the rule is configured.

Buckets with WORM enabled do not support cross-region replication.

Prerequisites

The source bucket version is 3.0 or later, and cross-region replication is available in the region of the source bucket. For details about the support for cross-region

replication in each region, search for "cross-region replication" on the [Function Overview](#) page.

Procedure

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the navigation pane, click **Cross-Region Replication**.
- Step 4** Click **Create Rule**. The **Create Cross-Region Replication Rule** dialog box is displayed. See [Figure 9-20](#).

Figure 9-20 Creating a cross-region replication rule

Create Cross-Region Replication Rule ×

i The versioning status of the source bucket and the destination bucket must keep the same.

i Buckets with the WORM retention enabled do not support cross-region replication.

Status Enable Disable

Source Bucket

Region LA-Mexico City2

Bucket Name

Replicate

Prefix
To replicate a folder, end the prefix with a slash (/). Example: folder1/

Synchronize Existing Objects

NOTE

- The versioning status of the source and destination buckets must keep the same.
- A bucket can have only one destination bucket and one IAM agency configured for cross-region replication. The destination bucket and IAM agency specified in a later replication rule will overwrite those in the previous replication rule of the bucket.

- Step 5** Configure a cross-region replication rule according to your service needs. For details about the parameters, see [Table 9-2](#).

Table 9-2 Cross-region replication parameters

| Parameter | | Description |
|---------------|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status | | Indicates whether the rule is enabled or disabled after being created. The versioning status of the source and destination buckets must keep the same. |
| Source Bucket | Replicate | Indicates the objects the rule will apply to. <ul style="list-style-type: none"> ● All objects: The rule applies to all objects in the bucket. ● Match by prefix: The rule applies only to objects with the specified prefix. |
| | Prefix | <ul style="list-style-type: none"> ● To apply the rule to objects with the specified prefix, you must set Prefix to a value no longer than 1,024 characters. ● If the specified prefix overlaps with the prefix of an existing rule, OBS regards these two rules as one and forbids you to configure the one you are configuring. For example, if there is already a rule with prefix abc in OBS, you cannot configure another rule whose prefix starts with abc. ● To copy a folder, end the prefix with a slash (/), for example, imgs/. |
| | Synchronize Existing Objects | Indicates whether to synchronize the objects that were already in the bucket before the rule configuration to the destination bucket. By default, these objects are not synchronized. |

| Parameter | | Description |
|--------------------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Replicate KMS encrypted objects | <p>OBS will try to copy KMS encrypted objects no matter whether this option is selected or not.</p> <ul style="list-style-type: none"> If this option is selected, only the IAM agencies that have the KMS Administrator permission for both source and destination ends are displayed in the drop-down list of IAM Agency in the Create Cross-Region Replication Rule dialog box. If this option is not selected, only the IAM agencies that do not have the KMS Administrator permission for either the source or destination end are displayed in the drop-down list of IAM Agency in the Create Cross-Region Replication Rule dialog box. <p>If KMS is not available in the destination region or the agency does not have the KMS Administrator permission in the source and destination regions, KMS encrypted objects will fail to be replicated to the destination bucket, and the object replication status will be failed.</p> <p>After a KMS-encrypted object is replicated to the destination bucket, the key for encrypting the object copy changes to the default key obs/default of the destination region.</p> |
| Destination Bucket | Region | Indicates the region of the destination bucket. The destination and source buckets must be in different regions. |
| | Bucket | Indicates the destination bucket. |
| | Change storage class for replicated objects | By default, this option is not selected, indicating that the storage class of object copies is the same as that of the source objects. If you need to change the storage class of objects copies, select this parameter, then you can specify a storage class. |

| Parameter | | Description |
|-------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Permissions | IAM Agency | <p>Delegates OBS to operate your resources, so that OBS can use this agency to implement cross-region replication.</p> <p>If there is no IAM agency available, click View IAM agencies to create one. If you have already created IAM agencies, select one from the drop-down list.</p> <p>NOTE The IAM agency selected here must be of OBS. The OBS project must have the Tenant Administrator permission. If Replicate KMS encrypted objects is selected, you also need the KMS Administrator permission in the regions where the source and destination buckets are located.</p> |

Step 6 (Optional) Create an IAM Agency. For details, see [Creating an IAM Agency](#).

Step 7 Click **OK**. The cross-region replication rule is created.

----End

9.6 Configuring URL Validation

OBS blocks access requests from blacklisted URLs and allows those from whitelisted URLs.

Prerequisites

Static website hosting has been enabled.

Procedure

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the navigation pane, choose **Overview**.

Step 4 In the **Basic Configurations** area, click **URL Validation**. The **URL Validation** page is displayed.

Step 5 Click  next to the text box of **Whitelisted Referers** or **Blacklisted Referers**, and enter the referers.

Principles for setting **Referers**:


- The length of a whitelist or blacklist cannot exceed 1024 characters.
- Referer format:
 - You can enter multiple referers, each in a line.

- The referer parameter supports asterisks (*) and question marks (?). An asterisk works as a wildcard that can replace zero or multiple characters, and a question mark (?) can replace a single character.
- If the referer header field contains **http** or **https** during download, the referer must contain **http** or **https**.
- If **Whitelisted Referers** is left blank but **Blacklisted Referers** is not, all websites except those specified in the blacklist are allowed to access data in the target bucket.
- If **Whitelisted Referers** is not left blank, only the websites specified in the whitelist are allowed to access the target bucket no matter whether **Blacklisted Referers** is left blank or not.

 **NOTE**

If **Whitelisted Referers** is configured the same as **Blacklisted Referers**, the blacklist takes effect. For example, if both **Whitelisted Referers** and **Blacklisted Referers** are set to **https://www.example.com**, access requests from this address will be blocked.

- If **Whitelisted Referers** and **Blacklisted Referers** are both left blank, all websites are allowed to access data in the target bucket by default.
- Before determining whether a user has the four types of permissions (read, write, ACL read, and ACL write) for a bucket or objects in the bucket, check whether this user complies with the URL validation principles of the **Referer** field.

Step 6 Click  to save the settings.

----End

10 Data Processing

10.1 Configuring an Online Decompression Policy

You can compress multiple files into a ZIP package and then upload it to OBS for auto decompression online.

