

Object Storage Service

Console Operation Guide

Issue 01
Date 2024-08-27



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	3
3 Getting Started	4
3.1 Process Description	4
3.2 Configuring User Permissions	5
3.3 Logging In to OBS Console	6
3.4 Creating a Bucket	7
3.5 Uploading an Object	10
3.6 Downloading an Object	12
3.7 Deleting an Object	13
3.8 Deleting a Bucket	13
4 Managing Buckets	15
4.1 Creating a Bucket	15
4.2 Viewing Basic Information of a Bucket	18
4.3 Searching for a Bucket	20
4.4 Deleting a Bucket	21
5 Managing Objects	22
5.1 Uploading an Object	22
5.2 Downloading an Object	25
5.3 Managing Folders	25
5.3.1 Creating a Folder	25
5.4 Other Object Operations	26
5.4.1 Listing Objects	26
5.4.2 Searching for an Object or Folder	27
5.4.3 Accessing an Object Using Its URL	27
5.4.4 Sharing an Object	28
5.4.5 Restoring an Object from Archive Storage	30
5.4.6 Configuring Direct Reading	32
5.4.7 Configuring Object Metadata	33
5.5 Deleting Objects	34
5.5.1 Deleting an Object or Folder	34
5.5.2 Undeleting an Object	37

5.5.3 Managing Fragments.....	40
6 Permissions Control.....	41
6.1 Configuring IAM Permissions.....	41
6.1.1 Creating an IAM User and Granting OBS Permissions.....	41
6.1.2 OBS Custom Policies.....	42
6.1.3 OBS Resources.....	45
6.1.4 OBS Request Conditions.....	46
6.2 Configuring a Bucket Policy.....	46
6.2.1 Creating a Bucket Policy with a Template.....	46
6.2.2 Creating a Custom Bucket Policy (Visual Editor).....	48
6.2.3 Creating a Custom Bucket Policy (JSON View).....	50
6.3 Configuring an Object Policy.....	52
6.4 Configuring a Bucket ACL.....	52
6.5 Configuring an Object ACL.....	53
7 Data Management.....	55
7.1 Configuring a Lifecycle Rule.....	55
7.2 Configuring Tags for a Bucket.....	58
7.3 Configuring a Bucket Inventory.....	59
7.4 Configuring Event Notifications.....	62
7.4.1 Configuring SMN-Enabled Event Notification.....	62
7.4.2 Application Example: Configuring SMN-Enabled Event Notification.....	65
8 Data Access.....	68
8.1 Static Website Hosting.....	68
8.1.1 Configuring Static Website Hosting.....	68
8.1.2 Configuring Redirection.....	73
8.2 Configuring a User-Defined Domain Name.....	75
9 Data Security.....	78
9.1 Configuring Server-Side Encryption.....	78
9.1.1 Configuring Bucket Server-Side Encryption.....	78
9.1.2 Enabling Server-Side Encryption When Uploading an Object.....	79
9.2 Configuring CORS.....	81
9.3 Configuring Versioning.....	84
9.4 Configuring URL Validation.....	87
10 Monitoring and Logging.....	89
10.1 Monitoring.....	89
10.1.1 Monitoring OBS.....	89
10.1.2 OBS Monitoring Metrics.....	90
10.2 Cloud Trace Service.....	92
10.3 Configuring Access Logging for a Bucket.....	95
11 Task Center.....	98

12 Related Operations.....	99
12.1 Creating an Agency.....	99
13 Troubleshooting.....	102
13.1 An Object Fails to Be Downloaded Using Internet Explorer 11.....	102
13.2 OBS Console Couldn't Be Opened in Internet Explorer 9.....	102
13.3 The Object Name Changes After an Object with a Long Name Is Downloaded to a Local Computer	103
13.4 Time Difference Is Longer Than 15 Minutes Between the Client and Server.....	104
14 Error Code List.....	105

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), 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.
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.
Fragment management	Manages and clears fragments generated due to object upload failures.

Function	Description
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.
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.
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).
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

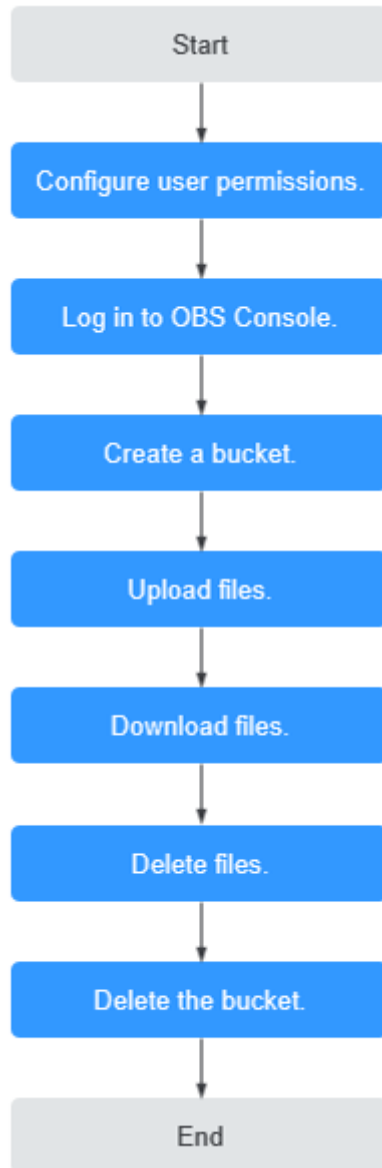
3 Getting Started

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



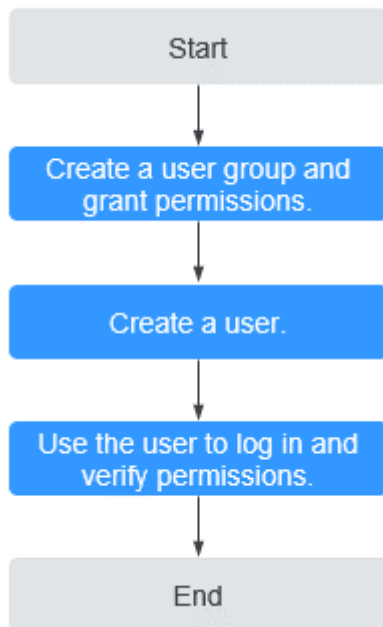
3.2 Configuring User Permissions

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 bar, click **Sign Up**.
2. Complete the creation as instructed.

After the creation is complete, you will be navigated to your 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

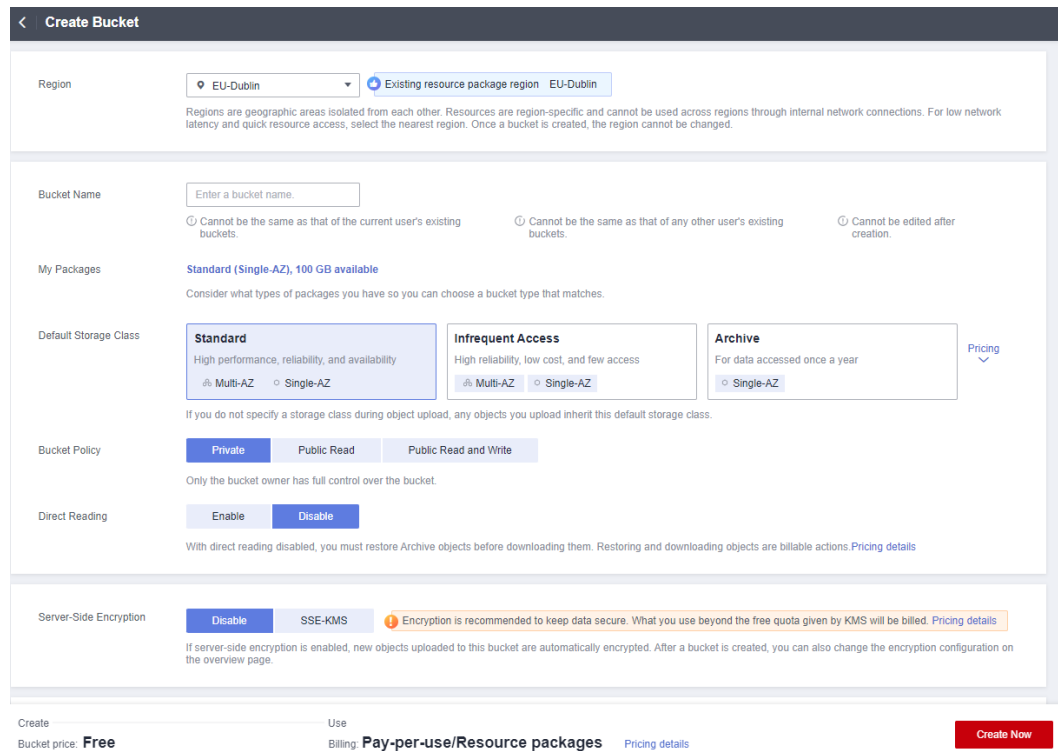
An account (including all IAM users under this account) can create a maximum of 100 buckets and parallel file systems. You can use the fine-grained access control of OBS to properly plan and use buckets. For example, you can create folders in a bucket based on object prefixes and use [fine-grained permission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

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>
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. <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>After you enable server-side encryption for the bucket, any object you upload to it will inherit the KMS encryption from the bucket by default.</p> <p>After you enable server-side encryption for the bucket, any object you upload to it will be encrypted with the obs/default key by default. You can also click Create KMS Key to create a key on the DEW console. Then select the created key on OBS Console for encryption.</p>

Parameter	Description
Direct Reading	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 . 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.
Tags	Optional. Tags are used to identify and classify buckets in OBS. Each tag is represented by a key-value pair. For more information, see Tags .

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 that support batch uploads, a maximum of 100 files can be uploaded at a time, with a total size of no more than 5 GB.
- In regions that do not support batch uploads, only one file can be uploaded at a time, with a size of no more than 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.

OBS Browser+ allows you to upload up to 500 files at a time. There is no limit on the number of files you can upload using obsutil at a time.

NOTE

Batch upload is available only when the following condition is met:

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.

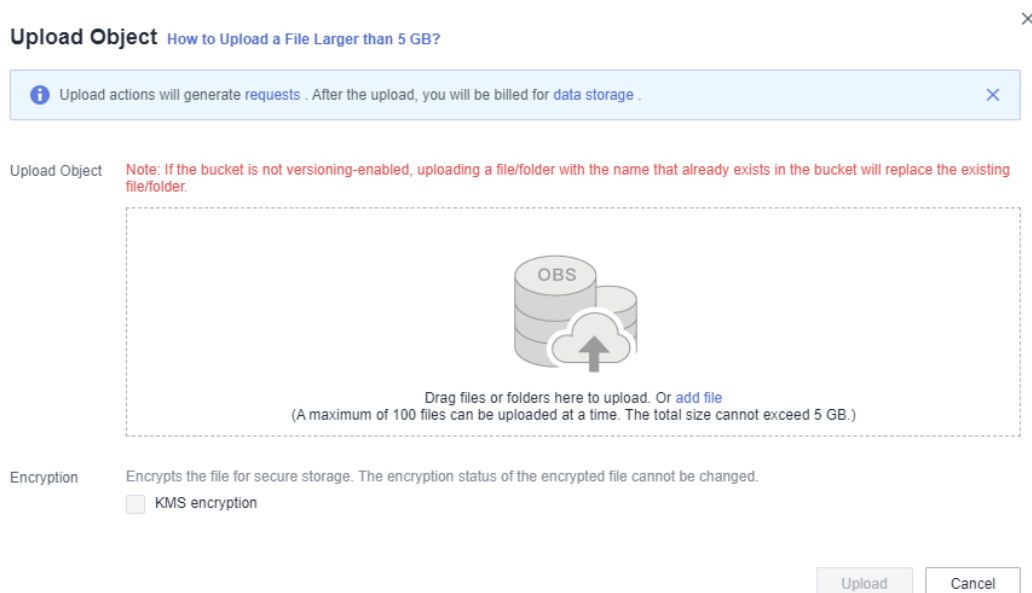
Step 3 Go to the folder where you want to upload files and click **Upload Object**. The **Upload Object** dialog box is displayed.

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** to select files.

Step 6 (Optional) Select **KMS encryption** to encrypt the uploaded file. For details, see [Enabling Server-Side Encryption When Uploading an Object](#).

 **NOTE**

If the bucket has server-side encryption enabled, any object you upload will inherit the KMS encryption from the bucket by default.

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

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**.

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 storage class can be downloaded only when they are in the **Restored** state.

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.

