Object Storage Service

FAQs

Issue 01

Date 2025-10-21

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property 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 Cloud 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.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 OBS Basics

1.1 How Do I Obtain an OBS Endpoint?

You can access OBS through domain names. When you are using the API, third-party tools, or other methods to access OBS, you can use domain names to conveniently locate resources in OBS.

Before using OBS, ensure that the DNS server address has been correctly configured on the client.

Each data center has its own domain name. For details about domain names, see **Regions and Endpoints**.

1.2 How Much Data Can I Store in OBS?

There are no restrictions on the total capacity or number of objects or files that can be stored by the OBS system or in any single bucket. However, there are limitations on what size you can upload to your bucket at a time.

- OBS Console supports batch upload in some regions. In a single batch upload, you can upload a maximum of 100 files, a total of no more than 5 GB. If you upload one file at once, the file cannot exceed 50 MB in size.
- If you use OBS Browser+, obsutil, an API, or an SDK, you can upload a single object of up to 48.8 TB.

The size of a resource package only relates to your billing, not the actual storage. Any usage beyond your package quota will be billed on a pay-per-use basis.

In addition, OBS bucket data is logically isolated. The performance of a bucket is independent of data volume in it.

1.3 How Can I Determine Which Region to Store My Data In?

When selecting a region, consider the following factors:

- Location

  Select a region close to you or your target users. This reduces network latency and improves access speed. However, Chinese mainland regions provide the same infrastructure, BGP network quality, as well as resource operations and configurations. If you or your target users are in the Chinese mainland, you do not need to consider differences in network latency when selecting a region.

  - If you or your target users are in Asia Pacific (excluding the Chinese mainland), select regions such as AP-Bangkok and AP-Singapore.
  - If you or your target users are in Africa, select the AF-Johannesburg region.
  - If you or your target users are in Europe, select the EU-Paris region.

- Relationships between cloud services

  If you use multiple cloud services together, note that:

  - ECS, RDS, and OBS cannot communicate with each other over a private intranet if they are not in the same region.
  - ECSs in different regions cannot be deployed on the same load balancer.

- Resource prices

  Resource prices may vary by region. For details, see **Product Pricing Details**.

1.4 Does OBS Support Access over HTTPS?

OBS supports access through the following over HTTPS:

- OBS bucket domain name: Replace HTTP with HTTPS in the URL of the bucket or object in the browser.
- OBS user-defined domain name: To use it, **submit a service ticket** first.
- OBS acceleration domain name after CDN acceleration is enabled: After CDN acceleration is enabled, you can manage HTTPS certificates on the CDN console and access OBS using HTTPS. For details, see **Configuring an HTTPS Certificate**.

1.5 Can Other Users Access My Data Stored in OBS?

Yes.

- Bucket ACLs and bucket policies can be used to grant other users read access to your buckets.
- You can grant other users read permissions for objects in your bucket by configuring object ACLs, object policies, or bucket policies. Alternatively, you can configure object sharing.

1.6 Why Is an Alarm Reported When I Access OBS and What Can I Do?

Cause

Users are not allowed to upload violent or illegal content to OBS buckets. Such content will be detected and blocked by OBS and third-party platforms (such as WeChat, Alipay, and Baidu). When a third-party platform blocks such content, it also lists the OBS domain name as an untrusted domain name, so other users who access this domain name receive the alarm.

Solution

If you need to access OBS via a third-party platform or program, such as WeChat, Alipay, or Baidu, use **a user-defined domain name** to access OBS resources, to avoid receiving the alarm.

1.7 Can Deleted Data Be Recovered?

Whether deleted data can be restored depends on whether versioning is enabled.

- Versioning enabled for a bucket:
  - If the **Historical Versions** button is disabled, a deleted object is not displayed in the object list. After the button is enabled, the current object version with a delete marker and the deleted object (also the historical object version) are displayed in the object list. In this case, you can click **Permanently Delete** in the **Operation** column of the current object version with a delete marker to recover the deleted object.

    NOTE

    If you delete an object from a versioning-enabled bucket, instead of deleting the object permanently, OBS inserts a delete marker, which becomes the current object version. The deleted object becomes the historical version. After that, if you enable the **Historical Versions** button above the object list, you can see the current object version with a delete marker and the deleted object that has become a historical version.
  - If the **Historical Versions** button is enabled, you choose **More** > **Permanently Delete** in the **Operation** column of an object version other than the current one with a delete marker to permanently delete the object. The deleted object cannot be recovered.
- If versioning is disabled for a bucket, OBS permanently deletes all data of a deleted object, and deleted objects cannot be recovered.

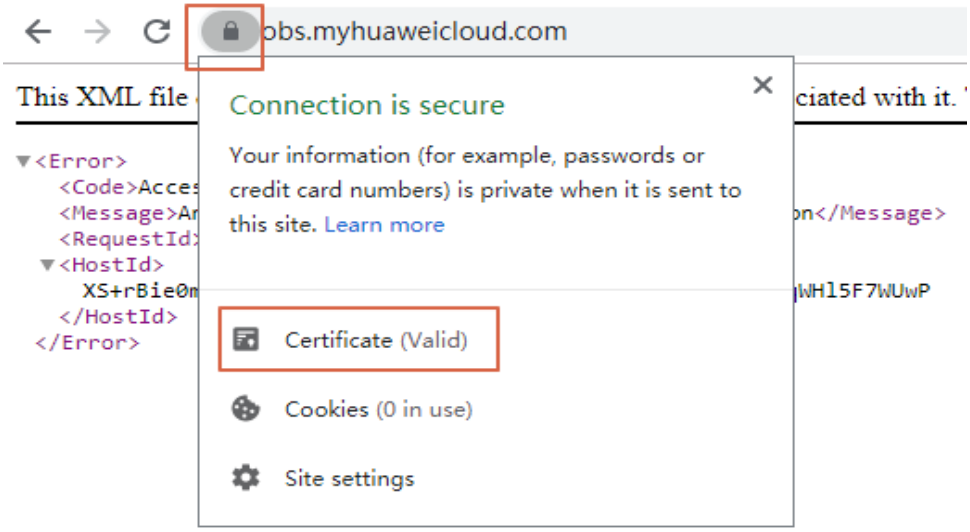
1.8 What Can I Do If My Access to the OBS Domain Name Failed Due to a CA Certificate Connection Failure?

If the certificate is untrusted, accessing the OBS domain name fails. You need to obtain the OBS certificate again and import it to the client trust store.

Step 1 Obtain the OBS certificate (using the Chrome browser as an example).

1. Enter the OBS domain name in the address box of a browser: **https://obs.myhuaweicloud.com**.
2. Click on the left of the domain name and select **Certificate**.

Figure 1-1 Exporting a certificate



3. Click **Details** > **Copy to File** and obtain the OBS certificate (**obs.cer**) as prompted.

Step 2 Import the OBS certificate to the client trust store.

For example, if a Java runtime environment is used, you need to import the certificate to **cacerts**. In the following example, **d:\obs.cer** is where the certificate is stored.

NOTE

OBS certificate formats vary depending on the runtime environments. This example uses the Java runtime environment as an example. In other environments, convert the certificate format as required before the import.

```
keytool -import -alias cacerts -keystore cacerts -file d:\obs.cer
```

----End

1.9 Why Did Some of My Data Stored in OBS Get Lost?

If the data stored in OBS is lost, perform the following operations:

- Check whether there is a lifecycle rule configured to automatically delete objects after a certain date.
- Check whether the write permission to the bucket has been granted to other users. If it was, those other users can delete objects from the bucket. If you have enabled logging, you can check the logs to find out who deleted the objects.

1.10 Does OBS Support Traffic Monitoring?

Yes.

On Cloud Eye, you can monitor the OBS metrics described in the following table.

Table 1-1 OBS metrics (for requests)