If the package you uploaded matches the configured decompression policy, it will be automatically decompressed upon upload. A decompression policy does not apply to the ZIP packages that already exist in OBS before the policy is created.

You can create online decompression policies or replicate existing policies from another bucket.

NOTE

Online decompression is only available in some regions. For details, see [Function Overview](#).

Creating an Online Decompression Policy

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the navigation pane, choose **Data Processing > Online Decompression**. The **Online Decompression** page is displayed.
- Step 4** Click **Create**. The dialog box shown in [Figure 10-1](#) is displayed.

Figure 10-1 Create Online Decompression Policy

Create Online Decompression Policy

Policy Name ?

Events ?

Prefix ?
If this field is left blank, the policy applies to all the files in the bucket.

Suffix ?
Currently, only .zip is supported.

Duplicate Name Processing ?

Decompress To ?

IAM Agency ? [Create Agency](#) ?
Select an IAM agency of OBS, with permission OBS OperateAccess assigned to this agency.

Step 5 Configure the online decompression policy. [Table 10-1](#) describes the related parameters.

Table 10-1 Parameter description

| Parameter | Description |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy Name | Enter a policy name that is easy to remember. The value can contain 1 to 256 characters, and only uppercase letters, lowercase letters, digits, underscores (_), and hyphens (-) are allowed, for example, event_0001 . |

| Parameter | Description |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Events | <p>Events that you want to trigger the online decompression policy for. Currently, the following event types are supported:</p> <ul style="list-style-type: none"> ● ObjectCreated: all object creation operations, including PUT, POST, COPY, and part assembling ● Put: object upload using PUT ● Post: object upload using POST ● Copy: object copying using COPY ● CompleteMultipartUpload: assembling of parts in a multipart upload <p>NOTE To decompress the ZIP package that contains other ZIP packages, set the event type to ObjectCreated or CompleteMultipartUpload.</p> |
| Prefix | <p>Optional. If this parameter is configured, the decompression policy applies to the packages whose name contains this prefix. The prefix cannot start with a slash (/) or contain double slashes (//), or contain special characters (\ : * ? " < >). The total length of the prefix and suffix cannot exceed 512 characters.</p> <ul style="list-style-type: none"> ● With this parameter configured, ZIP packages whose name contains the specified prefix will trigger online decompression. ● With this parameter left blank, the decompression policy applies to all the uploaded ZIP packages. <p>CAUTION</p> <ul style="list-style-type: none"> - You are advised to configure a prefix. Otherwise, cyclic decompression may occur if a package contains other packages. - The configured prefix must contain all levels of the directory for storing the object. For example, there is an object example123 that is stored under bucket/file/example123. If you want example to be the prefix, set the prefix to file/example. |
| Suffix | <p>If this parameter is specified, the decompression policy applies to the packages whose name contains this suffix. Currently, .zip is the default and only value.</p> |

| Parameter | Description |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Duplicate Name Processing | <p>It specifies how the decompressed objects are processed if they have the same names as the existing objects in the bucket.</p> <ul style="list-style-type: none"> • Do not decompress: Retains the existing objects, 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 in the bucket. |
| Decompress To | <p>Optional, this parameter specifies the path for storing decompressed files. It cannot contain special characters (\:*?\"<>), start or end with a period (.), or contain two or more consecutive slashes (/). The value can contain 0 to 1,023 characters.</p> <ul style="list-style-type: none"> • With this parameter configured, the path must end with a slash (/). After a ZIP package is decompressed, the decompressed files are stored in the folder with the same name as the path. If there is no such a folder in the bucket, OBS automatically creates one for storing the files. • With this parameter left blank, decompressed objects are stored in the home directory of the bucket. |
| IAM Agency | <p>Select an IAM agency of OBS, with the OBS OperateAccess permission assigned.</p> <p>If no such agency is available, create one.</p> |

Step 6 Click **OK**. The online decompression policy is created.

----End

Replicating Online Decompression Policies

Step 1 In the navigation pane of **OBS Console**, choose **Object Storage**.

Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

Step 3 In the navigation pane, choose **Data Processing > Online Decompression**. The **Online Decompression** page is displayed.

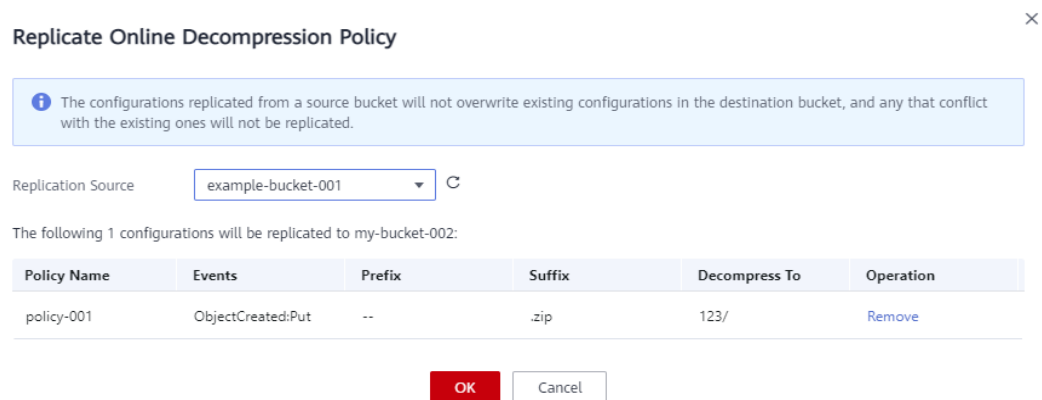
Step 4 Click **Replicate**.

Step 5 Select a replication source, which is the bucket whose online decompression policies you want to replicate.

 **NOTE**

- The online decompression policies replicated from a source bucket will not overwrite existing policies in the destination bucket, and any that conflict with the existing ones will not be replicated.
- Both source and destination buckets must be of the 3.0 version.
- You can remove the policies that you do not want to replicate.
- There can be 10 online decompression policies at most in a bucket. If the number of policies you will replicate plus the number of existing policies in the destination bucket exceeds 10, the replication will fail. Before replicating the policies, delete some if necessary.

Figure 10-2 Replicating online decompression policies



Step 6 Click **OK** to replicate the online decompression policies to the destination bucket.