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 **Yes** to confirm the deletion.

----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 **Yes** to confirm the deletion.

----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.

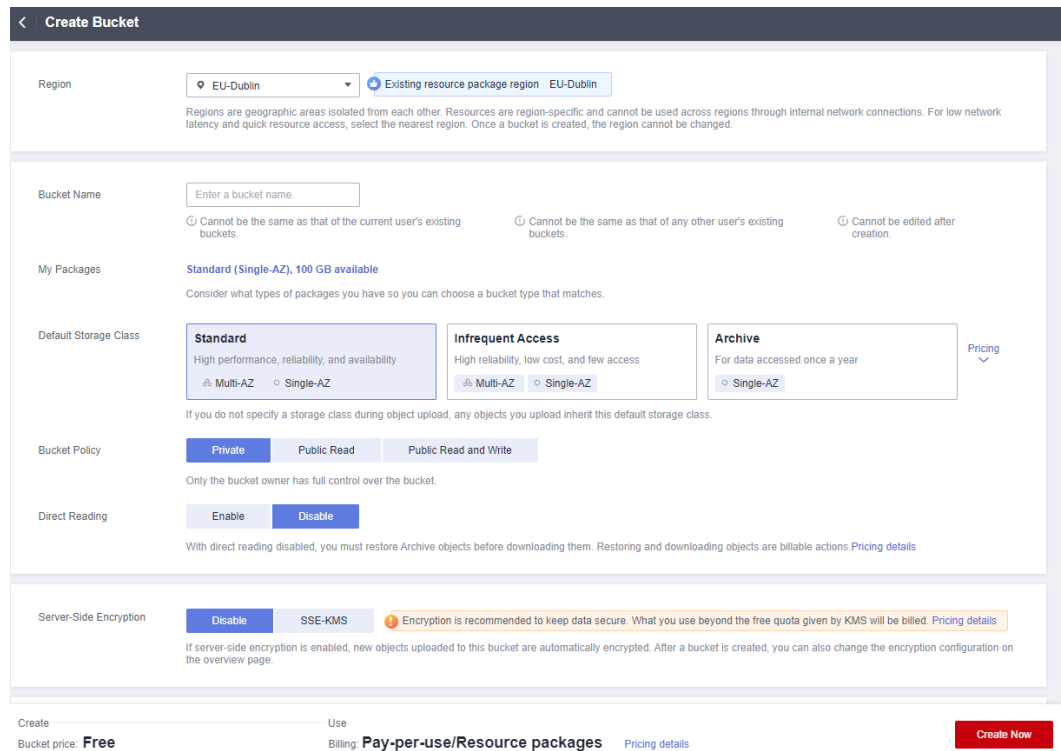
 **NOTE**

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 isolate permissions 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
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.

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>
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. <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>After you enable server-side encryption for the bucket, any object you upload to it will inherit the KMS encryption from the bucket by default.</p> <p>After you enable server-side encryption for the bucket, any object you upload to it will be encrypted with the obs/default key by default. You can also click Create KMS Key to create a key on the DEW console. Then select the created key on OBS Console for encryption.</p>

Parameter	Description
Direct Reading	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 . 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.
Tags	Optional. Tags are used to identify and classify buckets in OBS. Each tag is represented by a key-value pair. For more information, see Tags .

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 details about a bucket, including basic bucket information and configurations.

Procedure

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

Step 2 In the bucket list, click the bucket name you want. The **Objects** page is displayed.

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

Step 4 Under **Basic Information**, view the basic bucket information.

Figure 4-2 Basic information about the bucket

Basic Information

Bucket Name	eu-dublin-test
Storage Class	Standard
Bucket Version	3.0
Region	EU-Dublin
Used Capacity ?	251 bytes
Objects ?	1
Account ID	e[REDACTED].b
Created	Mar 17, 2023 15:14:02 GMT+08:00
Versioning ?	Enabled Edit
Endpoint ?	obs.eu-west-101.myhuaweicloud.eu
Access Domain Name ?	eu-dublin-test.obs.eu-west-101.myhuaweicloud.eu 📄
Enterprise Project	default
Storage Limitation	Unlimited Edit

Table 4-2 Parameter description

Parameter	Description
Bucket Name	Name of the bucket.
Storage Class	Storage class of the bucket, which can be Standard , Infrequent Access , or Archive .

Parameter	Description
Bucket Version	Version number of the bucket. 3.0 indicates the latest bucket version, and -- indicates versions earlier than 3.0.
Region	Region where the bucket resides.
Owner	Owner refers to the account that created the bucket.
Account ID	Unique identity of the bucket owner. It is the same as Account ID on the My Credentials page.
Created	Time when the creation of a bucket is completed.
Versioning	Versioning status
Endpoint	This parameter specifies the endpoint of the region where the bucket is located. OBS provides an endpoint for each region. An endpoint is a domain name to access OBS in a region and is used to process access requests of that region.
Access Domain Name	OBS assigns each bucket with a default domain name. A domain name is the address of a bucket on the Internet. It can be used to access a bucket over the Internet in scenarios such as cloud application development and data sharing. Structure: <i>BucketName.Endpoint</i>

 **NOTE**


The statistics of **Used Capacity** and **Objects** are not real-time data, which are usually updated 15 minutes in delay.

----End


4.3 Searching for a Bucket

You can search for a bucket by characters contained in its name.

Procedure

- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the search box at the upper right corner above the bucket list, enter characters contained in the name of the desired bucket.
- Step 3** Click  .

Buckets that meet the search criteria are displayed in the bucket list.

For example, if you want to search for buckets whose names contain **test**, you only need to enter **test** in the search box and click  . Then, all buckets that contain **test** in their names are displayed.

----End

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 **Yes** to confirm the deletion.

----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 that support batch uploads, a maximum of 100 files can be uploaded at a time, with a total size of no more than 5 GB.
- In regions that do not support batch uploads, only one file can be uploaded at a time, with a size of no more than 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.

OBS Browser+ allows you to upload up to 500 files at a time. There is no limit on the number of files you can upload using obsutil at a time.

NOTE

Batch upload is available only when the following condition is met:

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.

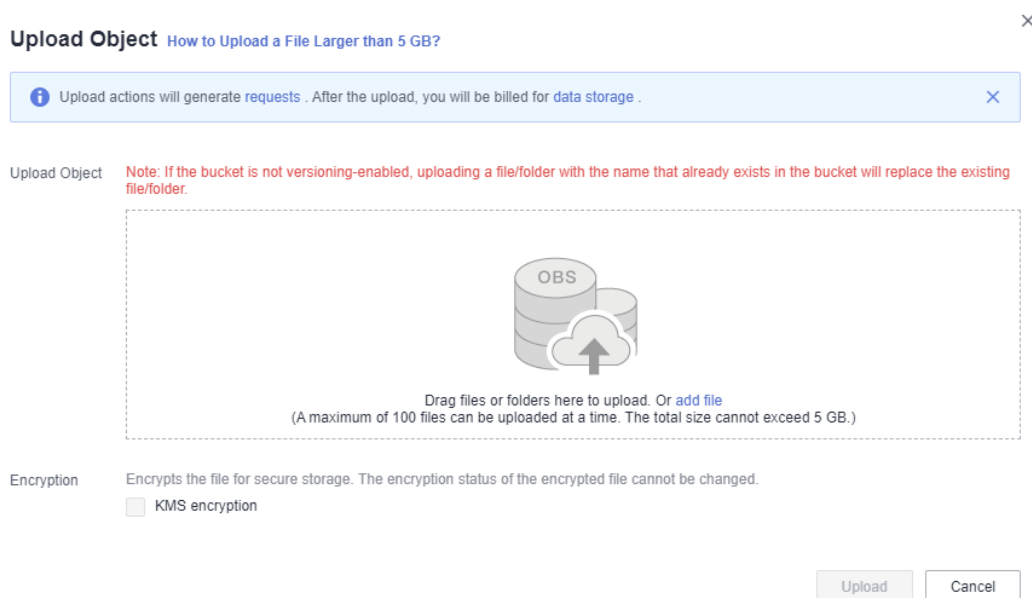
Step 3 Go to the folder where you want to upload files and click **Upload Object**. The **Upload Object** dialog box is displayed.

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** to select files.

Step 6 (Optional) Select **KMS encryption** to encrypt the uploaded file. For details, see [Enabling Server-Side Encryption When Uploading an Object](#).

 **NOTE**

If the bucket has server-side encryption enabled, any object you upload will inherit the KMS encryption from the bucket by default.

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

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**.

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 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. Changing objects from Infrequent Access or Archive to other storage classes incurs restore costs. Select an appropriate change option based on your actual needs.
 - From Standard to Infrequent Access, Archive
 - From Infrequent Access to Standard, Archive
 - From Archive to Standard, Infrequent Access. Before changing Archive objects, you must restore them first.
- 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 storage class can be downloaded only when they are in the **Restored** state.

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.

5.4 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 prefix.

Searching by Prefixes of Object Names

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 search box above the object list, enter the name prefix of the file or folder that you want to search for.

In the root directory of the bucket, files and folders whose name starts with the specified prefix are displayed.

NOTE


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

- In the search box of the root directory, enter *folder path/object name prefix*. 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 4 Click  . The search results are displayed in the object list.

----End

Related Operations

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

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 5-2](#).

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 5-2 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 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.eu-west-101.myhuaweicloud.eu: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.

Procedure

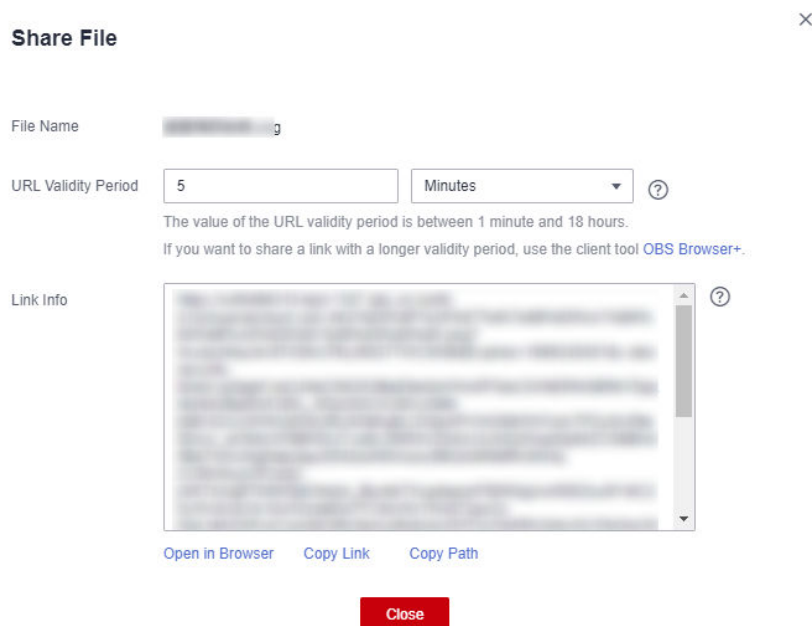
Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

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 5-3 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 Storage

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

Constraints

- If an 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 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

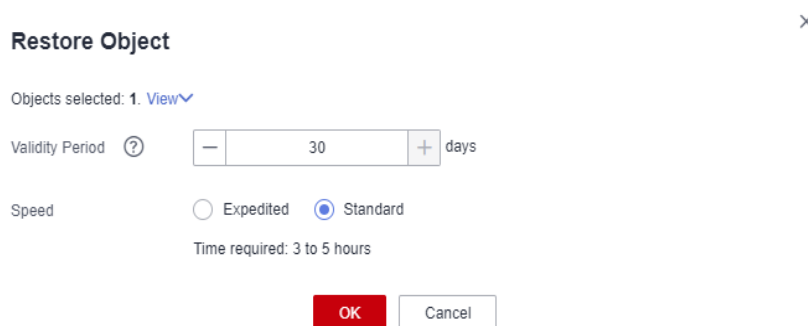
- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** Select the file you want to restore, and click **Restore** on the right. The following dialog box shown in **Figure 5-4** 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 5-4 Restoring an object




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

Table 5-1 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. ● Standard: Archive objects can be restored within 3 to 5 hours.

- Step 5** Click **OK**.

The **Restoration Status** column in the object list displays the restore statuses of objects.

You can click  to manually refresh the restore status.