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
get_request_count	GET Requests	Number of GET requests made to all buckets and objects in the buckets of a region.	≥ 0	Count	N/A	Bucket	1 minute
put_request_count	PUT Requests	Number of PUT requests made to all buckets and objects in the buckets of a region.	≥ 0	Count	N/A	Bucket	1 minute
post_request_count	POST Requests	Number of POST requests made to all buckets and objects in the buckets of a region.	≥ 0	Count	N/A	Bucket	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
head_request_count	HEAD Requests	Number of HEAD requests made to all buckets and objects in the buckets of a region.	≥ 0	Count	N/A	Bucket	1 minute
delete_request_count	DELETE Requests	Number of DELETE requests made to all buckets and objects in the buckets of a region.	≥ 0	Count	N/A	Bucket	1 minute
first_byte_latency	First Byte Download Delay	Average time from receiving a GET request to the time that the system starts to respond in a measurement period.	≥ 0	ms	N/A	Bucket	1 minute
request_count_4xx	4XX Status Codes	Number of requests whose status code returned by the server is 4*xx*.	≥ 0	Count	N/A	User Bucket API	1 minute
request_count_5xx	5XX Status Codes	Number of requests whose status code returned by the server is 5*xx*.	≥ 0	Count	N/A	User Bucket API	1 minute
total_request_latency	Average Request Latency	Average time from receiving a request to the time that the system response ends in a measurement period.	≥ 0	ms	N/A	User Bucket API	1 minute
total_request_callback_latency	Average Request Callback Latency	Average time required for calling a specific API in a request.	≥ 0	ms	N/A	Bucket	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
request_count_per_second	Total TPS	Average number of requests per second in a statistical period.	≥ 0	Count/s	N/A	User Bucket Domain name	1 minute
request_count_get_per_second	GET Request TPS	Average number of GET requests per second in a statistical period.	≥ 0	Count/s	N/A	User Bucket Domain name	1 minute
request_count_put_per_second	PUT Request TPS	Average number of PUT requests per second in a statistical period.	≥ 0	Count/s	N/A	User Bucket Domain name	1 minute
request_count_delete_per_second	DELETE Request TPS	Average number of DELETE requests per second in a statistical period.	≥ 0	Count/s	N/A	User Bucket Domain name	1 minute
request_count_post_per_second	POST Request TPS	Average number of POST requests per second in a statistical period.	≥ 0	Count/s	N/A	User Bucket Domain name	1 minute
request_count_head_per_second	HEAD Request TPS	Average number of HEAD requests per second in a statistical period.	≥ 0	Count/s	N/A	User Bucket Domain name	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
request_success_rate	Request Success Rate	Used to measure the availability of the storage service system. It refers to the percentage of non-server error requests (with status code 5*xx* returned) in the total request count. It is calculated as follows: (1 – 5*xx* requests/ Total requests) x 100%	≥ 0, ≤ 100	%	N/A	User Bucket API Domain name	1 minute
effective_request_rate	Valid request rate	Validity of client requests. Percentage of the valid requests in the total requests. It is calculated as follows: (Number of client requests whose returned status code is 2*xx* or 3*xx*/Total number of requests) x 100%	≥ 0, ≤ 100	%	N/A	User Bucket API	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
request_break_rate	Request interruption rate	Percentage of the number of requests interrupted by a client to the total number of requests. It is calculated as follows: (Number of requests interrupted by a client/Total number of requests) x 100%	≥ 0, ≤ 100	%	N/A	User Bucket API	1 minute
request_code_count	HTTP status code count	Measures the number of requests with status codes returned by the server. For details about the response status codes, see **HTTP Status Codes**.	≥ 0	Count	N/A	Bucket API HTTP status code	1 minute
api_request_count_per_second	API request TPS	Average number of specific API requests sent to all buckets and objects of a tenant per second within a statistical period. For details about the supported APIs, see **Request APIs**.	≥ 0	Count/s	N/A	Bucket API	1 minute
request_count_monitor_2XX	2xx Status Codes	Times that the server responds to requests whose status codes are 2*xx*.	≥ 0	Count	N/A	User Bucket Domain name	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
request_count_monitor_3XX	3xx Status Codes	Times that the server responds to requests whose status codes are 3*xx*.	≥ 0	Count	N/A	User Bucket Domain name	1 minute
request_count_monitor_4XX	4XX Status Codes	Times that the server responds to requests whose error codes are 4*xx*	≥ 0	Count	N/A	User Bucket Domain name	1 minute
request_count_monitor_5XX	5XX Status Codes	Times that the server responds to requests whose error codes are 5*xx*	≥ 0	Count	N/A	User Bucket Domain name	1 minute
download_bytes	Total Download Bandwidth	Total size of objects downloaded per second in a measurement period.	≥ 0	byte/s	1024 (IEC)	User Bucket Domain name	1 minute
download_bytes_extranet	Download Bandwidth (Internet)	Total size of objects downloaded over the Internet per second in a measurement period.	≥ 0	byte/s	1024 (IEC)	User Bucket Domain name	1 minute
download_bytes_intranet	Download Bandwidth (Intranet)	Total size of objects downloaded over the Intranet per second in a measurement period.	≥ 0	byte/s	1024 (IEC)	User Bucket Domain name	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
upload_bytes	Total Upload Bandwidth	Total size of objects uploaded per second in a measurement period.	≥ 0	byte/s	1024 (IEC)	User Bucket Domain name	1 minute
upload_bytes_extranet	Upload Bandwidth (Internet)	Total size of objects uploaded over the Internet per second in a measurement period.	≥ 0	byte/s	1024 (IEC)	User Bucket Domain name	1 minute
upload_bytes_intranet	Upload Bandwidth (Intranet)	Total size of objects uploaded over the Intranet per second in a measurement period.	≥ 0	byte/s	1024 (IEC)	User Bucket Domain name	1 minute
cdn_bytes	CDN Pull Bandwidth	The object size that CDN pulls per second from an origin server over the Internet in a given measurement period.	≥ 0	Byte/s	1024 (IEC)	User Bucket	1 minute
download_traffic	Total Download Traffic	Total size of objects downloaded in a measurement period.	≥ 0	byte	1024 (IEC)	User Bucket Domain name	1 minute
download_traffic_extranet	Download Traffic (Internet)	Total size of objects downloaded over the Internet in a measurement period.	≥ 0	byte	1024 (IEC)	User Bucket Domain name	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
download_traffic_intranet	Download Traffic (Intranet)	Total size of objects downloaded over the Intranet in a measurement period.	≥ 0	byte	1024 (IEC)	User Bucket Domain name	1 minute
download_traffic_infrequent_access	Download Traffic (Infrequent Access)	Total size of Infrequent Access objects downloaded in a measurement period.	≥ 0	Byte	1024 (IEC)	User Bucket	1 minute
upload_traffic	Total Upload Traffic	Total size of objects uploaded in a measurement period.	≥ 0	byte	1024 (IEC)	User Bucket Domain name	1 minute
upload_traffic_extranet	Upload Traffic (Internet)	Total size of objects uploaded over the Internet in a measurement period.	≥ 0	byte	1024 (IEC)	User Bucket Domain name	1 minute
upload_traffic_intranet	Upload Traffic (Intranet)	Total size of objects uploaded over the Intranet in a measurement period.	≥ 0	byte	1024 (IEC)	User Bucket Domain name	1 minute
cdn_traffic	CDN Pull Traffic	The total traffic generated when CDN pulls data from an origin server over the Internet in a given measurement period	≥ 0	Byte	1024 (IEC)	User Bucket	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
upload_transfer_rate	Average Upload Rate	Size of objects uploaded per second in a measurement period.	≥ 0	Bytes/s	1024 (IEC)	Bucket	1 minute
download_transfer_rate	Average Download Rate	Size of objects downloaded per second.	≥ 0	Bytes/s	1024 (IEC)	Bucket	1 minute
request_get_size_le_1MB_latency	GET Request Latency (Object ≤ 1 MB)	Average latency of GET requests against objects no larger than 1 MB in a measurement period.	≥ 0	ms	N/A	Bucket	1 minute
request_get_size_between_1MB_4MB_latency	GET Request Latency (1 MB < Object ≤ 4 MB)	Average latency of GET requests against objects that are larger than 1 MB but no larger than 4 MB in a measurement period.	≥ 0	ms	N/A	Bucket	1 minute
request_get_size_between_4MB_10MB_latency	GET Request Latency (4 MB < Object ≤ 10 MB)	Average latency of GET requests against objects that are larger than 4 MB but no larger than 10 MB in a measurement period.	≥ 0	ms	N/A	Bucket	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
request_get_size_between_10MB_100MB_latency	GET Request Latency (10 MB < Object ≤ 100 MB)	Average latency of GET requests against objects that are larger than 10 MB but no larger than 100 MB in a measurement period.	≥ 0	ms	N/A	Bucket	1 minute
request_get_size_gt_100MB_latency	GET Request Latency (Object > 100 MB)	Average latency of GET requests against objects larger than 100 MB in a measurement period.	≥ 0	ms	N/A	Bucket	1 minute
request_put_size_le_1MB_latency	PUT Request Latency (Object ≤ 1 MB)	Average latency of PUT requests against objects no larger than 1 MB in a measurement period.	≥ 0	ms	N/A	Bucket	1 minute
request_put_size_between_1MB_4MB_latency	PUT Request Latency (1 MB < Object ≤ 4 MB)	Average latency of PUT requests against objects that are larger than 1 MB but no larger than 4 MB in a measurement period.	≥ 0	ms	N/A	Bucket	1 minute
request_put_size_between_4MB_10MB_latency	PUT Request Latency (4 MB < Object ≤ 10 MB)	Average latency of PUT requests against objects that are larger than 4 MB but no larger than 10 MB in a measurement period.	≥ 0	ms	N/A	Bucket	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
request_put_size_between_10MB_100MB_latency	PUT Request Latency (10 MB < Object ≤ 100 MB)	Average latency of PUT requests against objects that are larger than 10 MB but no larger than 100 MB in a measurement period.	≥ 0	ms	N/A	Bucket	1 minute
request_put_size_gt_100MB_latency	PUT Request Latency (Object > 100 MB)	Average latency of PUT requests against objects larger than 100 MB in a measurement period.	≥ 0	ms	N/A	Bucket	1 minute
upload_server_request_latency	Total Server-Side Upload Latency	Average time required for uploading objects on the OBS server.	≥ 0	ms	N/A	Bucket	1 minute
upload_total_request_latency	Total E2E Upload Latency	Average end-to-end time required for uploading objects.	≥ 0	ms	N/A	Bucket	1 minute
download_server_request_latency	Total Server-Side Download Latency	Average time required for downloading objects on the OBS server.	≥ 0	ms	N/A	Bucket	1 minute
download_total_request_latency	Total E2E Download Latency	Average end-to-end time required for downloading objects.	≥ 0	ms	N/A	Bucket	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
request_size_le_1MB_latency_p99	P99 Request Latency (Object ≤ 1 MB)	P99 latency of the requests for objects no larger than 1 MB.	≥ 0	ms	N/A	Bucket	1 minute
request_size_between_1MB_4MB_latency_p99	P99 Request Latency (1 MB < Object ≤ 4 MB)	P99 latency of the requests for objects from 1 MB (exclusive) to 4 MB.	≥ 0	ms	N/A	Bucket	1 minute
request_size_between_4MB_10MB_latency_p99	P99 Request Latency (4 MB < Object ≤ 10 MB)	P99 latency of the requests for objects from 4 MB (exclusive) to 10 MB.	≥ 0	ms	N/A	Bucket	1 minute
request_size_between_10MB_100MB_latency_p99	P99 Request Latency (10 MB < Object ≤ 100 MB)	P99 latency of the requests for objects from 10 MB (exclusive) to 100 MB.	≥ 0	ms	N/A	Bucket	1 minute
request_size_gt_100MB_latency_p99	P99 Request Latency (Object > 100 MB)	P99 latency of the requests for objects larger than 100 MB.	≥ 0	ms	N/A	Bucket	1 minute
request_size_le_1MB_latency_p95	P95 Request Latency (Object ≤ 1 MB)	P95 latency of the requests for objects no larger than 1 MB.	≥ 0	ms	N/A	Bucket	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
request_size_between_1MB_4MB_latency_p95	P95 Request Latency (1 MB < Object ≤ 4 MB)	P95 latency of the requests for objects from 1 MB (exclusive) to 4 MB.	≥ 0	ms	N/A	Bucket	1 minute
request_size_between_4MB_10MB_latency_p95	P95 Request Latency (4 MB < Object ≤ 10 MB)	P95 latency of the requests for objects from 4 MB (exclusive) to 10 MB.	≥ 0	ms	N/A	Bucket	1 minute
request_size_between_10MB_100MB_latency_p95	P95 Request Latency (10 MB < Object ≤ 100 MB)	P95 latency of the requests for objects from 10 MB (exclusive) to 100 MB.	≥ 0	ms	N/A	Bucket	1 minute
request_size_gt_100MB_latency_p95	P95 Request Latency (Object > 100 MB)	P95 latency of the requests for objects larger than 100 MB.	≥ 0	ms	N/A	Bucket	1 minute
request_size_le_1MB_latency_p90	P90 Request Latency (Object ≤ 1 MB)	P90 latency of the requests for objects no larger than 1 MB.	≥ 0	ms	N/A	Bucket	1 minute
request_size_between_1MB_4MB_latency_p90	P90 Request Latency (1 MB < Object ≤ 4 MB)	P90 latency of the requests for objects from 1 MB (exclusive) to 4 MB.	≥ 0	ms	N/A	Bucket	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
request_size_between_4MB_10MB_latency_p90	P90 Request Latency (4 MB < Object ≤ 10 MB)	P90 latency of the requests for objects from 4 MB (exclusive) to 10 MB.	≥ 0	ms	N/A	Bucket	1 minute
request_size_between_10MB_100MB_latency_p90	P90 Request Latency (10 MB < Object ≤ 100 MB)	P90 latency of the requests for objects from 10 MB (exclusive) to 100 MB.	≥ 0	ms	N/A	Bucket	1 minute
request_size_gt_100MB_latency_p90	P90 Request Latency (Object > 100 MB)	P90 latency of the requests for objects larger than 100 MB.	≥ 0	ms	N/A	Bucket	1 minute
request_count_monitor_6XX	6XX Status Codes	Number of requests whose status code returned by the server is 6*xx*.	≥ 0	Count	N/A	User Bucket Domain name	1 minute
request_count_monitor_7XX	7XX Status Codes	Number of requests whose status code returned by the server is 7*xx*.	≥ 0	Count	N/A	User Bucket Domain name	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
get_mirror_range_bandwidths	Range Retrieval Bandwidth (Mirroring-based Back to Source)	Bandwidth for retrieving object ranges with mirroring-based back to source	≥ 0	Byte/s	1024 (IEC)	User	1 minute
get_mirror_fetch_bandwidths	Fetch Bandwidth (Mirroring-based Back to Source)	Bandwidth for fetches triggered by mirroring-based back to source	≥ 0	Byte/s	1024 (IEC)	User	1 minute
get_mirror_fetch_task_status	Fetch Status (Mirroring-based Back to Source)	Status of asynchronous fetches triggered by mirroring-based back to source. A value of 1 indicates that asynchronous fetches can be triggered, while a value less than 1 indicates that asynchronous fetches cannot be triggered.	≤ 1	Count	N/A	User	1 minute
standard_request_upload_bandwidths	Avg. Bandwidth for Uploading Standard Objects	Average size of all Standard objects uploaded using PUT and POST per second in a measurement period	≥ 0	Byte/s	1024 (IEC)	Bucket	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
infrequent_request_upload_bandwidths	Avg. Bandwidth for Uploading Infrequent Access Objects	Average size of all Infrequent Access objects uploaded using PUT and POST per second in a measurement period	≥ 0	Byte/s	1024 (IEC)	Bucket	1 minute
archive_request_upload_bandwidths	Avg. Bandwidth for Uploading Archive Objects	Average size of all Archive objects uploaded using PUT and POST per second in a measurement period	≥ 0	Byte/s	1024 (IEC)	Bucket	1 minute
standard_request_delete_bytes	Avg. Bandwidth for Deleting Standard Objects	Average size of all Standard objects deleted using DELETE per second in a measurement period	≥ 0	Byte/s	1024 (IEC)	Bucket	1 minute
infrequent_request_delete_bytes	Avg. Bandwidth for Deleting Infrequent Access Objects	Average size of all Infrequent Access objects deleted using DELETE per second in a measurement period	≥ 0	Byte/s	1024 (IEC)	Bucket	1 minute
archive_request_delete_bytes	Avg. Bandwidth for Deleting Archive Objects	Average size of all Archive objects deleted using DELETE per second in a measurement period	≥ 0	Byte/s	1024 (IEC)	Bucket	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
standard_request_download_bandwidths	Avg. Bandwidth for Downloading Standard Objects	Average size of all Standard objects downloaded using GET per second in a measurement period	≥ 0	Byte/s	1024 (IEC)	Bucket	1 minute
infrequent_request_download_bandwidths	Avg. Bandwidth for Downloading Infrequent Access Objects	Average size of all Infrequent Access objects downloaded using GET per second in a measurement period	≥ 0	Byte/s	1024 (IEC)	Bucket	1 minute
archive_request_download_bandwidths	Avg. Bandwidth for Downloading Archive Objects	Average size of all Archive objects downloaded using GET per second in a measurement period	≥ 0	Byte/s	1024 (IEC)	Bucket	1 minute
standard_download_request_count	Standard Object Download Requests	Average number of GET requests for Standard objects per second in a measurement period	≥ 0	Count	N/A	Bucket	1 minute
infrequent_download_request_count	Infrequent Access Object Download Requests	Average number of GET requests for Infrequent Access objects per second in a measurement period	≥ 0	Count	N/A	Bucket	1 minute