----End

11 Monitoring and Logging

11.1 Monitoring

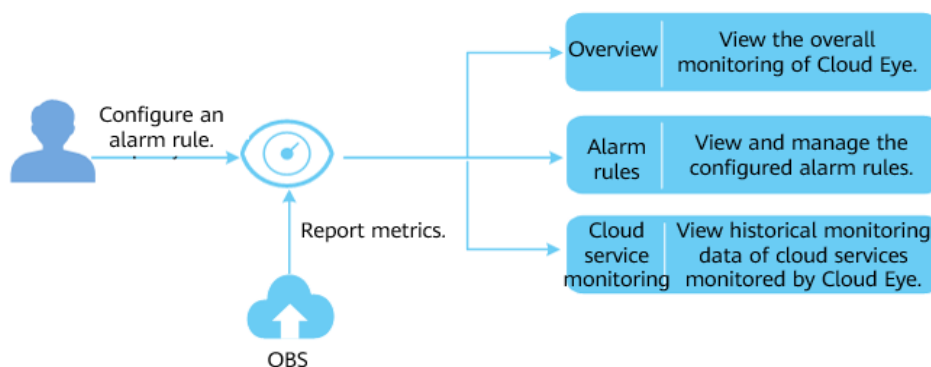
11.1.1 Monitoring OBS

Scenarios

In the use of OBS, you may send PUT and GET requests that generate upload and download traffic, or receive error responses from the server. To learn the requests, traffic, and error responses in a timely manner, you can use Cloud Eye to perform automatic and real-time monitoring over your buckets.

You do not need to separately subscribe to Cloud Eye. It starts automatically once you create a resource (a bucket, for example) in OBS. For more information about Cloud Eye, see [What Is Cloud Eye?](#)

Figure 11-1 Cloud Eye monitoring



Setting Alarm Rules

In addition to automatic and real-time monitoring, you can configure alarm rules in Cloud Eye to receive alarm notifications when specified events happen.

For details, see [Creating an Alarm Rule](#).

Viewing OBS Monitoring Metrics

Cloud Eye monitors **OBS monitoring metrics** in real time. You can view detailed monitoring statistics of each metric on the console of Cloud Eye.

For details, see [Querying Cloud Service Monitoring Metrics](#).

11.1.2 OBS Monitoring Metrics

Functions

This section defines the namespace, list, and dimensions of monitoring metrics reported by OBS to Cloud Eye. You can use the management console or [API](#) provided by Cloud Eye to search for monitoring metrics and alarms generated by OBS.

Namespace

SYS.OBS

Monitoring Metrics

| Metric ID | Metric | Description | Value Range | Monitored Entity | Monitoring Period (Original Metric) |
|-------------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------|-------------------------------------|
| download_bytes | Bytes Downloaded | Specifies the response bytes of all download requests made to all buckets in a region, including bytes in HTTP entity bodies. Unit: byte | ≥ 0 bytes | Bucket | 5 min |
| upload_bytes | Bytes Uploaded | Specifies the bytes of all upload requests made to all buckets in a region, including bytes in HTTP entity bodies. Unit: byte | ≥ 0 bytes | Bucket | 5 min |
| get_request_count | GET Requests | Specifies the number of GET, HEAD, or OPTIONS requests made to all buckets and objects in the buckets of a region. Unit: count | ≥ 0 counts | Bucket | 5 min |

| Metric ID | Metric | Description | Value Range | Monitored Entity | Monitoring Period (Original Metric) |
|--------------------|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------|-------------------------------------|
| put_request_count | PUT Requests | Specifies the number of PUT, POST, and DELETE requests made to all buckets and objects in the buckets of a region. Unit: count | ≥ 0 counts | Bucket | 5 min |
| first_byte_latency | First Byte Download Delay | Specifies the average time from receiving a GET, HEAD, or OPTIONS request to the time that the system starts to respond in a measurement period. Unit: ms | ≥ 0 ms | Bucket | 5 min |
| request_count_4xx | 4xx Errors | Specifies the times that the server responds to requests whose error codes are 4xx. Unit: count | ≥ 0 counts | Bucket | 5 min |
| request_count_5xx | 5xx Errors | Specifies the times that the server responds to requests whose error codes are 5xx. Unit: count | ≥ 0 counts | Bucket | 5 min |

Dimensions

Table 11-1 Dimensions

| Key | Value |
|-------------|-------------------------------------------------|
| bucket_name | Bucket dimension. The value is the bucket name. |

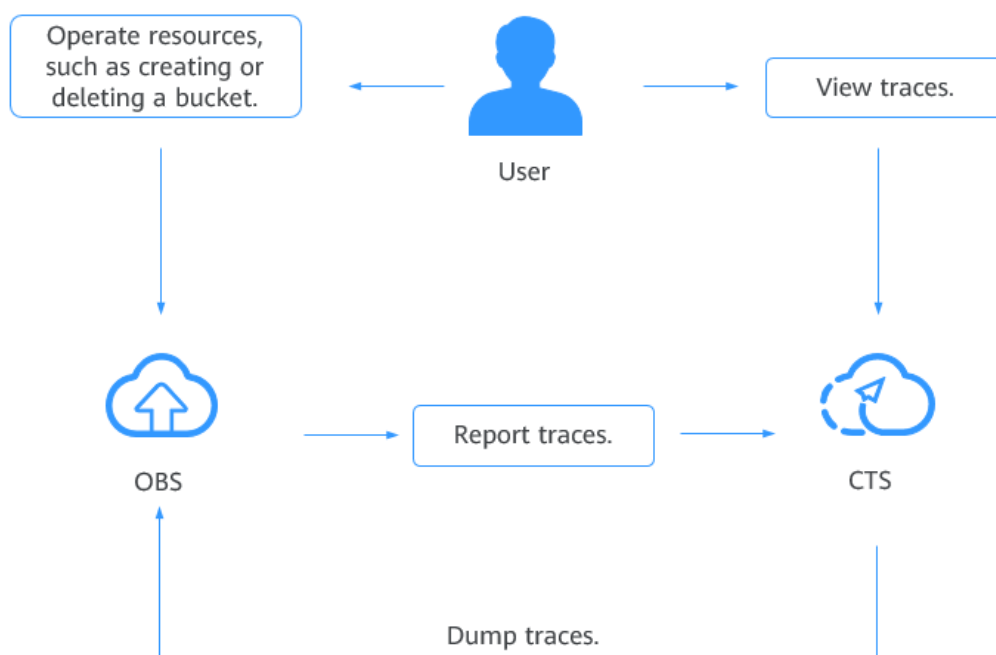
11.2 Cloud Trace Service

Cloud Trace Service (CTS) records operations on cloud resources in your account. You can use the logs to perform security analysis, track resource changes, audit compliance, and locate faults.