 **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

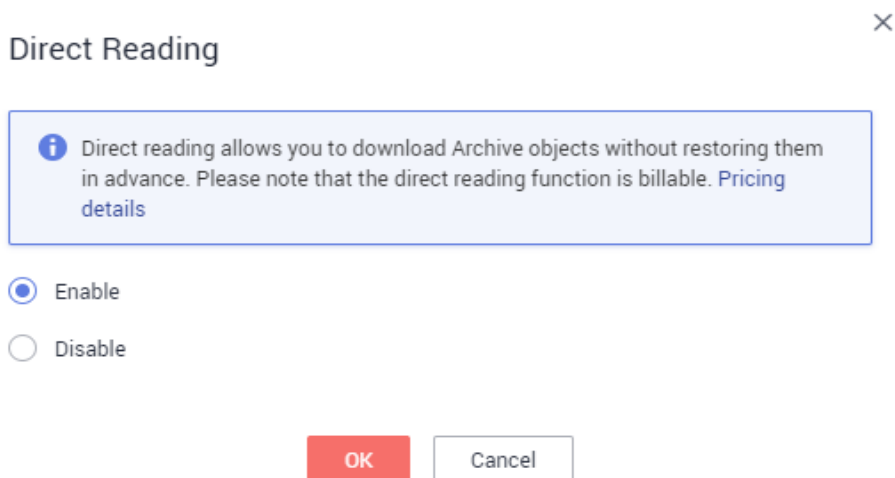
With direct reading enabled for a bucket, you can access objects in the Archive storage class without restoring them first. Downloading or copying Archive objects will incur costs for directly reading these objects. For details, see [Product Pricing Details](#).

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:

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 5-5 Enabling direct reading



Step 6 Click **OK**.

----End

5.4.7 Configuring Object Metadata

Procedure

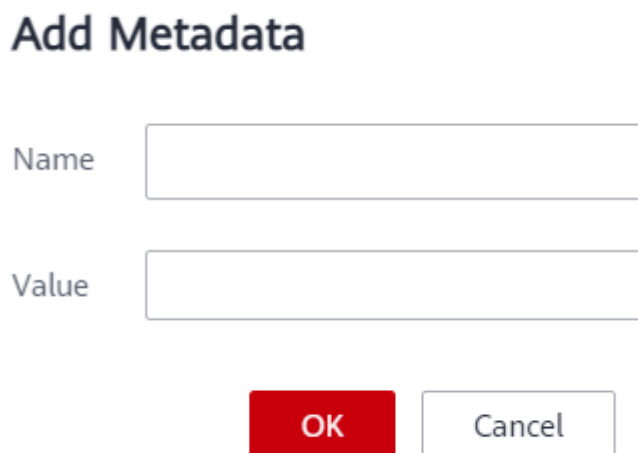
Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

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 5-6](#).

Figure 5-6 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.

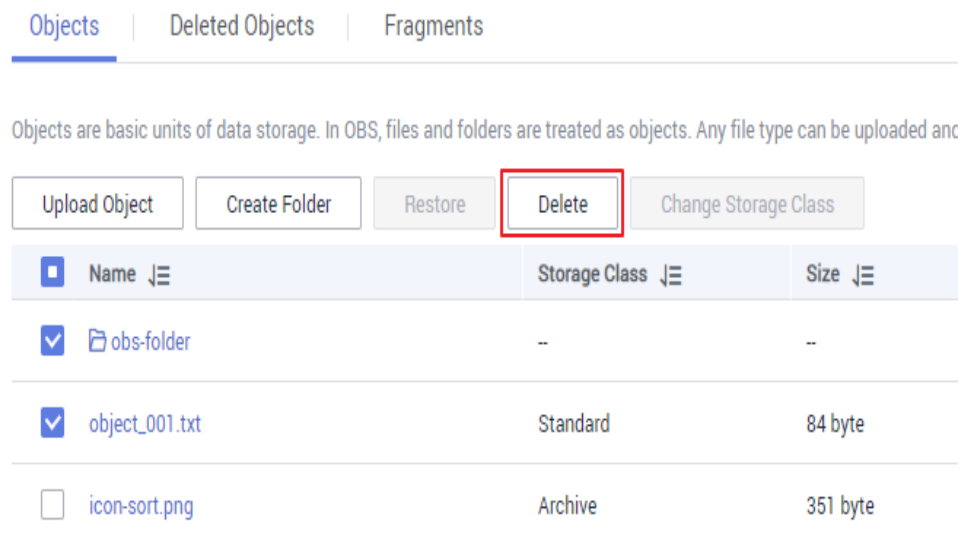
Background Information

Object Deletion with Versioning Enabled

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

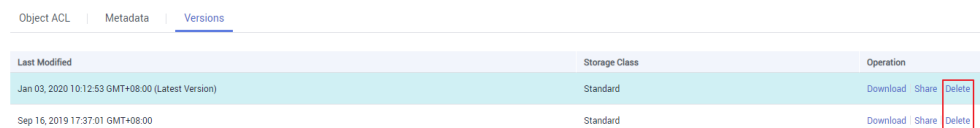
- Deleting a file or folder: The file or folder is not permanently deleted, but is retained in the **Deleted Objects** list and marked with the **Delete Marker**. In **Deleted Objects**, click the object name. On the **Versions** tab, you can see that the latest object version has the delete marker.

Figure 5-7 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 5-8 Deleting a version of an object

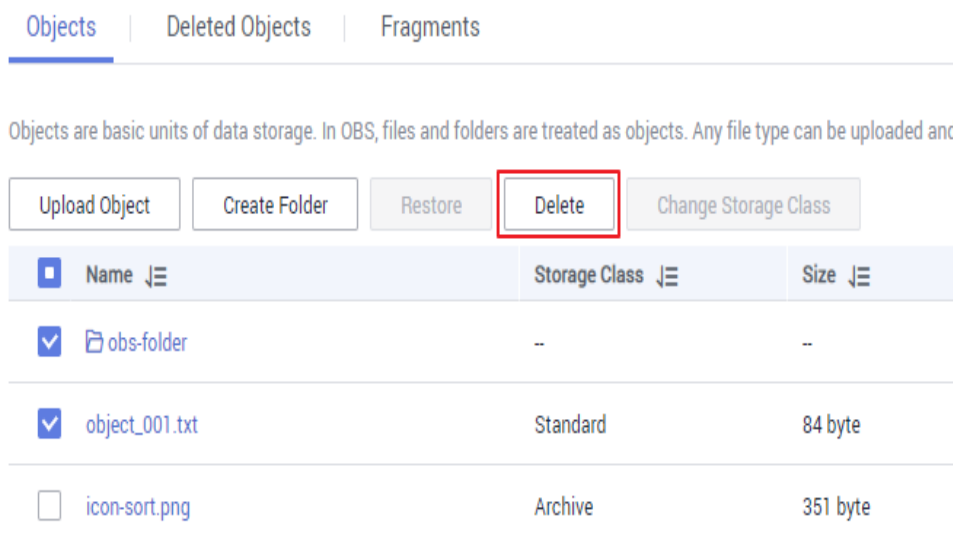


Procedure

- 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 5-9 Deleting a file or folder



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

CAUTION

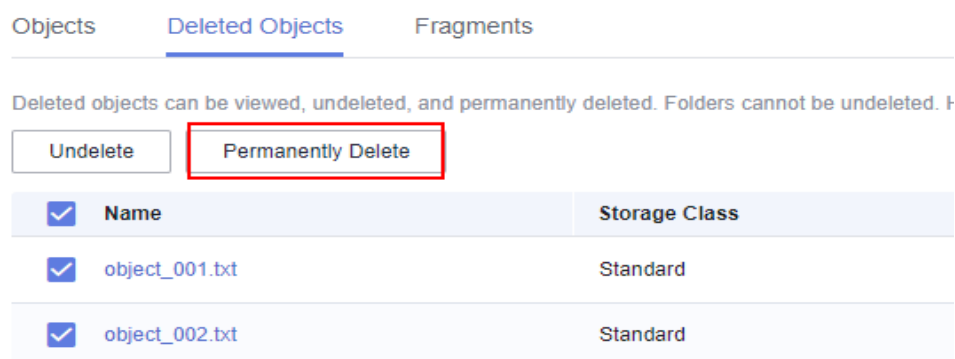
If you delete an object from a bucket with versioning enabled, the object is not permanently deleted but retained in the **Deleted Objects** list. All versions of the object are still kept in the bucket and are billed for storage. If you need to permanently delete the object, see the following steps.

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

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 5-10 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 5-11 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	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.

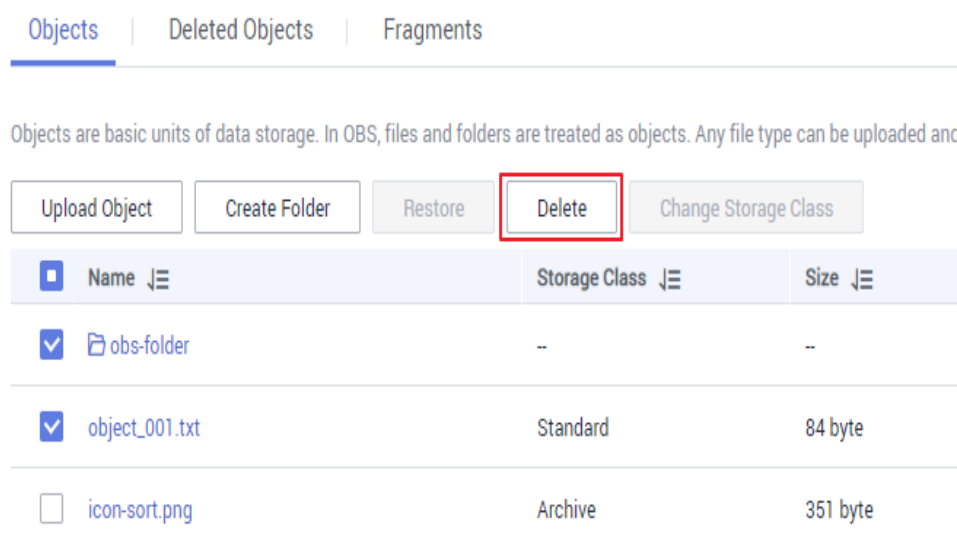
Background Information

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 5-12 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 5-13 Deleting a version of an object

Last Modified	Storage Class	Operation
Jan 03, 2020 10:12:53 GMT+08:00 (Latest Version)	Standard	Download Share Delete
Sep 16, 2019 17:37:01 GMT+08:00	Standard	Download Share Delete

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 5-14 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	Download Share Delete

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**.

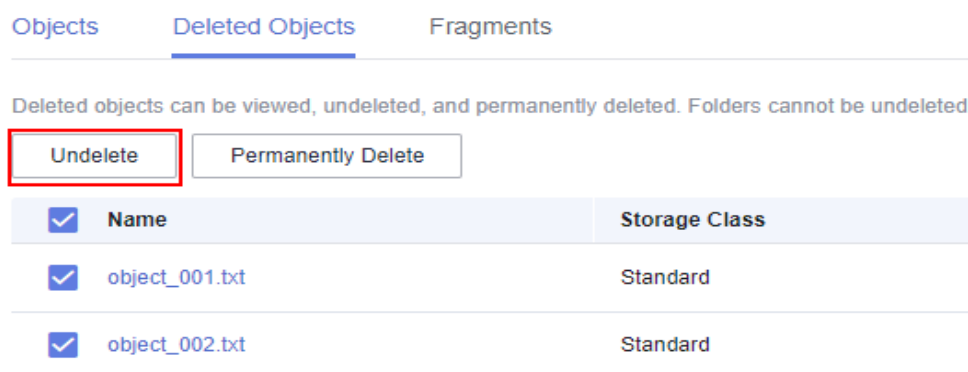
Step 2 In the bucket list, click the bucket you want to operate to go to the **Objects** page.

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 5-15 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 5-16 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	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.

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 **Yes** to confirm the deletion.

----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.

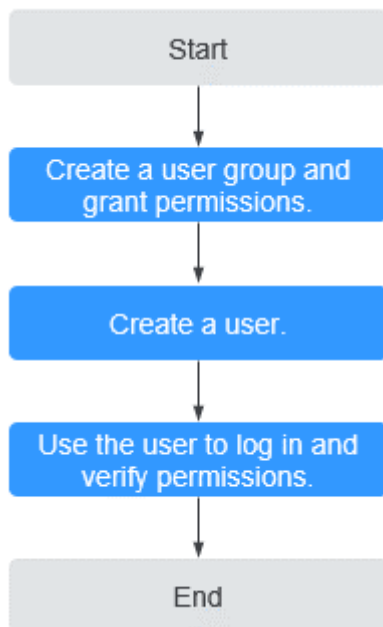
[Figure 6-1](#) shows the procedure for granting permissions.