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
archive_download_request_count	Archive Object Download Requests	Average number of GET requests for Archive objects per second in a measurement period	≥ 0	Count	N/A	Bucket	1 minute
standard_upload_request_count	Standard Object Upload Requests	Average number of PUT and POST requests for Standard objects per second in a measurement period	≥ 0	Count	N/A	Bucket	1 minute
infrequent_upload_request_count	Infrequent Access Object Upload Requests	Average number of PUT and POST requests for Infrequent Access objects per second in a measurement period	≥ 0	Count	N/A	Bucket	1 minute
archive_upload_request_count	Archive Object Upload Requests	Average number of PUT and POST requests for Archive objects per second in a measurement period	≥ 0	Count	N/A	Bucket	1 minute

Table 1-2 OBS metrics (for storage)

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
capacity_total	Total Used Storage Space	Measures the storage space occupied by all data.	≥ 0	Bytes	1024 (IEC)	User Bucket	30 minutes
capacity_standard	Used Space - Standard Storage	Measures the storage space occupied by Standard data.	≥ 0	Bytes	1024 (IEC)	User Bucket	30 minutes
capacity_infrequent_access	Used Space - Infrequent Access Storage	Measures the storage space occupied by Infrequent Access data.	≥ 0	Bytes	1024 (IEC)	User Bucket	30 minutes
capacity_archive	Used Space - Archive Storage	Measures the storage space occupied by Archive data.	≥ 0	Bytes	1024 (IEC)	User Bucket	30 minutes
capacity_deep_archive	Used Space - Deep Archive Storage	Measures the storage space occupied by Deep Archive data.	≥ 0	Byte	1024 (IEC)	User Bucket	30 minutes
capacity_standard_single_az	Standard Storage (Single-AZ)	Space occupied by Standard data stored in a single AZ	≥ 0	Byte	1024 (IEC)	User Bucket	30 minutes
capacity_standard_multi_az	Standard Storage (Multi-AZ)	Space occupied by Standard data stored in multiple AZs	≥ 0	Byte	1024 (IEC)	User Bucket	30 minutes
capacity_infrequent_access_single_az	Infrequent Access Storage (Single-AZ)	Space occupied by Infrequent Access data stored in a single AZ	≥ 0	Byte	1024 (IEC)	User Bucket	30 minutes