After you enable CTS and configure a tracker, CTS can record management and data traces of OBS for auditing.

For details about how to enable and configure CTS, see [Enabling CTS](#).

Figure 11-2 CTS



Procedure

- Step 1** Log in to the management console.
- Step 2** In the upper left corner of the top navigation menu, click  to select a region.
- Step 3** Choose **Service List > Management & Governance > Cloud Trace Service**. The **Trace List** page is displayed.
- Step 4** Configure the cloud audit for OBS by referring to [Configuring a Tracker](#) in the *Cloud Trace Service User Guide*.

----End

Table 11-2 OBS management operations logged by CTS

| Tracker Type | Operation | Resource | Trace Name |
|--------------|-----------------------------------------------------------------|----------|---------------------------|
| Management | Deleting a bucket | bucket | deleteBucket |
| Management | Deleting the CORS configuration of a bucket | bucket | deleteBucketCors |
| Management | Deleting the custom domain name configuration | bucket | deleteBucketCustom-domain |
| Management | Deleting the lifecycle configuration of a bucket | bucket | deleteBucketLifecycle |
| Management | Deleting a bucket policy | bucket | deleteBucketPolicy |
| Management | Deleting the cross-region replication configuration of a bucket | bucket | deleteBucketReplication |
| Management | Deleting the tag configuration of a bucket | bucket | deleteBucketTagging |
| Management | Deleting the static website hosting configuration of a bucket | bucket | deleteBucketWebsite |
| Management | Creating a bucket | bucket | createBucket |
| Management | Configuring the bucket ACL | bucket | setBucketAcl |
| Management | Configuring the CORS rule for a bucket | bucket | setBucketCors |
| Management | Setting the custom domain name for a bucket | bucket | setBucketCustomdomain |
| Management | Configuring the bucket lifecycle rules | bucket | setBucketLifecycle |
| Management | Configuring the bucket logging function | bucket | setBucketLogging |

| Tracker Type | Operation | Resource | Trace Name |
|--------------|---------------------------------------------------------------|----------|------------------------|
| Management | Configuring the event notification function for buckets | bucket | setBucketNotification |
| Management | Configuring the bucket policy | bucket | setBucketPolicy |
| Management | Configuring the bucket quota | bucket | setBucketQuota |
| Management | Configuring the cross-region replication function for buckets | bucket | setBucketReplication |
| Management | Configuring the bucket storage class | bucket | setBucketStorageclass |
| Management | Configuring the bucket tag | bucket | setBucketTagging |
| Management | Configuring the versioning function for buckets | bucket | setBucketVersioning |
| Management | Configuring the static domain name for buckets | bucket | setBucketWebsite |
| Management | Configuring bucket's default encryption | bucket | setBucketEncryption |
| Management | Deleting bucket's default encryption settings | bucket | deleteBucketEncryption |

Table 11-3 OBS data operations logged by CTS

| Tracker Type | Operation | Resource | Trace Name |
|--------------|-------------------------|----------|----------------|
| Data_Read | Downloading an object | object | GET.OBJECT |
| Data_Read | Querying the object ACL | object | GET.OBJECT.ACL |

| Tracker Type | Operation | Resource | Trace Name |
|--------------|-----------------------------------------------|----------|-----------------------------|
| Data_Read | Querying the bucket website configuration | object | GET.OBJECT.WEBSITE |
| Data_Read | Accessing an object through the website | object | HEAD.OBJECT.WEBSITE |
| Data_Read | Querying the object metadata | object | HEAD.OBJECT |
| Data_Read | Listing part data | object | LIST.OBJECT.UPLOAD |
| Data_Write | Deleting an object | object | DELETE.OBJECT |
| Data_Write | Canceling a part | object | DELETE.UPLOAD |
| Data_Write | Queries the cross-domain requests for objects | object | OPTIONS.OBJECT |
| Data_Write | Uploading an object | object | POST.OBJECT |
| Data_Write | Deleting objects in batches | object | POST.OBJECT.MULTIDELETE |
| Data_Write | Restoring Archive objects | object | POST.OBJECT.RESTORE |
| Data_Write | Merging parts | object | POST.UPLOAD.COMPLET E |
| Data_Write | Initializing multipart tasks | object | POST.UPLOAD.INIT |
| Data_Write | Uploading an object | object | PUT.OBJECT |
| Data_Write | Configuring the object ACL | object | PUT.OBJECT.ACL |
| Data_Write | Copying an object | object | PUT.OBJECT.COPY |
| Data_Write | Configuring the object storage class | object | PUT.OBJECT.STORAGECL ASS |
| Data_Write | Uploading a part | object | PUT.PART |
| Data_Write | Copying a part | object | PUT.PART.COPY |

Follow-up Procedure

You can click **Disable** under the **Operation** column on the right of a tracker to disable the tracker. After the tracker is disabled, the system will stop recording operations, but you can still view existing operation records.

You can click **Delete** under the **Operation** column on the right of a tracker to delete the tracker. Deleting a tracker has no impact on existing operation records. When you enable CTS again, you can view operation records that have been generated.

11.3 Configuring Access Logging for a Bucket

After logging is enabled for a bucket, OBS automatically converts bucket logs into objects following the naming rules and writes the objects into a target bucket.

Uploading bucket logs to the target bucket incurs billable PUT requests. For details about the pricing, see [Requests](#).

Procedure

- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the navigation pane, choose **Overview**.
- Step 4** In the **Basic Configurations** area, click **Logging**. The **Logging** dialog box is displayed.
- Step 5** Select **Enable**. For details, see [Figure 11-3](#).

Figure 11-3 Logging

Logging

i Access requests can be logged for analysis or auditing. [Learn more](#)

Enable

The log delivery user will be automatically granted permissions to read the ACL of the bucket where logs are to be saved and write logs to the bucket. Uploading logs to bucket incurs costs for PUT requests. For prices, check OBS Product Pricing Details.