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 global, while CTS and KMS are regional. 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 actions of all services, while service-level condition keys (starting with a service name acronym like **obs:**) are available only for actions 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 six typical scenarios. You can use these templates to quickly configure bucket policies.

Procedure

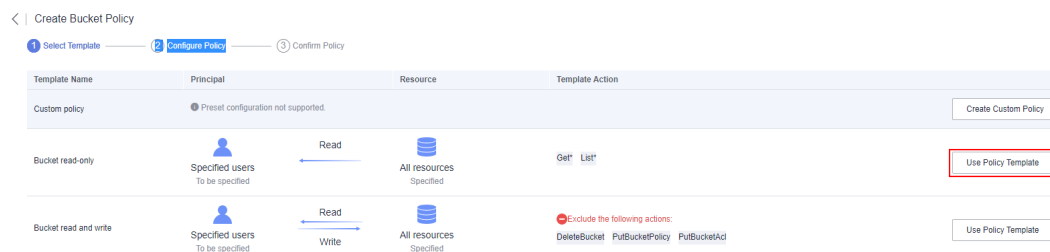
- Step 1** In the navigation pane of [OBS Console](#), choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** In the navigation pane, choose **Permissions > Bucket Policy**.

Step 4 Click **Create Bucket Policy**.

Step 5 In the template list, select a template and click **Use Policy Template** on the right.

For details about each template, see [Bucket Policy](#).

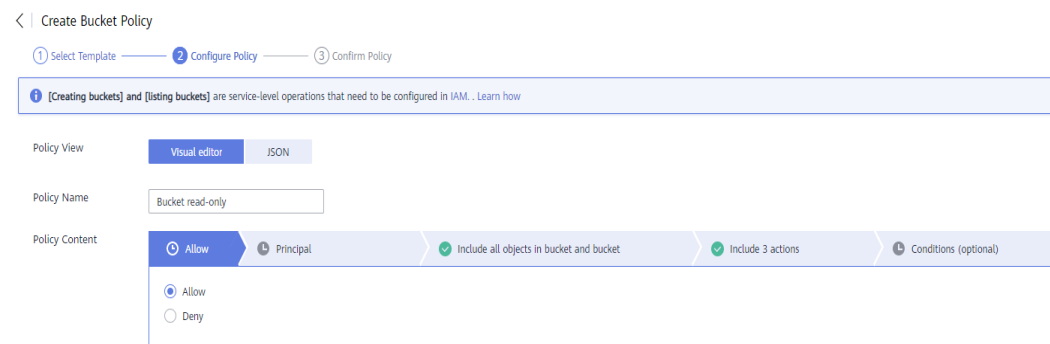
Figure 6-2 Creating a bucket policy using a template



Step 6 Input required information.

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

Figure 6-3 Configuring a bucket policy



Step 7 Click **Next** to confirm the policy configuration.

Figure 6-4 Confirming a bucket policy configuration



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

-----End

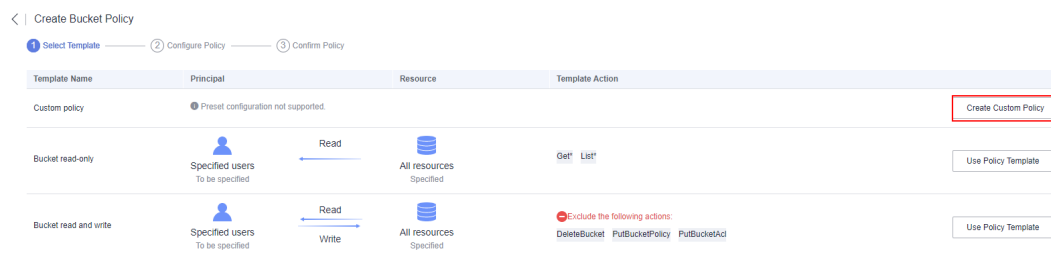
6.2.2 Creating a Custom Bucket Policy (Visual Editor)

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 Policy**.
- Step 4** Click **Create Bucket Policy**.
- Step 5** In the first row of the template list, click **Create Custom Policy** on the right.

Figure 6-5 Creating a custom policy



- Step 6** Configure a bucket policy.

Figure 6-6 Configuring a bucket policy

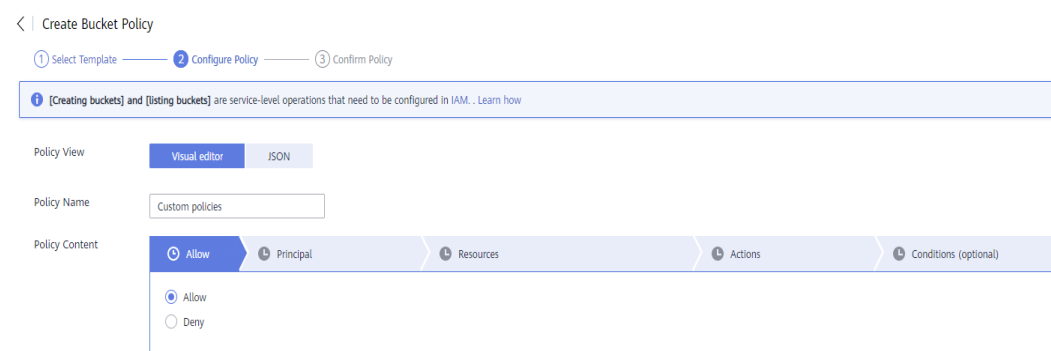


Table 6-2 Parameters for configuring a custom bucket policy

Parameter	Description
Policy View	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.

Parameter		Description
Policy Content	Effect	<ul style="list-style-type: none"> ● Allow: The policy allows the matched requests. ● Deny: The policy denies the matched requests.
	Principal	<ul style="list-style-type: none"> ● Configure authorized users: <ul style="list-style-type: none"> – Current account: Specify one or more IAM users under the current account. – Other account: Specify one or more other account IDs. If you want to grant access only to the IAM users under an account, you also need to enter one or more IAM user IDs. – Anonymous user: Grant the bucket policy to anyone. ● Select a user policy. <ul style="list-style-type: none"> – Include specified users: The bucket policy takes effect on specified users. – Exclude specified users: The bucket policy takes effect on users other than the specified ones.
	Resources	<ul style="list-style-type: none"> ● Select resource scope: <ul style="list-style-type: none"> – Current bucket: The policy applies to the current bucket. You can configure bucket actions in this policy. – Objects in bucket: The bucket policy applies to objects in the bucket. You can configure object-related actions. You can specify an object or a set of objects in the following formats: Object: <i>Object name</i> Object set: <i>Object name prefix*</i>, <i>*Object name suffix</i>, or <i>*</i> ● Select a resource policy. <ul style="list-style-type: none"> – Include specified resources: The bucket policy takes effect on specified resources. – Exclude specified resources: The bucket policy takes effect on resources other than the specified ones.

Parameter		Description
	Actions	<ul style="list-style-type: none"> • Select the actions you want to grant. For details about the actions, see Bucket Policy Parameters. <ul style="list-style-type: none"> – If only Current bucket is selected for Resource, you can configure common actions and bucket actions. – If only Objects in bucket is selected for Resource, you can configure common actions and object actions. – If you select both Current bucket and Objects in bucket for Resource, you can configure common actions, bucket actions, and object actions. • Select an operation strategy for the selected actions: <ul style="list-style-type: none"> – Include selected: The bucket policy takes effect on selected actions. – Exclude selected: The bucket policy takes effect on all actions except the selected ones.
	Conditions (optional)	<ul style="list-style-type: none"> • Conditional Operator: See Bucket Policy Parameters. • Key: See Bucket Policy Parameters. • Value: The entered value is associated with the key.

Step 7 Click **Next** to confirm the policy configuration.

Step 8 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 6-3 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 .
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 **Save**.

----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.

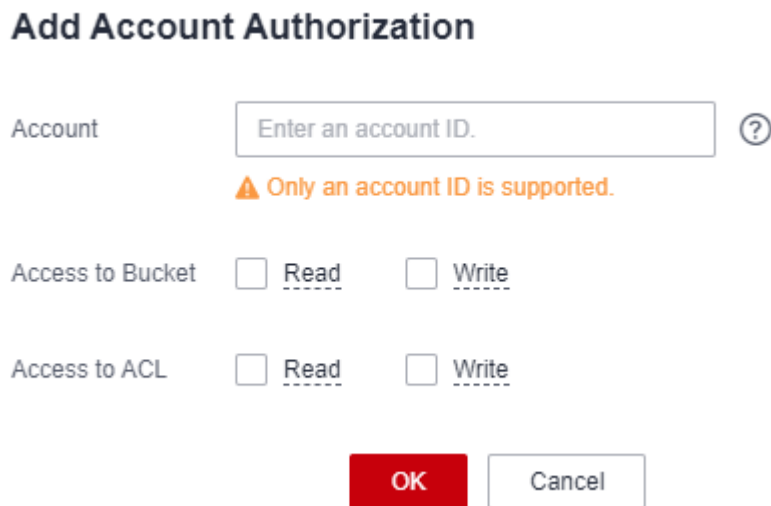
Step 3 In the navigation pane, choose **Permissions > Bucket ACLs**.

Step 4 Under **Bucket ACLs**, click **Edit** to grant the owner, anonymous user, and log delivery user required permissions for the bucket.

Step 5 Click **Add** to apply specific ACL permissions to an account, as shown in [Figure 6-7](#).

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

Figure 6-7 Granting permissions



Add Account Authorization

Account ?

⚠ Only an account ID is supported.

Access to Bucket Read Write

Access to ACL Read Write

OK Cancel

Step 6 Click **OK**.

----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

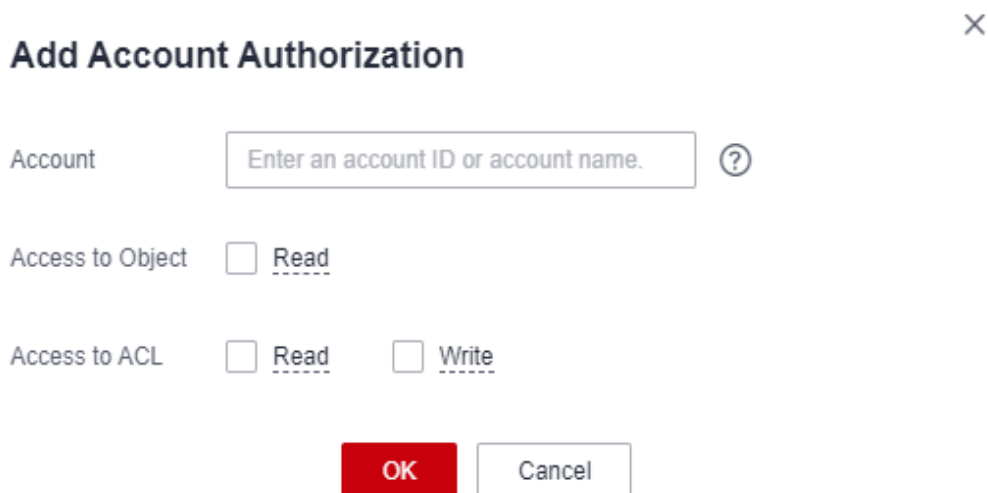
- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3** Click the object to be operated.
- Step 4** On the **Object ACL** tab page, click **Edit** to grant the owner and anonymous user ACL permissions for the object.

NOTE

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

- Step 5** Click **Add** to apply specific ACL permissions to an account, as shown in **Figure 6-8**. Enter an account ID or account name and specify ACL permissions for the account. You can obtain the account ID or account name from the **My Credentials** page.

Figure 6-8 Adding ACL permissions for an object



Add Account Authorization ×

Account ?

Access to Object Read

Access to ACL Read Write

OK

- Step 6** Click **OK**.
- 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.
- Transition objects from Infrequent Access to Archive.
- Expire objects and then delete 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 **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

Create Lifecycle Rule [Learn more](#)
×

i In a lifecycle rule, the required minimum storage period for objects in the Infrequent Access, or Archive storage class is 30, or 90 days respectively. If they are stored for less time than this minimum, you will be billed for the full minimum storage period. ×

Once a lifecycle rule is enabled, objects under the rule will be transitioned to the specified storage class or deleted automatically after the specified expiration time. As a result, your costs may change due to changes of storage space and storage classes. [Pricing details](#)

Basic Information

Status Enable Disable

Rule Name

Prefix ?