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
capacity_infrequent_access_multi_az	Infrequent Access Storage (Multi-AZ)	Space occupied by Infrequent Access data stored in multiple AZs	≥ 0	Byte	1024 (IEC)	User Bucket	30 minutes
object_num_all	Total Number of Objects	Total number of objects (including folders and all file versions) stored in all storage classes	≥ 0	Count	N/A	User Bucket	30 minutes
object_num_standard_total	Number of Objects - Standard Storage	Total number of objects (including folders and all file versions) stored in the Standard storage class	≥ 0	Count	N/A	User Bucket	30 minutes
object_num_infrequent_access_total	Number of Objects - Infrequent Access Storage	Total number of objects (including folders and all file versions) stored in the Infrequent Access storage class	≥ 0	Count	N/A	User Bucket	30 minutes
object_num_archive_total	Number of Objects - Archive Storage	Total number of objects (including folders and all file versions) stored in the Archive storage class	≥ 0	Count	N/A	User Bucket	30 minutes
object_num_deep_archive_total	Number of Objects - Deep Archive Storage	Total number of objects (including folders and all file versions) stored in the Deep Archive storage classes	≥ 0	Count	N/A	User Bucket	30 minutes

Metric ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Entity	Monitoring Period (Original Metric)
object_num_standard_single_az	Standard Objects (Single-AZ)	Total number of Standard objects (including folders and all object versions) stored in a single AZ	≥ 0	Count	N/A	User Bucket	30 minutes
object_num_standard_multi_az	Standard Objects (Multi-AZ)	Total number of Standard objects (including folders and all object versions) stored in multiple AZs	≥ 0	Count	N/A	User Bucket	30 minutes
object_num_infrequent_access_single_az	Infrequent Access Objects (Single-AZ)	Total number of Infrequent Access objects (including folders and all object versions) stored in a single AZ	≥ 0	Count	N/A	User Bucket	30 minutes
object_num_infrequent_access_multi_az	Infrequent Access Objects (Multi-AZ)	Total number of Infrequent Access objects (including folders and all object versions) stored in multiple AZs	≥ 0	Count	N/A	User Bucket	30 minutes

1.11 What Are the Factors that Affect the Upload and Download Speeds of OBS?

The OBS upload and download speeds may be affected by:

- Default upper limit of the OBS read/write bandwidth allowed for a single Huawei Cloud account: 16 Gbit/s (which means the total GET and PUT bandwidths over both public and private networks)

  If the actual bandwidth reaches this upper limit, flow control will be triggered.
- Bandwidth of the purchased VM NIC

If the NIC bandwidth is lower than 16 Gbit/s, the node bandwidth will be limited by the VM bandwidth. You need to purchase multiple VMs to run concurrently to reach 16 Gbit/s.

- Disk I/O and resource contention

1.12 What Are the Advantages of Object Storage over SAN and NAS Storage?

- SAN storage provides LUNs or volumes for applications. LUNs and volumes are forms of disk storage. Upper-layer applications use Fibre Channel or iSCSI protocols to access SAN storage. SAN storage focuses on disk management. For other purposes, SAN storage must rely on upper-layer applications.
- NAS storage provides file systems or folders for applications. Upper-layer applications use NFS or CIFS protocols to access NAS storage. Directory trees of file systems must be maintained.
- Object storage is suitable for web applications. A massive bucket storage space is provided based on a URL address to store a wide range of file objects. Object storage adopts a flat architecture. Users do not need to maintain complex file directories. There is no need to worry about running out of storage because the storage a bucket can provide is practically unlimited.

1.13 Can Folders in OBS Be Used the Same Way as in a File System?

No.

OBS does not involve files or folders like in a file system. For your convenience, OBS provides a way to simulate folders. On OBS Console, you can simulate a folder by adding a slash (/) to the name of an object, which is then displayed as a folder.

1.14 What Are the Differences Between OBS, EVS, and SFS?

Table 1-3 compares OBS, EVS, and SFS.

Table 1-3 Comparison between OBS, EVS, and SFS

Dimension	OBS	EVS	SFS
Concept	OBS provides massive, secure, reliable, and cost-effective data storage for users to store data of any type and size.	EVS provides scalable block storage that features high reliability, high performance, and robust specifications for ECSs to meet service requirements in different scenarios. An EVS disk is similar to a hard disk on a PC.	SFS provides on-demand high-performance file storage, which can be shared by multiple ECSs. SFS is similar to a remote directory for a Windows or Linux machine.
Data storage logic	Stores objects. Files can be stored directly to OBS. The files automatically generate corresponding system metadata. You can also customize the metadata if needed.	Stores binary data and cannot store files directly. To store files on an EVS disk, you need to format the file system first.	Stores files. Data is sorted and displayed in files and folders.
Access mode	You can access OBS over the Internet or using Direct Connect. Just specify the bucket address and use a transmission protocol, for example, HTTP or HTTPS.	EVS disks need to be attached to an ECS or a BMS and initialized before the ECS or BMS can be used and accessed by your applications.	SFS systems need to be mounted to an ECS or a BMS and then the ECS or BMS can be accessed using NFS or CIFS protocols. A network address must be specified or mapped to a local directory for access.

Dimension	OBS	EVS	SFS
Application scenario	Big data analysis, static website hosting, online video on demand (VoD), gene sequencing, and intelligent video surveillance	HPC, enterprise core cluster applications, enterprise application systems, and development and testing **NOTE** HPC: High-speed and high-IOPS storage is required, such as industrial design and energy exploration.	High-performance computing (HPC), media processing, file sharing, content management, and web services **NOTE** HPC: High bandwidth is required for shared file storage, such as gene sequencing and image rendering.
Capacity	Exabytes	Terabytes	Petabytes
Latency	Milliseconds	1 to 2 ms	3 to 10 ms
IOPS/TPS	Tens of millions	128,000 for a single disk	10,000 for a single file system
Bandwidth	TB/s	MB/s	GB/s
Data sharing supported	Yes	Yes	Yes
Remote access supported	Yes	No	Yes
Online editing supported	No	Yes	Yes
Used independently	Yes	No	Yes

Dedicated Enterprise Storage Service (DESS) provides out-of-the-box dedicated storage services with the same performance and reliability as that in private cloud environments. It is ideal for enterprises' mission-critical applications such as Oracle RAC and SAP HANA TDI. For more information about DESS, see **DESS Introduction**.

Dedicated Distributed Storage Service (DSS) provides dedicated physical storage resources. It features high availability, durability, and low latency, based on technologies such as data redundancy and cache acceleration. For more information about DSS, see **What Is Dedicated Distributed Storage Service?**

1.15 How Do I Determine Whether I Am Accessing OBS over an Intranet?

Suppose you have an ECS and an OBS bucket (named **example-bucket**) in the CN-Hong Kong region.

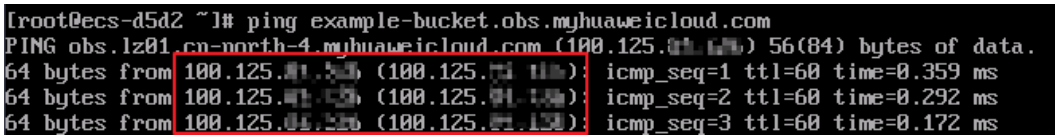
To check whether you are using an intranet for access, do as follows:

On the ECS, **ping** the global domain name of the bucket you are accessing. If the IP address that responds is in the IP address range starting with **100** or **214**, you are accessing the bucket from the ECS over a local intranet connection.

The global domain name of an OBS bucket is in the *Bucket name*.**obs.myhuaweicloud.com** format.

For example, you could ping **example-bucket.obs.myhuaweicloud.com** on the ECS.

Figure 1-2 Responses



1.16 Will My Bucket Performance Be Affected by Other Users' Services?

No.

- OBS buckets are isolated from each other, ensuring that their storage performance remains unaffected by one another.
- OBS ensures that access from different accounts is isolated, preventing any performance interference or impact between them.

1.17 Why Is My Data on the OBS Bucket Overview Page Inconsistent?

Background

OBS statistics on the **Overview** page of a bucket are inconsistent. Do as follows to go to the overview page:

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and choose **Storage** > **Object Storage Service**.

Step 3 In the navigation pane of **OBS Console**, choose **Object Storage**.

Step 4 In the bucket list, click the bucket you want to operate. The **Objects** page is displayed.

Step 5 In the navigation pane, choose **Overview**.

----End

On the **Overview** page of a bucket, you can view the usage of resources in the bucket, including the storage, traffic, and requests. There may be data inconsistency. The details are described as follows:

Data Inconsistency Description

The total storage is not equal to the sum of the Standard storage, Infrequent Access storage, and Archive storage. The possible causes are as follows:

- **Inconsistent data sources**: The total storage is provided by OBS in real time. The storage of Standard, Infrequent Access, or Archive is provided by Cloud Eye.
- **Total storage ≤ Sum of the Standard storage, Infrequent Access storage, and Archive storage**
  - When the total storage is obtained, the storage of some buckets may fail to be obtained.
  - Your account has granted you (an IAM user) the permissions for an enterprise project. Then, what you see is the total storage of only some buckets (the buckets you have permissions for). However, the storage of Standard, Infrequent Access, or Archive covers all buckets in your account.
  - There may be SFS 3.0 buckets in your account. The total storage does not cover this type of buckets, but the storage of Standard, Infrequent Access, and Archive does.
- **Total storage ≥ Sum of the Standard storage, Infrequent Access storage, and Archive storage**
  - Some data is not reported by OBS to Cloud Eye.