Save Logs To: ↻ ?

Log File Name Prefix: ?

IAM Agency: ↻ Create Agency ?

Disable

OK
Cancel

Step 6 Select an existing bucket where you want to store log files. Log delivery users of the selected bucket will be automatically granted the permissions to read the bucket ACL and write logs to the bucket.

Step 7 Enter a prefix for the **Log File Name Prefix**.

After logging is enabled, generated logs are named in the following format:

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

- *<Log File Name Prefix>* is the shared prefix of log file names.
- **YYYY-mm-DD-HH-MM-SS** indicates when the log is generated.
- *<UniqueString>* indicates a character string generated by OBS.

On OBS Console, if the configured *<Log File Name Prefix>* ends with a slash (/), logs generated in the bucket are stored in the *<Log File Name Prefix>* folder in the bucket, facilitating the management of log files.

Example:

- If the bucket named **bucket** is used to save log files, and the log file name prefix is set to **bucket-log/**, all log files delivered to this bucket are saved in the **bucket-log** folder. A log file is named as follows: **2015-06-29-12-22-07-N7MXLAF1BDG7MPDV**.
- If the bucket named **bucket** is used to save log files, and the log file name prefix is set to **bucket-log**, all log files are saved in the root directory of the

bucket. A log file is named as follows: **bucket-log2015-06-29-12-22-07-N7MXLAF1BDG7MPDV**.

Step 8 Select an IAM agency to grant OBS the permission to upload log files to the specified 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 default encryption is enabled for the log storage bucket, the IAM agency also requires the **KMS Administrator** permission for the region where the bucket is located.

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

You can choose an existing IAM agency from the drop-down list or click **Create Agency** to create one. For details about how to create an agency, see [Creating an IAM Agency](#).

Step 9 Click **OK**.

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

----End

Related Operations

If you do not need to record logs, in the **Logging** dialog box, click **Disable** and then click **OK**. After logging is disabled, logs are not recorded, but existing logs in the target bucket will be retained.

12 Managing Resource Packages

Scenarios

View your resource package usage on the **Resource Packages** page of OBS Console. On this page, you can quickly learn about the status, remaining capacity, start/end time, order ID, and other information of your packages.

Background Information

OBS offers you pay-as-you-go and yearly/monthly approaches for pricing resource packages. Yearly/monthly packages provide you with certain resource quota and duration, which is more favourable than pay-as-you-go.

For details about the OBS resource package types and functions, see [Resource Package Overview](#).

Prerequisites

You have purchased at least one resource package. For details, see [Resource Package Purchase](#).

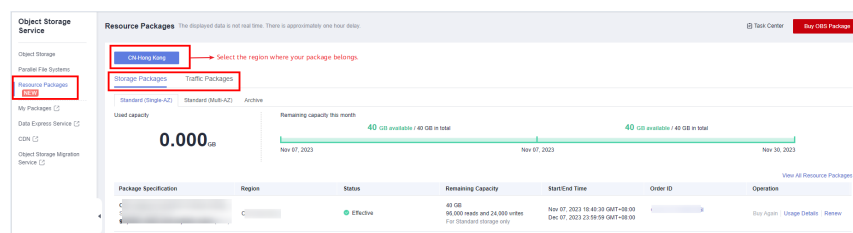
Viewing Resource Package Details

Step 1 In the navigation pane of OBS Console, select **Resource Packages**.

Step 2 Select the region and type of your package to view its details.

The detailed information includes the package specification, region, status, remaining capacity, start/end time, order ID and usage details.

Figure 12-1 Viewing resource package details

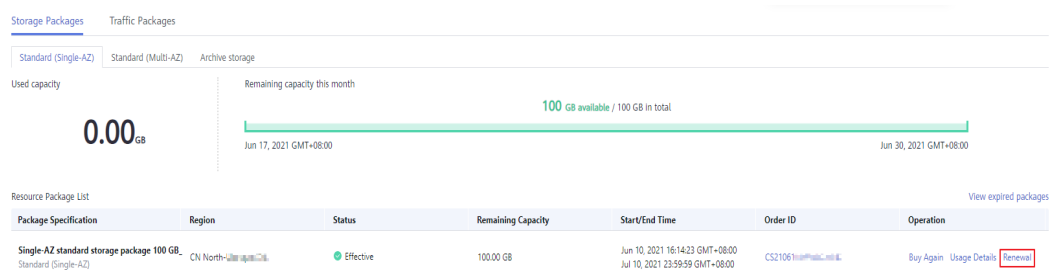


----End

Renewing a Resource Package

- Step 1** In the navigation pane of OBS Console, select **Resource Packages**.
- Step 2** Select the region and type of the resource package you want to renew.
- Step 3** In the row containing the target package, click **Renewal** in the **Operation** column.

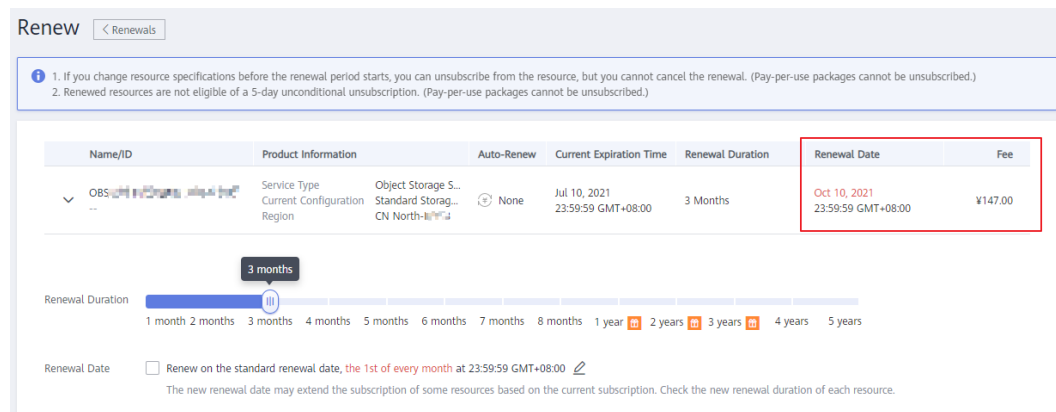
Figure 12-2 Renewing a resource package



- Step 4** Select a renewal duration.

The time when the resource package will expire and the corresponding renewal fee are displayed.