Current Version

Transition to Infrequent Access After (Days) ?

Transition to Archive After (Days) ?

OK
Cancel

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.
- **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 an integer 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.

 NOTE

The object update time refers to when common objects were uploaded or when historical objects became historical.

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. After an object is updated, OBS calculates its lifecycle from the next 00:00 (UTC time), so there may be a delay of up to 48 hours in transitioning objects between storage classes or deleting expired objects. 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

Follow-up Procedure

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

You can also select multiple lifecycle rules at a time and click **Delete** or **Disable** (or **Enable**) above the list to batch delete or disable (or enable) them.

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.

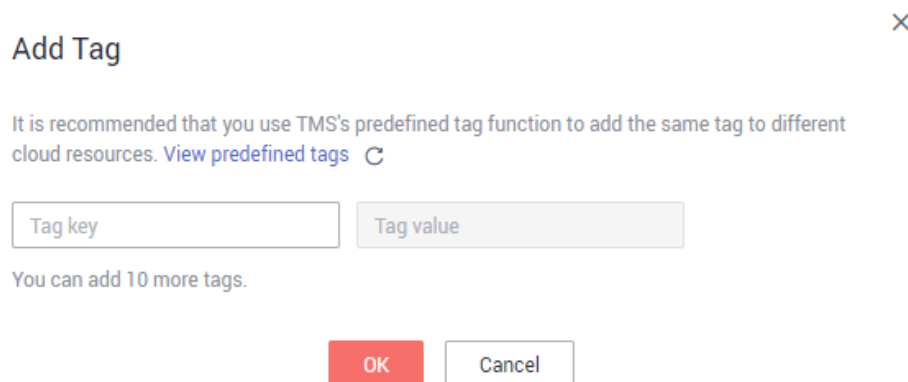
Step 3 In the navigation pane, choose **Overview**.

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 7-2](#) for details.

Figure 7-2 Add Tag



Add Tag ×

It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. [View predefined tags](#) 

Tag key Tag value

You can add 10 more tags.

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 7-3 Inventory settings

Create Inventory

① Configure Policy ——— ② Configure Report ——— ③ Confirm Bucket Policy

Inventory Name:

Filter: ?

Save Inventory Files To: C ?

Inventory File Name Prefix: ?

Frequency: Daily Weekly

Status: Enable Disable

Step 5 Configure required parameters.

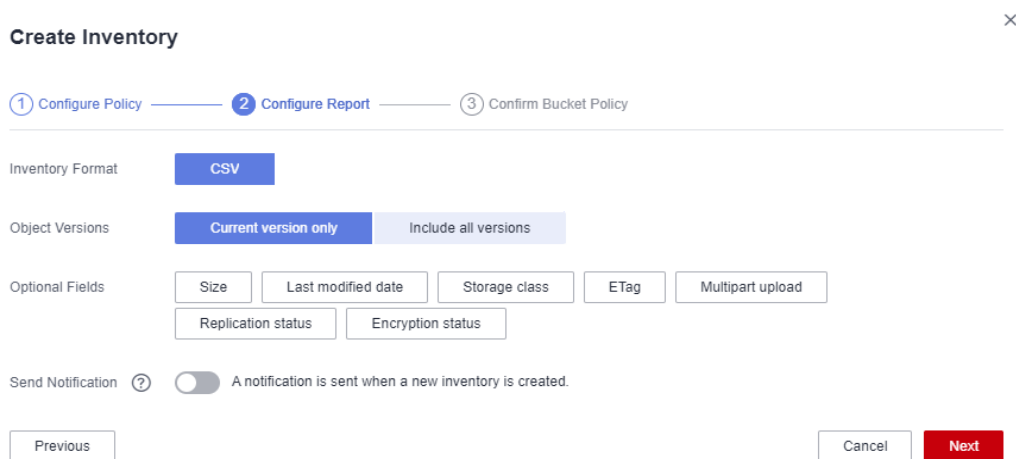
Table 7-2 Parameters for configuring a bucket inventory

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.
Frequency	How frequently inventory files are generated. It can be set to Daily or Weekly .

Parameter	Description
Status	Inventory status. You can enable or disable the generation of inventories.

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

Figure 7-4 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 .
Send Notification	If there is a new inventory file generated, a notification will be sent to the email address or mobile number specified in the SMN topic. If you enable the notification function, an SMN event notification rule will be created in the bucket where inventory files are stored. You can view details about the rule on the Event Notification page of the bucket. If you disable the notification function or modify the SMN topic, the SMN event notification rule will also be deleted or modified.

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 Configuring Event Notifications

7.4.1 Configuring SMN-Enabled Event Notification

This section describes how to configure an SMN-enabled event notification rule on OBS Console.

Background Information

For details, see [Event Notifications](#).

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 **Event Notification**. The **Event Notification** page is displayed.

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

Step 5 Click **Create**. The **Create Event Notification** dialog box is displayed. See [Figure 7-5](#) for details.

Figure 7-5 Creating an event notification rule

Create Event Notification
×

Name ?

Events ?

Prefix ?

Suffix ?

Notification Method SMN topic ?

C

C [Create Topic](#)

Step 6 Configure event notification parameters, as described in [Table 7-4](#).

Table 7-4 Event notification parameters

Parameter	Description
Name	Name of the event. If the event name is left blank, the system will automatically assign a globally unique ID.

Parameter	Description
Events	<p>Various types of events. Currently, OBS supports event notification for the following types of events:</p> <ul style="list-style-type: none"> ● ObjectCreated: all kinds of object creation operations, including PUT, POST, COPY, and part assembling <ul style="list-style-type: none"> – Put: Creates or overwrites an object using the PUT method. – Post: Creates or overwrites an object using the POST (browser-based upload) method. – Copy: Creates or overwrites an object using the COPY method. – CompleteMultipartUpload: Assembles parts of a multipart upload. ● ObjectRemoved: Deletes an object. <ul style="list-style-type: none"> – Delete: Deletes an object with a specified version ID. – DeleteMarkerCreated: Deletes an object without specifying a version ID. <p>Multiple event types can be applied to the same object. For example, if you have selected Put, Copy, and Delete in the same event notification rule, a notification will be sent to you when the specified object is uploaded to, copied to, or deleted from the bucket. ObjectCreated contains Put, Post, Copy, and CompleteMultipartUpload. If you select ObjectCreated, the events ObjectCreated contains are automatically selected. Similarly, if you select ObjectRemoved, Delete and DeleteMarkerCreated are automatically selected.</p>
Prefix	<p>Object name prefix for which notifications will be triggered.</p> <p>NOTE If neither the Prefix nor the Suffix is configured, the event notification rule applies to all objects in the bucket.</p>
Suffix	<p>Object name suffix for which notifications will be triggered.</p> <p>NOTE</p> <ul style="list-style-type: none"> ● A folder path ends with a slash (/). Therefore, if you want to configure event notification rules for operations on folders and you need to filter folders by suffix, the suffix must also end with a slash (/). ● If neither the Prefix nor the Suffix is configured, the event notification rule applies to all objects in the bucket.

Parameter	Description
SMN Topic	<p>Project: The project that contains the SMN topic you want to select.</p> <p>Projects are used to manage and classify cloud resources, including SMN topics. Each project contains different SMN topics. Select a project first and then a topic.</p>
	<p>Topic: specifies the SMN topic that authorizes OBS to publish messages. You can create such topics on the SMN management console.</p> <p>NOTE</p> <ul style="list-style-type: none"> Once SMN topics are selected for pushing OBS event notifications, do not delete them or cancel their authorizations to OBS. If the topics are deleted or their authorizations to OBS are canceled, the following conditions may occur: <ul style="list-style-type: none"> a. The subscriber of the topic cannot receive messages. b. Event notifications associated with unavailable topics are automatically cleared. For details about how to use SMN, see Creating a Topic, Adding a Subscription, and Configuring Topic Policies in the <i>Simple Message Notification User Guide</i>.

Step 7 Click **OK**.

----End

Related Operations

You can click **Edit** in the **Operation** column of an event notification rule, to edit the notification rule, or click **Delete** to delete the rule.

If you want to batch delete event notification rules, select the rules to delete and click **Delete** above the list.

7.4.2 Application Example: Configuring SMN-Enabled Event Notification

Background Information

An enterprise has a large number of files to archive but it does not want to cost much on storage resources. Therefore, the enterprise subscribes to OBS for storing daily files and expects that an employee can be informed of every operation performed on OBS via email.

Procedure

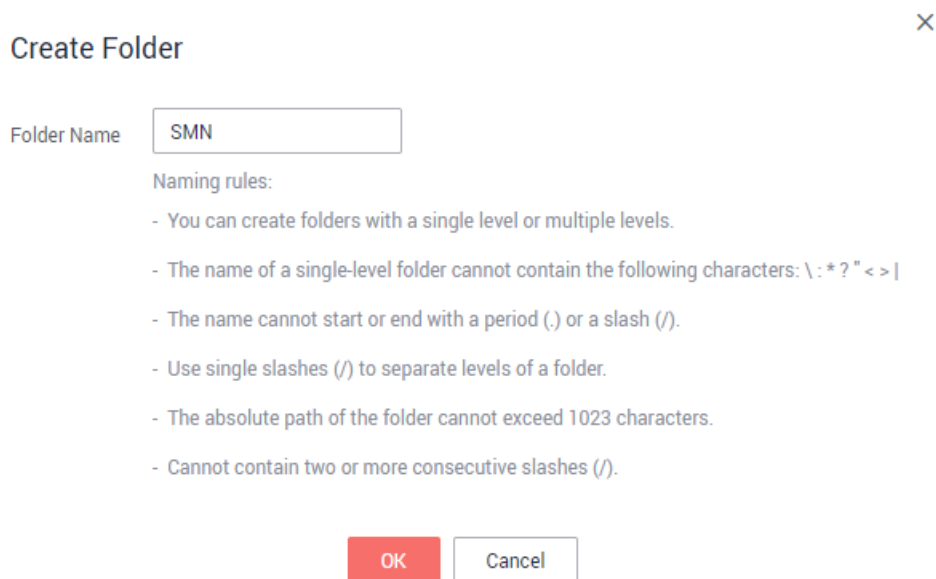

Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

Step 2 Create a bucket.

Click **Create Bucket** in the upper right corner of the page. On the page, select a region and storage class, and specify a bucket name and other parameters. Then, click **Create Now**.

Step 3 Create a folder.

Click the name of the bucket created in [Step 2](#) to go to the **Objects** page. Then, click **Create Folder**. In the displayed dialog box, enter a folder name and click **OK**. In the following example, **SMN** is the folder name.

Figure 7-6 Creating a folder**Step 4** In the upper left corner of the page, click  and choose **Simple Message Notification**. On the displayed SMN page, create a topic.

In the following example, **TestTopic** is the SMN topic and the notifications are sent via email.

Use SMN to create a notification topic for OBS as follows:

1. Create an SMN topic.
2. Add a subscription.
3. Modify the topic policy. On the **Configure Topic Policy** page, select **OBS** under **Services that can publish messages to this topic**.

For details, see [SMN Topic Management](#).

Step 5 Go back to OBS Console.**Step 6** Configure an event notification rule.

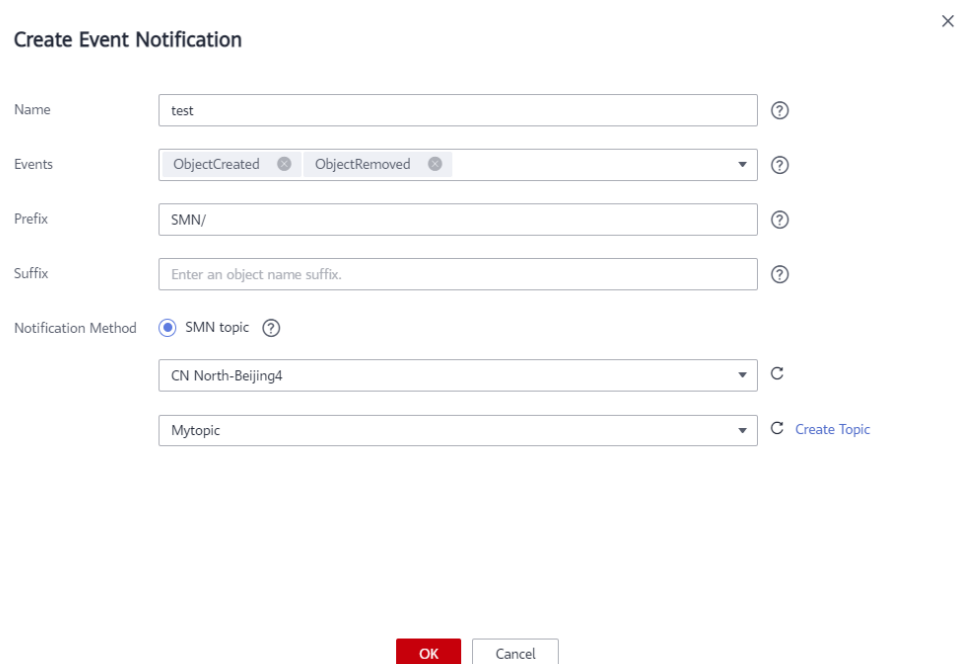
1. In the bucket list, click the bucket that you have created in [Step 2](#).
2. In the navigation pane, choose **Basic Configurations** > **Event Notification**. The **Event Notification** page is displayed.
3. Click **Create**. The **Create Event Notification** dialog box is displayed.