The number of GET or PUT requests on the Overview page is different from that in the bill obtained from Billing Center. The possible causes are as follows:

- On the **Overview** page, POST or HEAD requests are not counted. However, Billing Center takes POST requests as PUT requests and HEAD requests as GET requests.
- LIST requests are taken as GET requests on the OBS **Overview** page, but as PUT requests in Billing Center.

The total number of requests is not equal to the sum of GET, PUT, and DELETE requests. The possible causes are as follows:

In addition to GET, PUT, and DELETE requests, the total number of requests covers that of other types of requests such as POST and HEAD.

1.18 What Can I Do If There Are Packet Loss and Network Instability Problems In Cross-Border Data Transfer Scenarios?

In cross-border data transfer scenarios, your network may be located at the edge node of the carrier network, and the success rate of requests to the carrier network is low. As a result, packet loss and network instability may occur.

You are advised to use **Cross-Region Replication** or **Cloud Connect** to transfer data to a region in the country where you need to access and download the data.

2 Billing

2.1 Why Does My Bucket Generate Storage Costs Even Though There Are No Objects in It?

OBS storage space is billable. In addition to objects, deleted objects and fragments in a bucket all take up storage space.

Checking for Deleted Objects

What Is a Deleted Object?

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. The **Objects** page is displayed.

Step 3 On the displayed page, click the **Deleted Objects** tab to view the deleted objects in the bucket.

To permanently delete these objects, select all deleted objects and click **Delete** above the list.

----End

Checking for Fragments

Deleting Fragments

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. The **Objects** page is displayed.

Step 3 On the displayed page, click the **Fragments** tab to view the fragments in the bucket.

To clear up fragments, select all fragments and click **Delete** above the list.

----End

2.2 Why Does My Bucket Generate Traffic When There Are No Objects in It?

Principle for Generating Data Traffic

Sending requests to OBS generating data traffic when the requests or responses contain message bodies.

Traffic Types

OBS traffic is classified into inbound intranet traffic, outbound intranet traffic, inbound internet traffic, outbound internet traffic, cross-region replication traffic, and pull traffic. Not all traffic is billed. For details, see **Billing Overview**.

In What Situations Is Traffic Generated When There Are No Objects in a Bucket?

- Traffic is tallied once every hour. During this period, another user may have uploaded an object to the bucket and then deleted it. You would be billed for that traffic even though the bucket is currently empty.
- There could be multipart upload fragments in the bucket. Though fragments have not yet been merged into objects, they still generate traffic. You can list multipart tasks in the bucket or go to OBS Console to check if there are fragments.
- A request to OBS fails with a 4*xx* error, and the server returns a response body that generates traffic.
- Operations, such as configuring bucket ACLs and configuring lifecycle rules, contain message bodies that generate data traffic.

Monitoring OBS Data Traffic

You can enable Cloud Eye to monitor OBS operations, so that you can have a clear understanding about statistics including data traffic. For details, see **Monitoring OBS**.

Why Am I Billed on a Pay-per-Use Basis Even If I Have Resource Packages?

For more information, see **Why Am I Still Being Billed After I Purchased a Resource Package?**

2.3 Why Am I Still Being Billed After I Purchased a Resource Package?

Problem Description

You have purchased a yearly/monthly OBS resource package, but you are still being billed for pay-per-use usage.

Problem Analysis

Possible causes are described here in order of how likely they are to occur. To locate the root cause as fast as possible, go through the list in order, from most likely to least.

If the fault persists after a possible cause is rectified, move down the list to the next most likely cause.

Figure 2-1 Analysis process

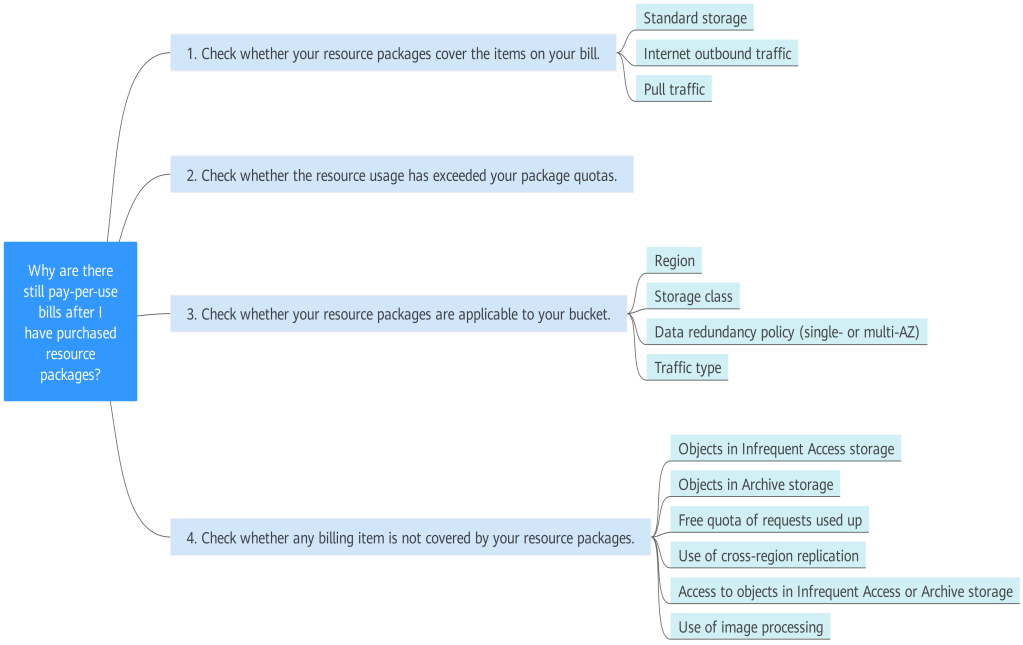


Table 2-1 Problem Analysis

Possible Cause	Solution
No applicable resource package was purchased.	For details, see **Checking If There Are Applicable Resource Packages Available**.
Your resource package quota has been used up.	For details, see **Checking If a Resource Usage Has Exceeded Your Package Quota**.
Your resource package cannot be used for the billed bucket.	For details, see **Checking If Your Resource Package Can Be Used for Your Bucket**.
Your resource package does not cover all of the OBS billing items.	For details, see **Checking If There Are Any Billing Items Not Covered by Your Resource Package**.

Checking If There Are Applicable Resource Packages Available

Packages are provided only for Standard storage, outbound internet traffic, and data restoration traffic.

Resource packages can be used to cover the fees generated by only the corresponding billing items. For details, see **Resource Package Overview**. Check whether you have purchased resource packages that can cover the items in the pay-per-use bills.

If you do not have such resource packages, you may be billed for pay-per-use usage. If you already have such resource packages, it may be a quota issue.

Checking If a Resource Usage Has Exceeded Your Package Quota

If the actual usage of the month exceeds your package quota, you will be billed for subsequently used resources on a pay-per-use basis. **Viewing Resource Package Details**

You can use multiple resource packages together. If your package quota is insufficient, you can purchase additional resource packages to supplement your existing quota. However, quotas of newly purchased resource packages cannot be applied to resources that have already been used.

If your resource usage has exceeded your resource package quota, you will be billed for subsequent usage on a pay-per-use basis. If the resource usage is within your resource package quota, it may be that the package you purchased cannot be used with the bucket you intended to apply it to.

Checking If Your Resource Package Can Be Used for Your Bucket

For billing items that support yearly/monthly packages, the quotas can only be applied to a purchase where the region, storage class, and data redundancy policy of the resource package are consistent with those of the bucket. Otherwise, pay-per-use billing is used for your resource usage. A traffic package can be used to pay for traffic fees only in specific scenarios.

Check the following properties:

1. **Region**

   The resource package and the bucket should be in the same region. If they are not, create a bucket in the resource package's region or purchase another resource package in the region where the bucket resides.

2. **Storage class**

   OBS provides Standard resource packages, which can only be used for objects stored in Standard storage class. Objects in a bucket may have different storage classes as the bucket. If you want to use your resource package quota for storage usage, make sure that the storage class of your resource package is same as that of the stored objects.

3. **Data redundancy policy (single-AZ or multi-AZ)**

   A Standard storage package comes with either multi-AZ or single-AZ data redundancy policy. Check if your bucket data redundancy policy is consistent with that of your resource package. If they are not the same, then the package cannot be used for that bucket. For details about how to view the data redundancy policy of a bucket, see **Viewing Basic Information of a Bucket**.

4. **Traffic type**

   OBS provides outbound internet traffic packages and pull traffic packages.

  - An outbound Internet traffic package can be used to cover the fees incurred by downloading data from OBS to a local device over an Internet connection.
  - A pull traffic package can be used to cover the fees incurred by data transferred by CDN when an OBS bucket is used as a CDN origin server.

  If you need to use the outbound Internet traffic or pull traffic, ensure that you have corresponding resource packages to cover these billing items.

Any of these issues can result in pay-per-use fees being generated. If you can rule out these four possibilities, the next step is to check if the charges are being generated by billing items not covered by your resource package.