Figure 12-3 Selecting a renewal duration



- Step 5** (Optional) Set the renewal date to the first day of each month as needed.

Selecting **Renew on the standard renewal date** may result in additional renewal days and incur additional fees accordingly. Once you select this option, ensure that you are clear about the renewal duration and fee.

- Step 6** Check that all configurations are correct and click **Pay Now**, and then complete the payment.

----End

13 Task Center

When you upload objects, restore objects in batches, change storage classes in batches, or delete folders, corresponding records of the tasks will be displayed in the task center for you to view the tasks' progress and status.

 **NOTE**

When the web page is reloaded, the task records in the task management list will get lost.

Procedure

Step 1 In the object list of your bucket, click **Task Center** in the upper right corner.

Step 2 View the records of uploading objects, restoring objects in batches, changing storage classes in batches, or deleting folders.

- Click **Clear Records** to clear all task records.
- On the **Upload** tab page, you can click **Pause All** or **Start All** to manage upload tasks in batches.

----End

14 Related Operations

14.1 Creating an IAM Agency

To use some OBS features, you need to use IAM agencies to grant required permissions to OBS for processing your data.

Creating an Agency for Cross-Region Replication

Step 1 In the **Create Cross-Region Replication Rule** dialog box on OBS Console, click **View IAM agencies** to jump to the **Agencies** page on the IAM console.

Step 2 Click **Create Agency**.

Step 3 Enter an agency name.

Step 4 Select **Cloud service** for the **Agency Type**.

Step 5 Select **Object Storage Service (OBS)** for **Cloud Service**.

Step 6 Set a validity period.

Step 7 Click **Next**.

 **NOTE**

The console for creating an agency has the new and old editions. Here describes how to create an agency on the console of the new edition.

Step 8 On the **Select Policy/Role** page, search for and select **OBS Administrator** and click **Next**.

Step 9 On the **Select Scope** page, select **Global services** for **Scope** and click **OK**.

Step 10 (Optional) If **Replicate KMS encrypted objects** is selected, the IAM agency also needs the **KMS Administrator** permissions in the regions where the source and destination buckets are located.

1. Go to the **Agencies** page of the IAM console and click the name of the agency created in the previous step.
2. Choose the **Permissions** tab and click **Authorize**.

3. On the **Select Policy/Role** page, search for and select **KMS Administrator**. Then, click **Next**.
4. On the **Select Scope** page, select **Region-specific projects** for **Scope**. Then, select the projects in the regions where the source and destination buckets are located.

----End

Creating an Agency for Uploading Logs

Step 1 In the **Logging** dialog box, click **Create Agency** to jump to the **Agencies** page on the **Identity and Access Management** console.

Step 2 Click **Create Agency**.

Step 3 Enter an agency name.

Step 4 Select **Cloud service** for the **Agency Type**.

Step 5 Select **Object Storage Service (OBS)** for **Cloud Service**.

Step 6 Set a validity period.

Step 7 Click **Next**.

Step 8 On the **Select Policy/Role** page, select a custom policy that has the permission to upload data to the log storage bucket and click **Next**.

If no custom policy is available, create one by referring to [Creating a Custom Policy](#).

Select **Global services** for **Scope**. Select **JSON** for **Policy View**. The policy content is as follows.

NOTE

When coding the policy content in an actual scenario, replace **mybucketlogs** with the actual bucket name:

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

Step 9 On the **Select Scope** page, select **Global services** for **Scope** and click **OK**.

Step 10 (Optional) If the default encryption is enabled for the log storing bucket, the IAM agency also requires the **KMS Administrator** permission in the region where the log storing bucket resides.

1. Go to the **Agencies** page on the **Identity and Access Management** console and click the name of the agency created in the previous step.

2. Choose the **Permissions** tab and click **Authorize**.
3. On the **Select Policy/Role** page, search for and select **KMS Administrator**. Then, click **Next**.
4. On the **Select Scope** page, select **Region-specific projects** for **Scope**. Then, select the project in the region where the log storage bucket is located.

----End

15 Troubleshooting

15.1 An Object Fails to Be Downloaded Using Internet Explorer 11

Symptom

A user logs in to OBS Console using Internet Explorer 11 and uploads an object. When the user attempts to download the object to the original path to replace the original object without closing the browser, a message is displayed indicating a download failure. Why does this happen?

For example, a user uploads object **abc** from the root directory of local drive C to a bucket in OBS Console. When the user attempts to download the object to the root directory of local drive C to replace the original object without closing the browser, a message is displayed indicating a download failure.

Answer

This problem is caused by browser incompatibility. It can be solved by using a different web browser.

If this problem occurs, close the browser and try again.

15.2 OBS Console Cannot Be Opened in Internet Explorer 9

Question

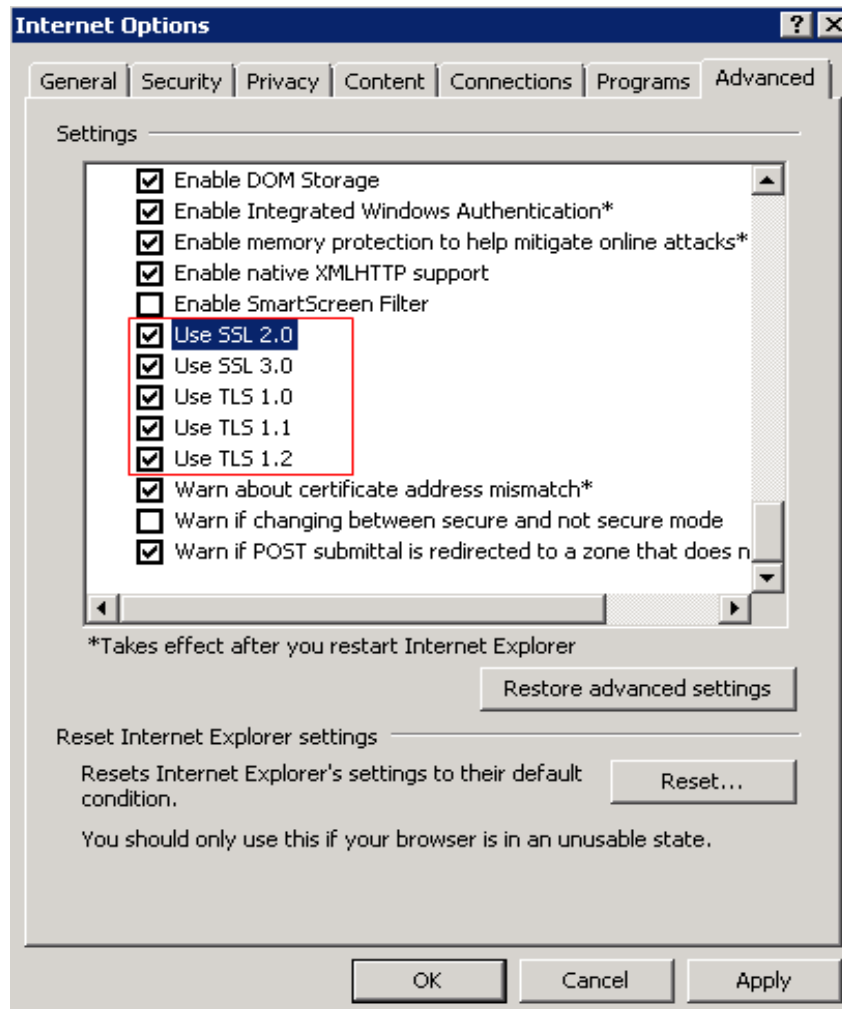
Why OBS Console cannot be opened in Internet Explorer 9, even if the address of OBS Console can be pinged?