- Configure event notification parameters, as shown in [Figure 7-7](#). After the notification is configured, an employee will be informed of all specified operations on the **SMN** folder in bucket **testbucket**. For details about the parameters, see [Table 7-4](#).

 **NOTE**

- A folder path ends with a slash (/). Therefore, if you want to configure event notification rules for operations on folders and you need to filter folders by suffix, the suffix must also end with a slash (/).
- If neither the **Prefix** nor the **Suffix** is configured, the event notification rule applies to all objects in the bucket.

Figure 7-7 Adding an event notification rule



Create Event Notification ×

Name: ?

Events: ?

Prefix: ?

Suffix: ?

Notification Method: SMN topic ?

C

C [Create Topic](#)

----End

Verification

Step 1 Log in to OBS Console as an enterprise user.

Step 2 Upload the **test.txt** file to the folder created in [Step 3](#).

After the file is uploaded, an employee receives an email. Keyword **ObjectCreated:Post** in the email indicates that the object is successfully uploaded.

Step 3 Delete the **test.txt** file uploaded in [Step 2](#).

After the file is successfully deleted, an employee will receive an email. Keyword **ObjectRemoved>Delete** in the email indicates that the object is successfully deleted.

----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.

It can take up to two minutes for the configuration of static website hosting 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.

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 anonymous users.

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

Procedure

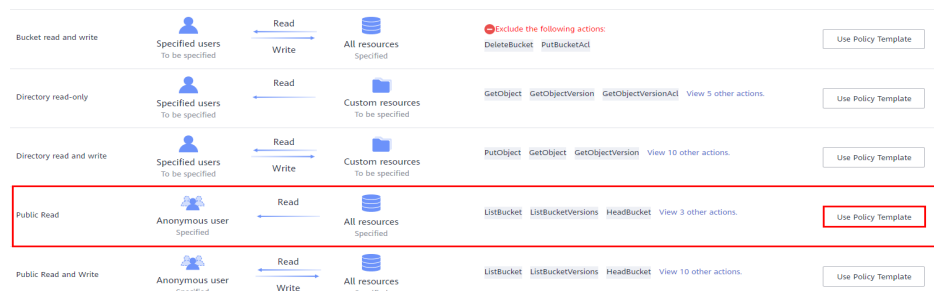
- Step 1** In the navigation pane of **OBS Console**, choose **Object Storage**.
- Step 2** In the bucket list, click the bucket you want to operate to go to the **Objects** page.
- Step 3 (Optional)** If the static website files in the bucket are not accessible to anonymous users, perform this step. If they are already accessible to everyone, skip this step.

Grant the read permission for static website files to anonymous users. For details, see [Granting Public Read Permissions on Objects to Anonymous Users](#).

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

1. Choose **Permissions > Bucket Policy**.
2. Click **Create Bucket Policy**.
3. In the template list, locate **Public Read** in the **Template Name** column and click **Use Policy Template** on the right.

Figure 8-1 Configuring the public read permission



4. Keep the default settings of the template and click **Next** and then **Create**.

- 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

Configure Static Website Hosting ×

i With static website hosting, your static website contents can be easily accessed through the endpoint provided by OBS.

Status

Hosting Type **Host a static website** Redirect requests [Learn more](#)

This option requires that the bucket policy is Public Read or anonymous users have been granted permissions through an object ACL to read hosted static website files.

Homepage
Only HTML files under the root directory are supported.

404 Error Page
Only HTML, JPG, PNG, BMP, and WEBP files under the root directory are supported.

Redirection Rule

OK Cancel

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 8-1](#).

Table 8-1 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.
	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 .

Container	Key	Description
	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 anonymous users.

Static web page files in the Archive storage class have been restored. For more information, see [Restoring an Object from 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.

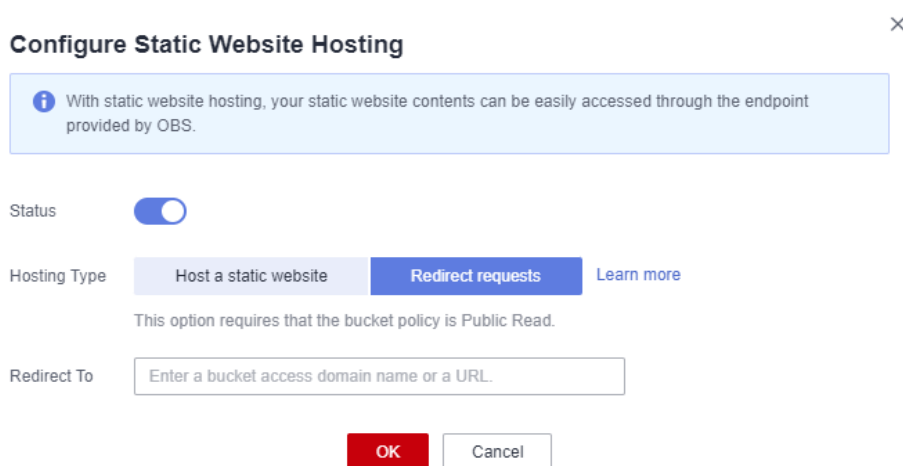
Alternatively, you can choose **Basic Configurations** > **Static Website Hosting** from the navigation pane on the left.

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.

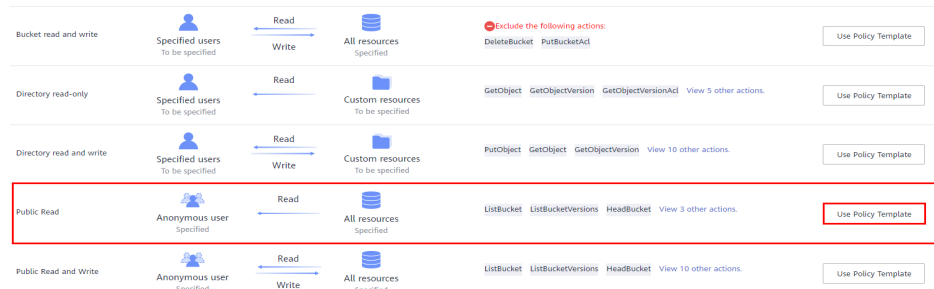
Step 10 (Optional) If the static website files in the bucket are not accessible to anonymous users, perform this step. If they are already accessible to everyone, skip this step.

Grant the read permission for static website files to anonymous users. For details, see [Granting Public Read Permissions on Objects to Anonymous Users](#).

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

1. Choose **Permissions** > **Bucket Policy**.
2. Click **Create Bucket Policy**.
3. In the template list, locate **Public Read** in the **Template Name** column and click **Use Policy Template** on the right.

Figure 8-4 Configuring the public read permission



4. Keep the default settings of the template and click **Next** and then **Create**.

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 User-Defined Domain Name

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?](#)

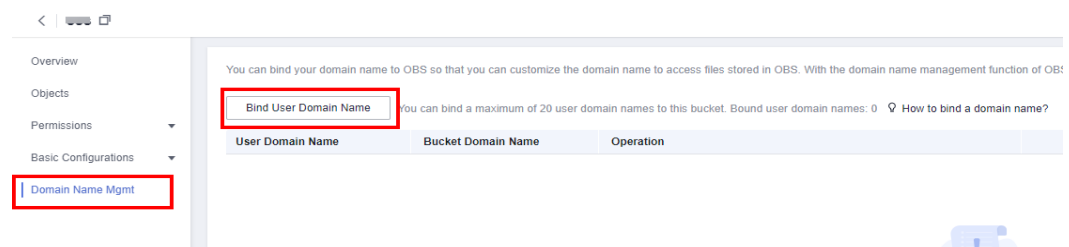
Procedure

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 8-5 Domain name management page

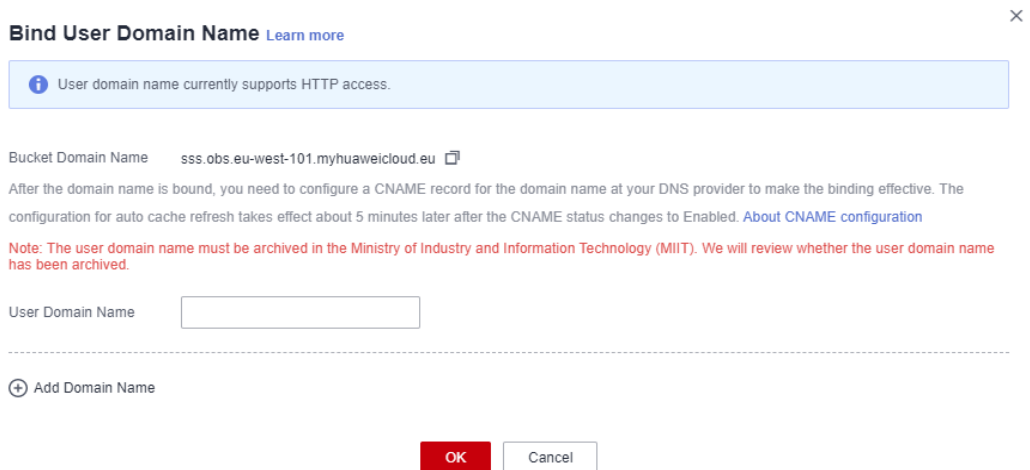


Step 4 Click **Bind User Domain Name**. In the displayed dialog box, enter the domain name to configure, as shown in **Figure 8-6**. If you want to choose one of the existing Huawei Cloud domain names from the drop-down list on OBS Console, you must have the **Domains:domains:getDetails** permission. 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 8-6 Binding a user domain name



Step 5 Click **OK**.

Step 6 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 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 8-2](#). Retain the default values for those not listed in the table below.

Table 8-2 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

Parameter	Description	Example Value
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 Server-Side Encryption

You can configure server-side encryption for an OBS bucket. Once configured, any objects you upload to the bucket will be encrypted with the specified KMS key by default.

You can enable server-side encryption when creating a bucket (see [Creating a Bucket](#)). You can also enable or disable server-side encryption for an existing bucket.

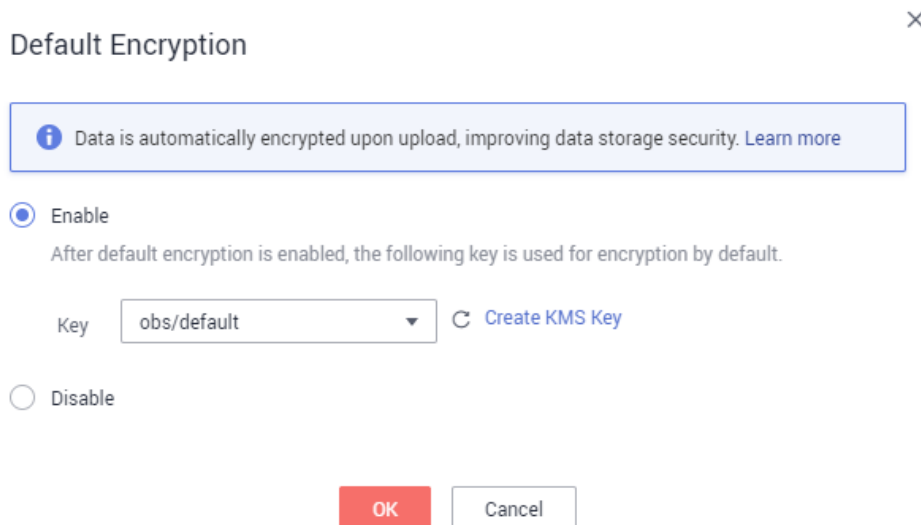
OBS only encrypts the objects uploaded after server-side encryption is enabled for the bucket, and does not encrypt those uploaded before. After server-side encryption is disabled, encryption status of existing objects in the bucket remains unchanged, and you can still encrypt objects when you upload them.