Checking If There Are Any Billing Items Not Covered by Your Resource Package

OBS billing items include storage, Internet traffic, requests, data retrievals, and data processing.

However, packages are provided only for the following resources: Standard storage, internet outbound traffic, and data restoration traffic.

- Standard storage packages can offset the used Standard storage space.
- Internet outbound traffic packages and pull traffic packages can offset data traffic volume used for downloading data from OBS and pulling content from OBS over the internet.

Standard storage packages offer some free requests, but any other billing items are not covered by resource packages. These billing items include storage of objects in the Infrequent Access or Archive storage class, cross-region replication traffic, data retrievals, and data processing.

For details, see **OBS Billing Items**.

Pay-per-use bills are generated if:

- you have objects stored in the Infrequent Access storage class.
- you have objects stored in the Archive storage class.
- your free quotas of requests are used up, but requests are still initiated. For details, see **Requests**.
- you have used the cross-region replication function, with corresponding traffic being generated.
- you have accessed objects stored in Infrequent Access or Archive storage class.
- you have used the image processing function.

Submitting a Service Ticket

If the problem persists, **submit a service ticket** to contact Huawei Cloud customer service for assistance.

Helpful Link

Resource Package Purchase

2.4 Why Am I Still Being Billed for Pull Traffic Used by CDN Acceleration When I Already Have a Pull Traffic Package?

- Check whether the purchased pull traffic package and the bucket configured as the origin server on CDN are in the same region.
  a. Log in to OBS Console.
  b. In the navigation menu on the top, choose **Resources** > **My Resources** to check the region of your pull traffic package.
  c. Log in to the CDN console. Click **Domain Name Management**, and click the domain name that uses the OBS bucket as its origin server. On the **Basic Settings** tab page, and under the **Primary Origin Server**, check the address of the bucket, which can tell you what region the bucket is in.
  d. Check whether the pull traffic package and the bucket are in the same region. If they are in different regions, purchase another pull traffic package from the region where the bucket is located.
- Log in to the CDN console, check the configuration for domain name acceleration to see if the origin server type is an OBS bucket domain name. If the origin server type is an IP address or a domain name, the OBS pull traffic package will not cover the pull traffic.

2.5 Why Are OBS Resources Still Unavailable Even Though My Account Has a Valid Payment Method and There Are No Outstanding Bills?

On the **Overview** page of Billing Center, check whether your account has an outstanding amount.

- If your account has an outstanding amount, your payment failed or was not enough. To prevent related resources from being stopped or released, you need to pay immediately. For details, see **Top-Up and Repayment**.
- If your account has no outstanding amount but your resources are still unavailable, **submit a service ticket**.

2.6 Do I Have to Purchase a Resource Package? Can I Apply a Package to a Specific Bucket?

You can use OBS even if you have not purchased any resource packages. Without using resource packages, you will be billed on a pay-per-use basis. After you purchase a resource package, you can use it to cover the fees for using OBS. Using resource packages is more cost-effective than the pay-per-use billing. It is recommended that you purchase resource packages based on your needs.

Resource packages are currently managed by type and region. For example, after you purchase a resource package in a region, this package can be used to cover

the fees generated by all buckets in that region as long as these buckets meet certain requirements. Therefore, there is no mapping between resource packages and buckets, and you cannot apply a resource package to a specific bucket.

CAUTION

OBS has multiple billing items. Even if you already have a resource package, there may be also other fees generated before the resource package is used up. If you are still being billed for pay-per-use usage when you are using a resource package, see **Why Am I Still Being Billed After I Purchased a Resource Package?** for troubleshooting.

2.7 Can I Unsubscribe from or Modify a Resource Package?

Once a resource package is purchased, it cannot be unsubscribed from or modified. Resource packages are currently managed by region, storage class, and others. To use a resource package for fee deduction, ensure that the region and storage class of a bucket match those of the resource package, or you will be billed on a pay-per-use basis.

CAUTION

- After a bucket is created, its data redundancy policy (single-AZ or multi-AZ storage) cannot be modified. Configure the data redundancy policy based on your service needs when purchasing or creating a bucket.
- If the storage class of your resource package is different from that of the bucket, change the bucket's storage class to be the same as that of your resource package. For details, see **Configuring Storage Class for a Bucket**.
- After a bucket is created, the region where the bucket locates cannot be changed. Select a region corresponding to your services during bucket creation. If the bucket and resource package are in different regions, and you want to migrate data from the source bucket to a new bucket in the region where the resource package locates, asynchronously migrate data across regions (for details, see **Configuring Cross-Region Replication**) or use obsutil to replicate objects (for details, see **Copying an Object**).

2.8 What Can I Do If My Resource Package Expires?

After your resource package expires, you can renew it to extend its validity period. For details, see **Resource Package Renewals**. If your resource package is not renewed, you will be billed on a pay-per-use basis later. With pay-per-use billing, you can continue using OBS as long as your account has enough balance.

NOTE

If your account is in arrears, your data stored in OBS will be retained, and your account will be suspended. During the retention period, pay-per-use resources cannot be accessed or used. If your outstanding amount is not paid off when the retention period ends, data stored in OBS will be deleted and cannot be recovered.

2.9 Do Parallel File Systems Support Resource Packages?

Parallel file systems currently support the following types of resource packages:

- Standard storage packages: including the types of single-AZ and multi-AZ
- Archive storage packages
- Outbound Internet traffic packages

NOTE

Cross-region replication traffic and pull traffic packages are currently not available for parallel file systems.

2.10 How Are Requests Counted?

Each calling of an API is counted as a request. When you perform operations on OBS through OBS Console, tools, APIs, or SDKs, you are actually calling APIs.

Request Types

OBS requests fall into the following types:

- Read requests: GET (for downloading objects), HEAD (for obtaining bucket locations or bucket policies), LIST (for listing objects), and others
- Write requests: PUT/POST (for uploading objects), COPY (for copying objects), and others
- Delete requests: DELETE (for deleting objects or canceling multipart uploads) and others
- Storage class transition requests: requests generated when objects are transitioned from Standard to Infrequent Access or Archive or from Infrequent Access to Archive during the execution of a lifecycle rule

Billing

Requests are billed on a pay-per-use basis. The unit prices for different types of requests are the same. For details, see **Product Pricing Details**.

If you buy a Standard storage package, you will receive a free quota of read and write requests for each month. The free quota is used first. After the free quota is used up, subsequent requests are billed on a pay-per-use basis. If you continue to purchase additional Standard storage packages, the free requests rewarded to you will be accumulated.

NOTE

Except the requests whose status code returned by the server is 5*XX* or 403, all other requests are counted in the number of requests.

Examples

Example 1

Take object upload for example. Each time you upload an object or an object part is counted as a request. Assuming that a folder has 100 objects:

- If you call the PutObject API to upload all objects, sending 100 PUT requests means that the number of requests is 100.
- If you use multipart upload tasks to upload the large objects in the folder, the final number of requests is greater than 100, because the processing of object parts will increase the number of requests. In addition, extra requests are required for initializing multipart upload tasks and merging parts into objects.

Example 2

Each operation on OBS Console delivers a request that is counted for billing.

For example, when you open the home page of OBS Console, the list of buckets is loaded. In this process, requests are sent to obtain the bucket list and bucket locations. Then when you switch to the **Overview** page of a bucket, requests are sent to query bucket storage information and bucket metadata.

Example 3

Take object download as an example. Each time you download an object is counted as a request. Assume that you need to download 100 objects:

- Downloading 100 Standard or Infrequent Access objects will send 100 GET requests.
- If these 100 objects are in the Archive storage class and direct reading is not enabled, you need to restore the objects before downloading them. Restoring 100 Archive objects to the Standard storage class will generate 100 PUT requests. Then, downloading the restored 100 Standard objects will send another 100 GET requests. In this case, there are 200 requests in total.
- If these 100 objects are in the Archive storage class and direct reading is enabled, you can directly download the objects without restoring them first. In such case, only 100 GET requests will be sent.

2.11 Can I Purchase Requests?

Currently, requests cannot be purchased separately.

Requests are billed on a pay-per-use basis. You will be billed based on the number of GET, PUT, and storage class transition requests. Requests include PUT, POST, COPY, LIST, GET, and HEAD.

2.12 Will My Data Write Be Restricted When My OBS Package Has Been Used Up?

No.

An OBS bucket provides unlimited storage. Any usage beyond the package quota will be billed on a pay-per-use basis, but you can also purchase additional resource packages. For details, see **Purchase of Additional Resource Packages**.

2.13 Will the Remaining Package Quota in a Given Month Be Carried over to the Following Month?

No.

Monthly reset rules for resource packages:

Reset by subscription period means that after a resource package is purchased, its quota will reset at 24:00:00 on the same day (the purchase day) of each month. For example, after you purchase an Internet outbound traffic package of 2 TB (each month) for 6 months on April 15, you will have 2 TB Internet outbound traffic available to use from April 15 to 24:00:00 of May 15. Then, at 00:00:00 on May 16, another 2 TB outbound Internet traffic will be allocated to you, so you can use this 2 TB traffic between 00:00:00 on May 16 and 24:00:00 on June 15. The following months follow the same rule until the purchased package expires. If you do not use up your quota in a given month, the remaining quota will not be carried over to the following month. The quota resets every month.