Answer

Confirm whether **Use SSL** and **Use TLS** are selected in **Internet Options**. If not, do as follows and try again:

- Step 1** Open Internet Explorer 9.
- Step 2** Click **Tools** in the upper right corner and choose **Internet Options > Advanced**. Then select **Use SSL 2.0**, **Use SSL 3.0**, **Use TLS 1.0**, **Use TLS 1.1**, and **Use TLS 1.2**, as shown in **Figure 15-1**.

Figure 15-1 Internet Options



- Step 3** Click **OK**.

----End

15.3 The Object Name Changes After an Object with a Long Name Is Downloaded to a Local Computer

Question

After an object with a relatively long name is downloaded to a local path, the object name changes.

Answer

For Windows, a file name, including the file name extension, can contain a maximum of 255 characters. When an object with a name containing more than 255 characters is downloaded to a local computer, the system keeps only the first 255 characters automatically.

15.4 Time Difference Is Longer Than 15 Minutes Between the Client and Server

Question

Error message "Time difference is longer than 15 minutes between the client and server" or "The difference between the request time and the current time is too large" is displayed during the use of OBS.

Answer

For security purposes, OBS verifies the time offset between the client and server. If the offset is longer than 15 minutes, the OBS server will reject your requests and this error message is reported. To resolve this problem, adjust your local time (UTC) and try again.

16 Error Code List

If a request fails to be processed due to errors, an error response is returned. An error response contains an error code and error details. [Table 16-1](#) lists some common error codes in OBS error responses.

Table 16-1 OBS error codes

| Error Code | Description |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Obs.0000 | Invalid parameter. |
| Obs.0001 | All access requests to this object are invalid. |
| Obs.0002 | The absolute path of a file cannot exceed 1023 characters. Please retry. |
| Obs.0003 | The connection timed out. |
| Obs.0004 | Time difference is longer than 15 minutes between the client and server. Correctly set the local time. For security purposes, OBS verifies the time offset between the client and server. If the offset is longer than 15 minutes, the OBS server will reject your requests and this error message is reported. To resolve this problem, adjust your local time (UTC) and try again. |
| Obs.0005 | The server load is too heavy. Try again later. |
| Obs.0006 | The number of buckets has reached the upper limit. An account (including all IAM users under this account) can create a maximum of 100 buckets and parallel file systems. You can use the fine-grained access control of OBS to properly plan and use buckets. |
| Obs.0007 | The target bucket does not exist or is not in the same region with the current bucket. |
| Obs.0008 | The account has not been registered with the system. Only a registered account can be used. |

| Error Code | Description |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Obs.0009 | <p>A conflicting operation is being performed on this resource. Please retry.</p> <p>This is because that there is a bucket with the same name as the bucket you are creating in OBS and the existing bucket has been released in the recent period due to arrears. In such case, try another bucket name.</p> |
| Obs.0010 | <p>Deletion failed. Check whether objects or objects of historical versions exist in the bucket.</p> |
| Obs.0011 | <p>The bucket policy is invalid. Configure it again.</p> |
| Obs.0012 | <p>The requested bucket name already exists. Bucket namespace is shared by all users in the system. Enter a different name and try again.</p> |
| Obs.0013 | <p>The requested folder name already exists. Enter a different name and try again.</p> |
| Obs.0014 | <p>The file size has exceeded 50 MB. Use OBS Browser+ to upload it.</p> |
| Obs.0015 | <p>The absolute path in the search criteria cannot exceed 1023 characters. Please retry.</p> |
| Obs.0016 | <p>Upload failed. Possible causes:</p> <ol style="list-style-type: none"> 1. The network is abnormal. 2. You have incorrect or no permissions to write the bucket. 3. Your account is in arrears or has insufficient balance. 4. Your account has been frozen. |
| Obs.0017 | <p>The end time of the new validity period must be later than that of the old validity period.</p> |
| Obs.0018 | <p>The validity period cannot be shorter than the remaining period.</p> |
| Obs.0019 | <p>Cannot determine whether the bucket has objects or fragments. Check whether you have the read permission for this bucket.</p> |
| Obs.0020 | <p>TMS system error. Try again later.</p> |
| Obs.0021 | <p>You do not have permissions to access TMS. Configure the required permissions in IAM.</p> |
| Obs.0022 | <p>The TMS system is busy. Try again later.</p> |