Enabling Server-Side 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 **Server-Side Encryption**. The **Server-Side Encryption** dialog box is displayed.
- Step 5** Select **Enable**.

Key **obs/default** is selected by default for KMS encryption. You can also click **Create KMS Key** to switch to the KMS management console and create a customer master key. Then go back to OBS Console and select the key from the drop-down list.

Figure 9-1 Enabling KMS-based encryption for a bucket



Step 6 Click **OK**.

----End

Disabling Server-Side 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 **Server-Side Encryption**. The **Server-Side Encryption** dialog box is displayed.

Step 5 Select **Disable**.

Step 6 Click **OK**.

----End

9.1.2 Enabling Server-Side Encryption When Uploading an Object

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

When you upload an object to a bucket with server-side encryption disabled, you can separately configure server-side encryption for the object. If the bucket has server-side encryption enabled, the object you upload inherits encryption from the bucket by default. You can also configure new encryption for the object.

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.

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 **KMS encryption** and select a key that you have created on DEW.

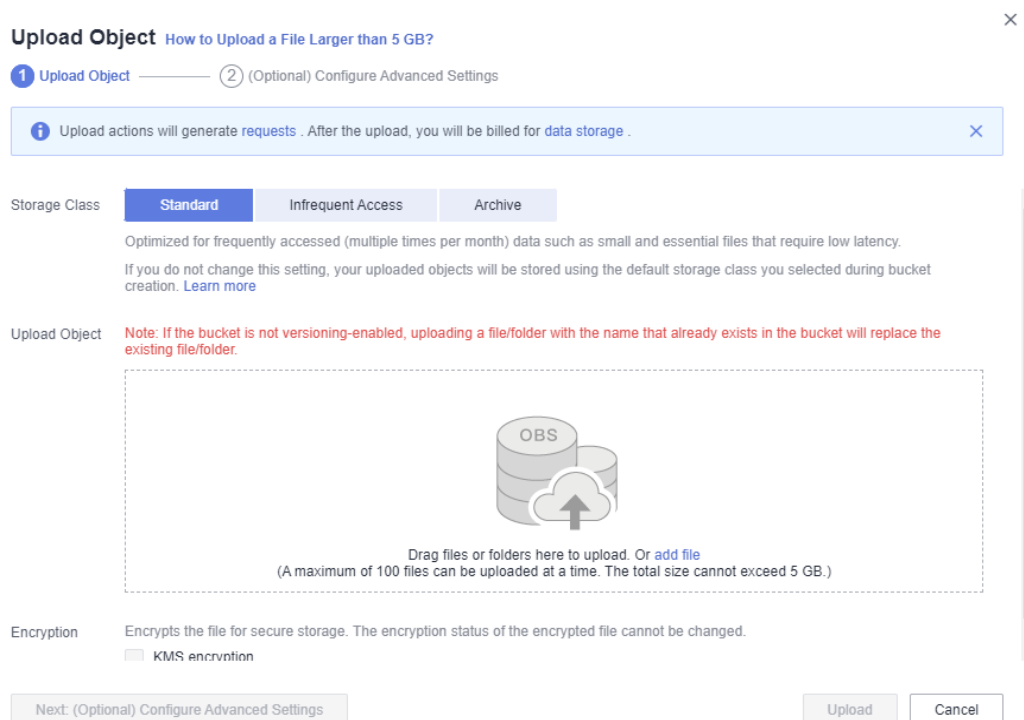
NOTE

If the bucket has server-side encryption enabled, any object you upload will inherit the KMS encryption from the bucket by default.

After **KMS encryption** is selected, **obs/default** is selected by default as the key for the encryption. You can also click **Create KMS Key** to switch to the KMS management console and create a customer master key. Then go back to OBS Console and select the key from the drop-down list.

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

Figure 9-2 Encrypting an object to be uploaded



Step 6 Click **Upload**.

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

----End

9.2 Configuring CORS

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

Prerequisites

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

Procedure

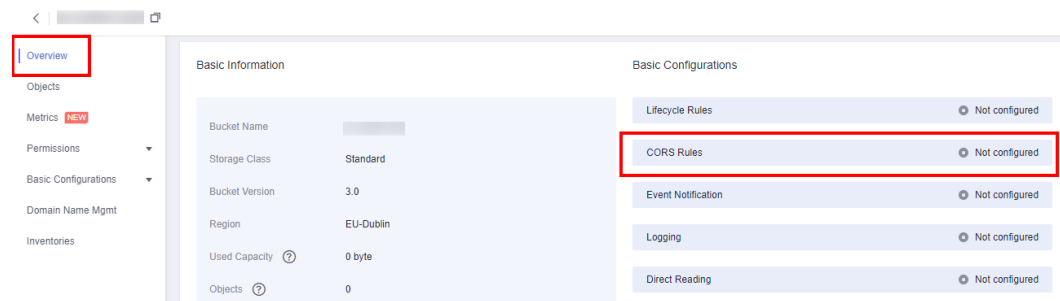
Step 1 In the navigation pane of [OBS Console](#), choose **Object Storage**.

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**.

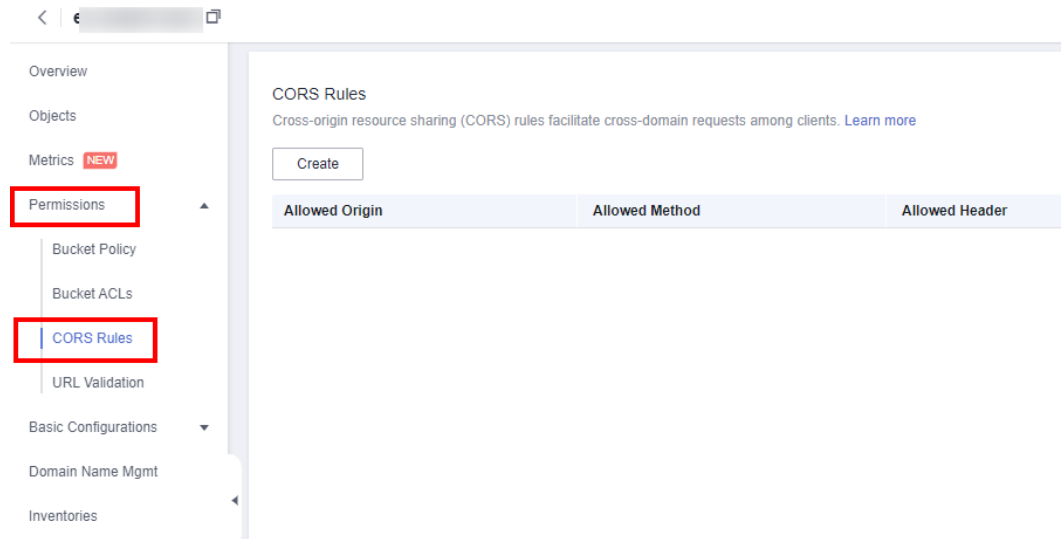
Step 4 In the **Basic Configurations** area, click **CORS Rules**. The **CORS Rules** page is displayed.

Figure 9-3 Overview > Basic Configurations > CORS Rules



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

Figure 9-4 Permissions > CORS Rules

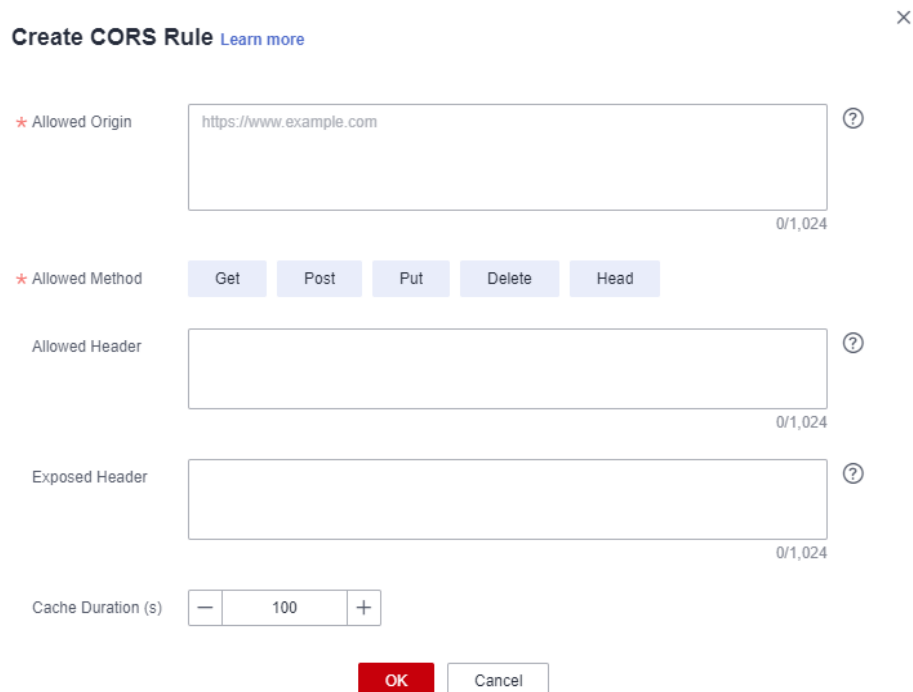


Step 5 Click **Create**. The **Create CORS Rule** dialog box is displayed. See [Figure 9-5](#) for details.

NOTE

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

Figure 9-5 Creating a CORS rule



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

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: http://rds.example.com https://*.vbs.example.com</p>
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>
Allowed Header	<p>Optional</p> <p>Specifies the allowed headers in cross-origin requests. Only CORS requests matching the allowed headers are valid.</p> <p>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.</p>
Exposed Header	<p>Optional</p> <p>Specifies the exposed headers in CORS responses, providing additional information for clients.</p> <p>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 them in this parameter. For the configuration of other headers, see Configuring CORS for a Bucket.</p> <p>You can enter multiple exposed headers (one per line). Spaces and special characters including * and < are not allowed.</p>
Cache Duration (s)	<p>Mandatory</p> <p>Specifies the duration that your browser can cache CORS responses, expressed in seconds. The default value is 100.</p>

Step 7 Click **OK**.

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

Then, only the addresses specified in **Allowed Origin** can access the OBS bucket over the methods specified in **Allowed Method**. Suppose you need to configure a

CORS rule for bucket **testbucket** and you set **Allowed Origin** to **https://www.example.com**, **Allowed Method** to **GET**, **Allowed Header** to *****, **Exposed Header** to **ETag**, and **Cache Duration (s)** to **100**. Then, only GET requests from **https://www.example.com** are allowed to access bucket **testbucket**. In addition, there are no limits put on headers in the requests, the ETag value can be returned in the response, and the client where the requests are from can cache the CORS response for 100 seconds.

----End

9.3 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 Information** area, find **Versioning** and click **Edit**. The **Versioning** dialog box is displayed.

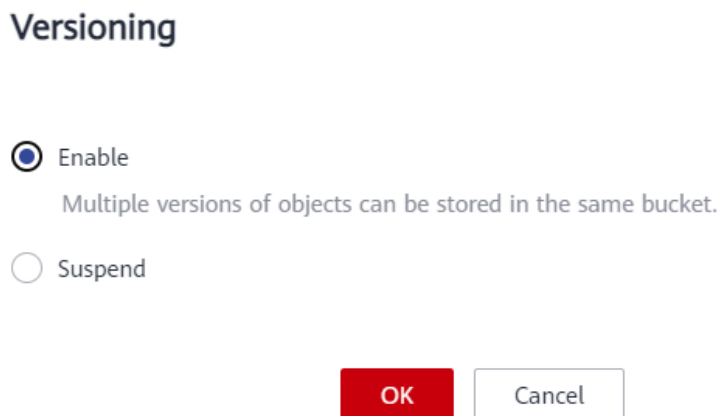
Figure 9-6 Editing versioning status

Basic Information

Bucket Name	
Storage Class	Standard
Bucket Version	3.0
Region	CN North-Beijing4
Used Capacity ?	0 byte
Objects ?	0
Account ID	
Created	May 24, 2022 19:46:50 GMT+08:00
Versioning ?	Disabled Edit
Endpoint ?	obs.cn-north-4.myhuaweicloud.com
Access Domain Name ?	<input type="text"/> Copy
Data Redundancy Policy	Multi-AZ storage

Step 5 Select **Enable**. For details, see [Figure 9-7](#).