Note that if you purchase a resource package on January 28, the quota will reset at 00:00:00 on March 1 because there are only 28 days in February. Also, in the months following March, the quota still resets on the first day of a given month.

2.14 Which Types of Resource Packages Will Reset Their Quota by Month and Which Types Will Not?

Resource packages that will reset their quota by month:

- Outbound Internet traffic packages
- Pull traffic packages

The following resource packages are valid within a specific period and will not reset their quota by month.

- Standard storage packages

NOTE

- Monthly quota reset: For example, if you purchase a 10 TB outbound Internet traffic package for one year, you will have 10 TB traffic available **each month** in this year. After the 10 TB of a month is used up, you will be billed for the subsequent usage in that month on a pay-per-use basis. If you do not use up your quota in a given month, the remaining quota will not be carried over to the following month. The quota resets every month.
- No monthly quota reset: For example, if you purchase a 10 TB standard storage package for one year, it can be used to cover the fees for storing 10 TB data at most **within a year**. After this 10 TB quota is used up, you will be billed for the subsequent usage on a pay-per-use basis.

2.15 Do I Need to Purchase an Outbound Internet Traffic Package If I Already Have a Pull Traffic Package?

A pull traffic package can be used for data that CDN downloads from OBS buckets when those OBS buckets are used as origin sites for CDN.

An outbound internet traffic package can be used for traffic for data transferred from OBS to local devices over the internet.

The following explains which type of data traffic is used in different scenarios:

- Outbound internet traffic is generated when you download objects from or otherwise query buckets (for instance, listing objects and obtaining bucket or object metadata) on OBS Console. Using various software tools or SDKs to download objects over the Internet without CDN acceleration will also generate outbound internet traffic.
- Accessing a bucket through its access domain name generates outbound internet traffic.
- Suppose that you use an OBS bucket as the origin server of a CDN acceleration domain name, and set the origin server type to **Domain name**. Accessing that accelerated domain name generates outbound internet traffic, which is then billed by OBS and CDN, when the CDN cache is not hit.
- If the origin server type is set to **OBS bucket**, accessing the accelerated domain name consumes the quota of your OBS pull traffic package and counts as CDN traffic when the CDN cache is not hit.

If your application scenario involves a lot of data being transferred over the internet, outbound internet traffic packages are also recommended. If you do not expect to generate much outbound internet traffic, you can choose to not buy a package and pay for traffic on a pay-per-use basis.

2.16 Why Is There a Charge of $0.01 USD on My OBS Bill?

If your bill contains a record of $0.01 USD, there may be small-amount accumulation.

The minimum cost billed is $0.01 USD. If you spend less than $0.01 USD per hour, small-amount accumulation will be triggered. If the accumulative amount is still less than $0.01 USD at the end of the day, the amount accumulation continues the next day. There will not be any cost until the accumulative amount is greater than or equal to $0.01 USD.

Suppose you send 10 upload requests and 10 download requests from 08:00 to 09:00 the first day, which incurs less than $0.01 USD. At the end of the day and of the second day, the amount is still less than $0.01 USD. At 09:00 of the third day, the accumulative amount reaches $0.01 USD. The system then will deduct $0.01 USD from your account at about 10:00.

There is an SDR delay. Generally, pay-per-use usage can be billed by hour, day, or month. After bills are created, corresponding costs will be deducted from your account. If no records can be found, the billing period might not have ended.

2.17 Why Is There a Large Amount of Outbound Internet Traffic in My Bill?

The outbound Internet traffic of OBS consists of:

- **Outbound Internet traffic for Standard storage**: This type of traffic is generated when Standard objects are downloaded and listed over the Internet.
- **Outbound Internet traffic for Infrequent Access storage**: This type of traffic is generated when the restored Infrequent Access objects are downloaded over the Internet.
- **Outbound Internet traffic for Archive storage**: This type of traffic is generated when the restored Archive objects are downloaded over the Internet.
- **Outbound Internet traffic for Deep Archive storage**: This type of traffic is generated when the restored Deep Archive objects are downloaded over the Internet.

To reduce the outbound Internet traffic, you can do as follows:

- Disable public read (if enabled) for the bucket.

  If public read is enabled for a bucket, anyone can access the bucket and download any object from it. This will generate a large amount of outbound Internet traffic.

  You are advised to **make the entire bucket private**. If needed, you can **configure public read for a single directory or object** and then **share the object's URL** with others for access.
- Enable logging and configure a bucket policy.

  After enabling logging for your bucket, you can analyze the logged IP addresses that sent requests to your bucket after a period of time. If the IP addresses are fixed and do not need to access the objects in your bucket, you can configure a bucket policy to **deny access to your bucket from those IP addresses**.
- Configure URL validation using a whitelist or blacklist.

Check the logs generated at a point in time when there is a large number of requests in the bill. Then, search for the Referer field of the request source and **configure URL validation**.

3 Access Control

3.1 Why Is the Message "Access denied" Still Appearing After OBS System Permissions or Bucket Read and Write Permissions Are Allowed?

Cause

- **OBS system permissions**

  System permissions such as OBS ReadOnlyAccess, OBS OperateAccess, and **OBS Buckets Viewer** configured in IAM only allow certain OBS operations. For example, the OBS OperateAccess permission lets you list buckets, obtain basic bucket information, obtain bucket metadata, list objects (excluding versioned objects), upload, download, delete objects, and obtain object ACLs.

- **Bucket read and write permissions**

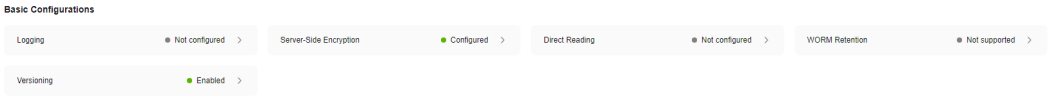
  If you use a bucket policy to grant users the bucket read and write permissions, the users have the permissions to:

  - GetObject: Download objects.
  - GetObjectVersion: Download objects and their versions.
  - PutObject: Upload objects.
  - DeleteObject: Delete objects.
  - DeleteObjectVersion: Delete objects and their versions.

Each API requires an operation permission. Users can call these APIs directly or through SDKs. However, when users log in to OBS Console or OBS Browser+, APIs, such as ListAllMyBuckets and ListBucket, are called to load the bucket list and object list. Some other APIs are also called on other pages. But their permissions do not cover those APIs. In such case, the message is displayed.

For example, loading the bucket's overview page involves API calls to query the configuration statuses of lifecycle and CORS rules. See **Figure 3-1**. However, the preset system permissions do not cover these operations.

Figure 3-1 Basic bucket configurations



Solutions

Authorized permissions are valid, though operations on the console or client are restricted. You can call the APIs directly or through SDKs.

When the OBS OperateAccess permission or bucket read and write permissions are allowed, you can upload or download objects on OBS Console or OBS Browser+.

If you do not want those error messages to appear, you can configure **OBS custom policies** on the IAM console to grant more OBS permissions to a user group, and add the user who requires the permissions to this group.

Why Can't I List Objects on OBS Console Even If I Have Been Granted the OBS OperateAccess and OBS ReadOnlyAccess Permissions?

System policies OBS OperateAccess and OBS ReadOnlyAccess contain only **obs:bucket:ListBucket** (used to list objects), but do not contain **obs:bucket:ListBucketVersions** (used to list multiple versions of objects).

If a bucket has multiple versions of objects, IAM users may fail to list objects in the bucket through OBS Console. In such case, IAM users need to be granted the obs:bucket:ListBucketVersions permission.

3.2 Why Can't I Access OBS (403 AccessDenied) After Being Granted with the OBS Access Permission?

Problem Description

By configuring IAM permissions, bucket policies, or bucket ACLs, you have been granted the permissions needed to access OBS. However, when you try to access OBS, the error message **Access denied** or **403 AccessDenied** is displayed.

Problem Analysis

Possible causes are described here in order of how likely they are to occur. To locate the root cause as fast as possible, go through the list in order, from most likely to least.

If the fault persists after a possible cause is rectified, move down the list to the next most likely cause.

NOTE

OBS provides multiple ways to control permissions. To better understand how permissions management works, read **Introduction to OBS Permissions Management**. For details about how to configure permissions for different scenarios, see **Typical Permissions Management Scenarios**.