17 Change History

| Release Date | What's New |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2024-02-28 | <p>This issue is the thirty-third official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none">Added the content related to Deep Archive storage (under limited beta testing). |
| 2023-11-16 | <p>This issue is the thirty-second official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none">Added Manually and Permanently Deleting Objects from a WORM-Enabled Bucket and Using a Lifecycle Rule to Delete Objects from a WORM-Enabled Bucket in Configuring WORM Retention. |
| 2023-11-15 | <p>This issue is the thirty-first official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none">Optimized parameter descriptions in Configuring Static Website Hosting. |

| Release Date | What's New |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2023-10-25 | <p>This issue is the thirtieth official release.</p> <ul style="list-style-type: none"> ● Updated Viewing Basic Information of a Bucket. ● Updated Searching for an Object or Folder. ● Updated Creating a Bucket Policy with a Template. ● Updated Creating a Custom Bucket Policy (Visual Editor). ● Updated Configuring a Bucket ACL. ● Updated Configuring an Object ACL. ● Updated Figure 8-8. ● Added notes for passing HTTP headers in Configuring a Back-to-Source Rule. ● Updated the bucket policy configuration in Configuring Static Website Hosting. ● Optimized the structure and functions of the object and bucket lists. ● Updated the content related to deletion windows. |
| 2023-09-12 | <p>This issue is the twenty-ninth official release.</p> <ul style="list-style-type: none"> ● Put online decompression into commercial use. |
| 2023-09-06 | <p>This issue is the twenty-eighth official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none"> ● Optimized the constraints. |
| 2023-07-06 | <p>This issue is the twenty-seventh official release.</p> <p>This issue incorporates the following changes:</p> <ul style="list-style-type: none"> ● Added the descriptions about SSE-OBS. ● Adjusted the document structure. |
| 2023-05-05 | <p>This issue is the twenty-sixth official release.</p> <p>This issue incorporates the following changes:</p> <ul style="list-style-type: none"> ● Updated the content related to domain name management. ● Updated the content related to folder sharing by URL. |
| 2023-04-23 | <p>This issue is the twenty-fifth official release.</p> <ul style="list-style-type: none"> ● Added WORM-related sections. |
| 2023-01-19 | <p>This issue is the twenty-fourth official release.</p> <ul style="list-style-type: none"> ● Removed sections related to event notifications. |
| 2022-08-08 | <p>This issue is the twenty-third official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none"> ● Added descriptions about the back-to-source by mirroring. |

| Release Date | What's New |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2022-07-30 | <p>This issue is the twenty-second official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none"> • Added descriptions about online decompression. |
| 2021-05-19 | <p>This issue is the twenty-first official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none"> • Optimized the bucket policy configuration process. |
| 2020-02-04 | <p>This issue is the twentieth official release.</p> <p>This issue incorporates the following changes:</p> <ul style="list-style-type: none"> • Added descriptions about binding a user-defined domain name. |
| 2020-01-20 | <p>This issue is the nineteenth official release.</p> <p>This issue incorporates the following changes:</p> <ul style="list-style-type: none"> • Updated the description of IAM permissions. |
| 2019-11-30 | <p>This issue is the eighteenth official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none"> • Updated the description of operations for configuring fine-grained policies. |
| 2019-08-14 | <p>This issue is the seventeenth official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none"> • Added the function of synchronizing existing objects in cross-region replication. |
| 2019-07-18 | <p>This issue is the sixteenth official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none"> • Added the function of direct reading of data in the Archive storage class. |
| 2019-07-16 | <p>This issue is the fifteenth official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none"> • Added the bucket inventory function. |
| 2019-06-13 | <p>This issue is the fourteenth official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none"> • Added the function of batch upload of files. |
| 2019-05-22 | <p>This issue is the thirteenth official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none"> • Updated the description of permission control. |

| Release Date | What's New |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2019-04-19 | <p>This issue is the twelfth official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none"> • Added examples 3, 4, and 5 to section "Bucket Permissions." |
| 2019-02-27 | <p>This issue is the eleventh official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none"> • Added the user-defined domain name binding function. |
| 2019-02-22 | <p>This issue is the tenth official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none"> • Updated the procedures for basic configurations, including logging, tags, event notification, lifecycle rules, static website hosting, CORS rules, and URL validation. |
| 2019-02-19 | <p>This issue is the ninth official release.</p> <p>This issue incorporates the following change:</p> <ul style="list-style-type: none"> • Added the cross-region replication function. |
| 2018-11-30 | <p>This issue is the eighth official release.</p> <p>This issue incorporates the following changes:</p> <ul style="list-style-type: none"> • Updated the descriptions about GUI parameters of bucket information. • Updated the methods for configuring the versioning function. • Added the function for copying object URLs. • Added the section "Object Policy". |
| 2018-10-31 | <p>This issue is the seventh official release.</p> <p>This issue incorporates the following changes:</p> <ul style="list-style-type: none"> • Updated the section "Versioning Overview". • Updated the bucket logging parameters. • Added the note for folder-related event notifications. • Updated the screenshots based on changes in the GUI. |
| 2018-08-13 | <p>This issue is the sixth official release.</p> <p>This issue incorporates the following changes:</p> <ul style="list-style-type: none"> • Updated the description about the bucket policy description and bucket policy configuration. • Added the cloud trace service. • Added the tag function. • Updated the screenshots based on changes in the GUI. |

| Release Date | What's New |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2018-06-08 | <p>This issue is the fifth official release.</p> <p>This issue incorporates the following changes:</p> <ul style="list-style-type: none"> ● Added the session: Cloud Eye Monitoring Metrics. ● Updated the screenshots based on changes in the GUI. |
| 2018-05-31 | <p>This issue is the fourth official release.</p> <p>This issue incorporates the following changes:</p> <ul style="list-style-type: none"> ● Added the procedure of canceling a file deletion after versioning is enabled. ● Added the description about operations on file versions when versioning is enabled. ● Added a screenshot to the procedure of creating a key. ● Updated the description about the bucket and object ACL. ● Updated the description about the redirection. ● Updated the screenshots based on changes in the GUI. |
| 2018-3-20 | <p>This issue is the third official release.</p> <p>This issue incorporates the following changes:</p> <ul style="list-style-type: none"> ● Added object storage classes. ● Added the functions of changing bucket and object storage classes. ● Updated the screenshots based on changes in the GUI. |
| 2018-01-19 | <p>This issue is the second official release.</p> <p>This issue incorporates the following changes:</p> <ul style="list-style-type: none"> ● Added the section of "Accessing OBS with Domain Names". ● Added the section of "Time Difference Is Longer Than 15 Minutes Between the Client and Server". ● Added error codes. ● Updated the method of obtaining AK/SK, account ID, and user ID. ● Updated the description about the ACL. |
| 2017-12-31 | <p>This issue is the first official release.</p> |