Figure 9-7 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 9-8 Viewing object versions

Objects / object_001.txt Versioning

Name	object_001.txt	Storage Class	Standard Change Storage Class
Last Modified	Jun 07, 2022 14:47:14 GMT+08:00	Size	0 byte
Link	object_001.txt	Version ID	
Encrypted	No		
Object ACL	Metadata	Versions	

Last Modified	Storage Class	Operation
Jun 07, 2022 14:47:14 GMT+08:00(Latest Version)	Standard	Download Share Delete
Jun 07, 2022 14:47:10 GMT+08:00	Standard	Download Share Delete
Jun 07, 2022 14:47:04 GMT+08:00	Standard	Download Share Delete

----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.

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 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 choosing **Delete** in the **Operation** column. If you delete the latest version, the most recent version will become the latest version.

----End


9.4 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 **Permissions > URL Validation**.
- Step 4** 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.
- Referrer 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 5 Click  to save the settings.

----End

10 Monitoring and Logging

10.1 Monitoring

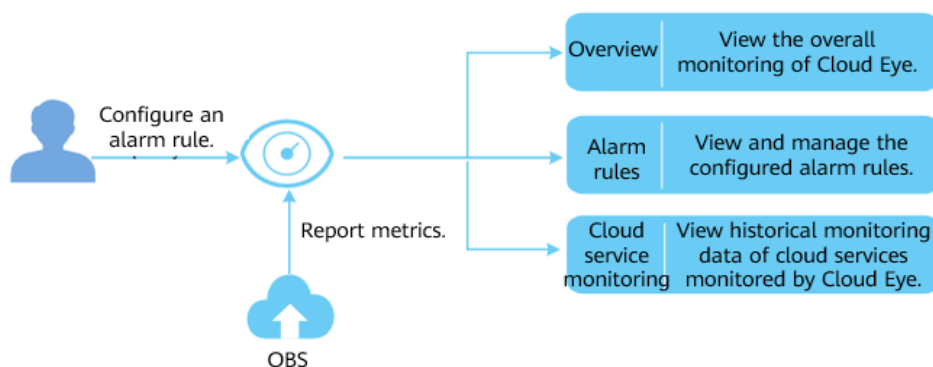
10.1.1 Monitoring OBS

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 10-1 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 there are exceptions.

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

On Cloud Eye, you can configure alarm rules for events. When specified events happen, you will receive alarm notifications. For details, see [Creating an Alarm Rule to Monitor an Event](#).

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 Metrics of a Cloud Service](#).

Cloud Eye monitors [OBS events](#) in real time. You can view the monitoring data on the Cloud Eye console. For details, see [Viewing Event Monitoring Data](#).

10.1.2 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

Metric ID	Metric	Description	Value Range	Monitored Entity	Monitoring Period (Original Metric)
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
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

Event Monitoring

Table 10-1 OBS events that can be monitored

Event Source	Event Name	Event ID	Event Severity
OBS	Delete bucket	deleteBucket	Major

Event Source	Event Name	Event ID	Event Severity
	Delete bucket policy	deleteBucketPolicy	Major
	Set bucket ACL	setBucketAcl	Minor
	Set bucket policy	setBucketPolicy	Minor

Dimensions

Table 10-2 Dimensions

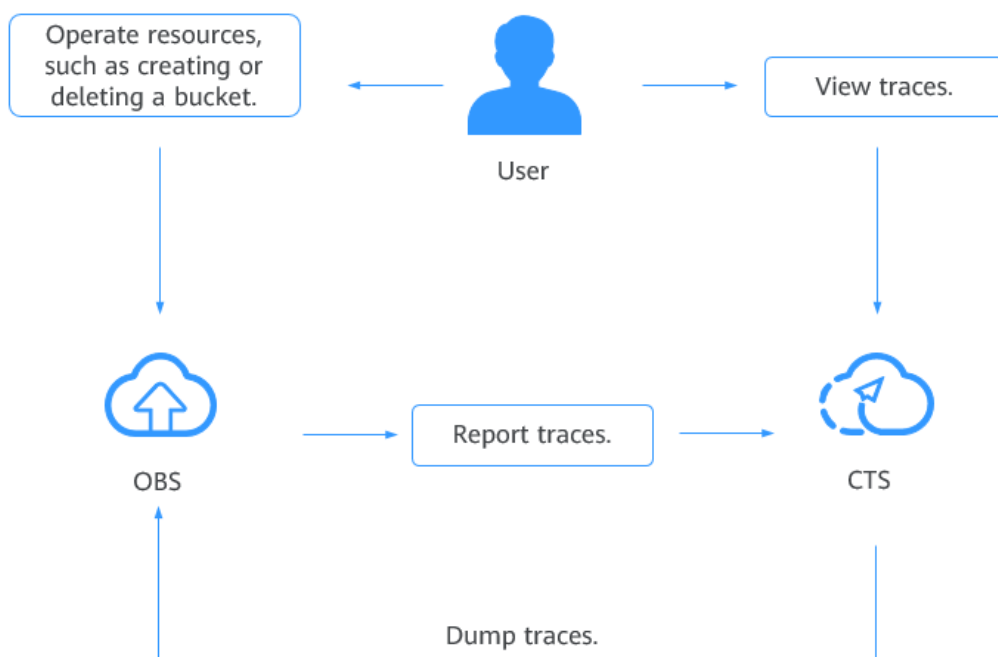
Key	Value
bucket_name	Bucket dimension. The value is the bucket name.

10.2 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.

Figure 10-2 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 the tracker configuration section in the *Cloud Trace Service User Guide*.
- End

Table 10-3 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 lifecycle configuration of a bucket	bucket	deleteBucketLifecycle
Management	Deleting a bucket policy	bucket	deleteBucketPolicy
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	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 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

Table 10-4 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
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

Tracker Type	Operation	Resource	Trace Name
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.MULTIDEL ETE
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.

10.3 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 10-3](#).

Figure 10-3 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

- 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 the log storage bucket has server-side encryption enabled, the 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 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, select **Disable** and then click **OK**. After logging is disabled, logs are not recorded, but existing logs in the target bucket will be retained.

11 Task Center

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

12 Related Operations

12.1 Creating an 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 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** In the navigation pane, choose **Policy Management > Agency Policies**.
- Step 3** Click **Create Agency**.
- Step 4** Enter an agency name.
- Step 5** Select **Cloud service** for the **Agency Type**.
- Step 6** Select **OBS** for **Cloud Service**.
- Step 7** Set a validity period.
- Step 8** Click **Next**.
- Step 9** 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": [  
    {  
      "Effect": "Allow",  
      "Action": "obs:*",  
      "Resource": "arn:aws:iam::123456789012:role/mybucketlogs"    }  
  ]  
}
```

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

Step 10 On the **Select Scope** page, select **Global services** for **Scope** and click **OK**.

Step 11 (Optional) If the log storage bucket has server-side encryption enabled, the agency also requires the **KMS Administrator** permission for the region where the bucket is 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 project in the region where the log storage bucket is located.

----End

Creating an Agency for Back to Source

Step 1 In the **Create Back-to-Source Rule** dialog box on OBS Console, click **View Agencies** to jump to the **Agencies** page on the IAM console.

Step 2 Click **Create Agency**.

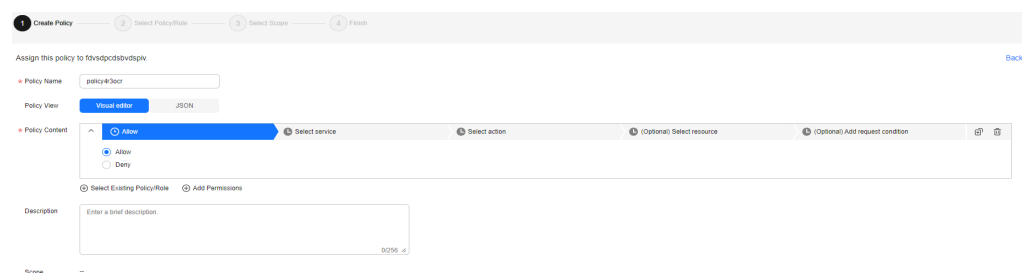
Step 3 On the **Create Agency** page, specify an agency name, select **Cloud service** for **Agency Type**, and choose **Object Storage Service (OBS)** for **Cloud Service**.

Step 4 Select a validity period and enter a description.

Step 5 Click **Done**. In the displayed dialog box, click **Authorize**.

Step 6 If there is already a policy meeting your requirements, go to 9. Otherwise, click **Create Policy** in the upper right corner.

Figure 12-1 Creating a policy



Step 7 Specify a policy name and choose **Visual editor** for **Policy View**.

Step 8 Configure **Policy Content** as follows:

1. Select **Allow**.
2. For the service, select **Object Storage Service (OBS)**.
3. For actions, under **ReadOnly**, select **obs:object:GetObject**, under **Read/Write**, select **obs:object:PutObject** and **obs:object:AbortMultipartUpload**, and under **ListOnly**, select **obs:bucket:ListBucket**.
4. For resources, select **All**.
5. Click **Next**.

Step 9 Select the policy and click **Next**. Then, set **Scope** to **All resources** and click **OK**.

 **NOTE**

The **All resources** option means that OBS can use all resources, including those in enterprise projects, region-specific projects, and global services under the account based on assigned permissions.

----End

13 Troubleshooting

13.1 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.

13.2 OBS Console Couldn't Be Opened in Internet Explorer 9

Question

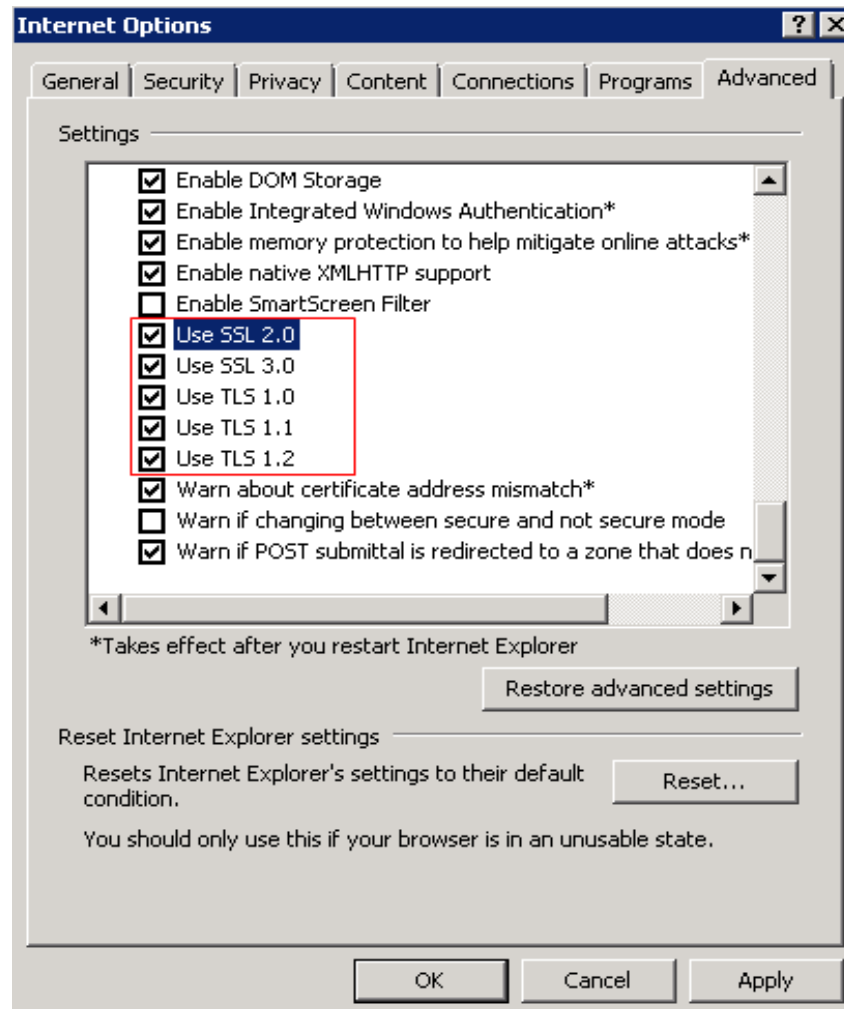
Why OBS Console cannot be opened in Internet Explorer 9, even if the address of OBS Console can be pinged?

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 13-1**.

Figure 13-1 Internet Options



- Step 3** Click **OK**.

----End

13.3 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.

13.4 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.

14 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 14-1](#) lists some common error codes in OBS error responses.

Table 14-1 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>