Figure 3-2 Analysis process

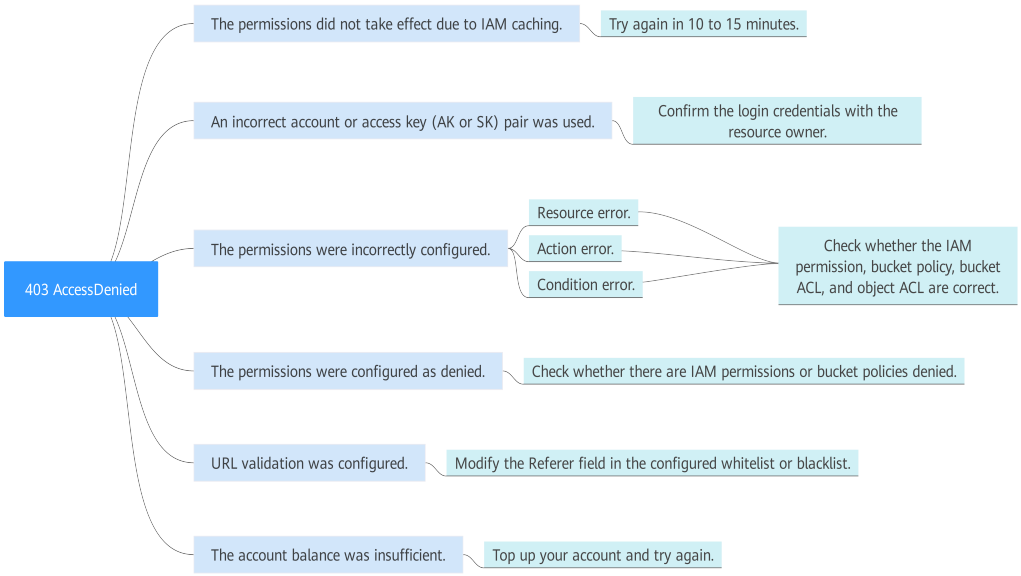


Table 3-1 Problem Analysis

Possible Cause	Solution
The permissions did not take effect due to IAM caching.	Due to data caching, it can take about 10 to 15 minutes for a new IAM permission configuration to take effect. Try again in 10 to 15 minutes.
An incorrect account or access key (AK or SK) was used to access OBS.	If you do not have the permissions needed to access OBS, the login information, such as the account or AK/SK used was likely incorrect. Incorrect use of AK/SK is more common. For example, you may be using an AK/SK or password for a different account. Confirm the login credentials with the resource owner.
The permissions were incorrectly configured.	For details, see **Checking Whether Permissions Are Correctly Configured**.
The permissions were configured as denied.	For details, see **Checking Whether a Permission Is Configured as Denied**.
URL validation was configured.	Modify the Referer field in the whitelist or blacklist by referring to **Configuring URL Validation**.
The account balance was insufficient.	Top up your account and try again. For details, see **Topping Up an Account**.

Checking Whether Permissions Are Correctly Configured

OBS provides multiple mechanisms for permissions management, and in some scenarios there may be dependencies involved. If you cannot access OBS, contact the person who assigned the permissions (usually the resource owner) to check whether the permissions were configured correctly. There are two critical elements to check: **Resources** (what resources are authorized) and **Actions** (what operations are authorized). For common known mistakes, see **Table 3-2**. If **Condition** is configured in the IAM permission or bucket policy, check whether the specified rules are met.

Table 3-2 Commonly seen mistakes in configuring **Resources** and **Actions**

Type	Common Mistake
Resources	• You were granted access to a given bucket but tried to access a different bucket. • You were granted access to a bucket but not to the objects in that bucket. • You were granted access to view a bucket but not to perform any operations (for example, listing objects in the bucket). • You were only granted access to certain objects in a bucket but tried to access other objects.
Actions	• Actions configured incorrectly: For example, the download permission (GetObject) may have been mistakenly assigned instead of the upload permission (PutObject). • Required actions are missing from the configuration: Some permissions required by OBS Console or OBS Browser+ for other actions are often ignored. The most often ignored actions are **ListAllMyBuckets** and **ListBucket**, which are needed for viewing a list of the buckets and of the objects in those buckets. Typical examples are described in: **Why Is the Message "Access denied" Still Appearing After OBS System Permissions or Bucket Read and Write Permissions Are Allowed?**

Checking IAM permissions

1. Use the resource owner's account to log in to Huawei Cloud and click **Console** in the upper right corner.
2. On the management console, hover over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.
3. On the **Users** page, search for the name of the user that could not access OBS. Click the name to check which user group the user belongs to.

4. On the **User Groups** page, search for the user group to which the user belongs. In the **Operation** column of the user group, click **Manage Permissions** to see which IAM permissions have been granted.

Checking the bucket policy

1. Use the resource owner's account to log in to Huawei Cloud and click **Console** in the upper right corner.
2. In the service list, choose **Storage** > **Object Storage Service**.
3. In the bucket list, search for the bucket that fails to be accessed and click the bucket name. The **Objects** page is displayed.
4. In the navigation pane, choose **Permissions** > **Bucket Policies** to view the configured bucket policies.

Checking the bucket ACL

1. Use the resource owner's account to log in to Huawei Cloud and click **Console** in the upper right corner.
2. In the service list, choose **Storage** > **Object Storage Service**.
3. In the bucket list, search for the bucket that fails to be accessed and click the bucket name. The **Objects** page is displayed.
4. In the navigation pane, choose **Permissions** > **Bucket ACL** to view the configured bucket ACL.

Checking the object ACL

1. Use the resource owner's account to log in to Huawei Cloud and click **Console** in the upper right corner.
2. In the service list, choose **Storage** > **Object Storage Service**.
3. In the bucket list, search for the bucket that fails to be accessed and click the bucket name. The **Objects** page is displayed.
4. In the object list, search for the object that fails to be accessed and click the object name. On the page that is displayed, view the object ACL configuration on the **Object ACL** tab.

Checking Whether a Permission Is Configured as Denied

If the required permissions are correctly configured but OBS still cannot be accessed, the possible cause is that the permission effect is configured as denied.

Based on the **principle of least-privilege**, decisions default to deny, and an explicit deny statement always takes precedence over an allow statement. If there are multiple IAM permissions or bucket policies, as long as there is an explicit deny statement, it will take precedence over allow statements, even the denied permissions are allowed in other bucket policies.

Both IAM permissions and bucket policies can include deny statements, so you need to check these configurations separately.

Checking IAM permissions

1. Use the resource owner's account to log in to Huawei Cloud and click **Console** in the upper right corner.

2. On the management console, hover over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.
3. On the **Users** page, search for the name of the user that could not access OBS. Click the name to check which user group the user belongs to.
4. On the **User Groups** page, search for the user group to which the user belongs. In the **Operation** column of the user group, click **Manage Permissions** to see which IAM permissions have been granted.

Checking the bucket policy

1. Use the resource owner's account to log in to Huawei Cloud and click **Console** in the upper right corner.
2. In the service list, choose **Storage** > **Object Storage Service**.
3. In the bucket list, search for the bucket that fails to be accessed and click the bucket name. The **Objects** page is displayed.
4. In the navigation pane, choose **Permissions** > **Bucket Policies** to view the configured bucket policies.

Submitting a Service Ticket

If the problem persists, **submit a service ticket** to contact Huawei Cloud customer service for assistance.

3.3 What Is the Relationship Between a Bucket Policy and an Object Policy?

An object policy takes effect on only one object in a bucket. A bucket policy takes effect on the configured bucket and multiple or all objects in the bucket.

3.4 How Do I Control Access to Folders in an OBS Bucket?

You can customize a bucket policy and specify a prefix in it to control access to folders.

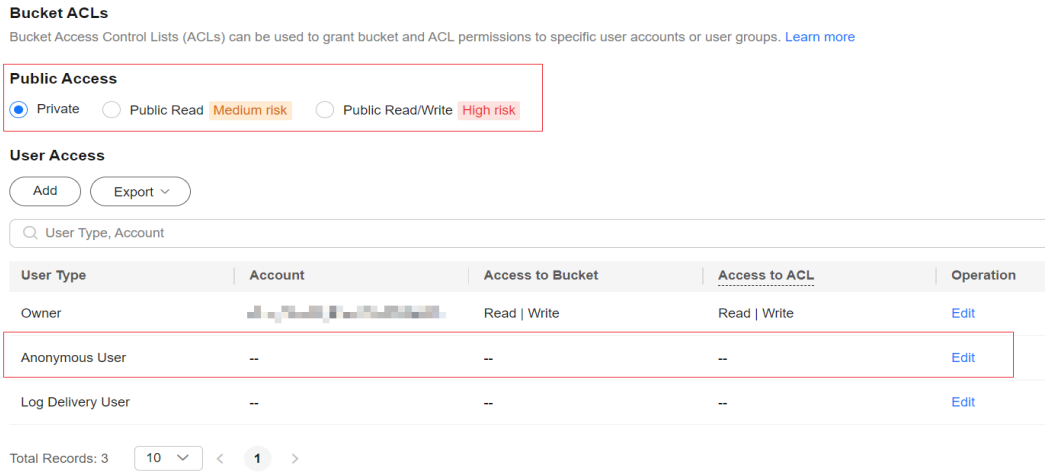
For example, if the prefix is set to **abc/**, configured permissions will apply to folder **abc**.

For details, see **Creating a Custom Bucket Policy (Visual Editor)**.

3.5 Why Was the Value of the delivered Parameter Changed to false After I Configured the Bucket ACL for Anonymous Users on the OBS Console?

- OBS Console currently does not support configuring the bucket ACL inheritance for anonymous users. You can only use OBS **SDKs** or **APIs** to configure the bucket ACL inheritance, indicated by the **delivered** parameter.
- If you have configured the **delivered** parameter for anonymous users using the SDKs or APIs and then modified the ACL for them on the console, the value of the **delivered** parameter will be changed to **false**. On the console, the ACL for anonymous users will be modified if either of the following actions is taken:
  - Modify **Public Access**.
  - **Edit** the ACL for **Anonymous User** in the **User Access** area.

Figure 3-3 Modifying the ACL for anonymous users



4 Buckets and Objects

4.1 Why Am I Unable to Create a Bucket?

- If the number of created buckets has reached 100 (the maximum number allowed), delete some unneeded buckets and try again.
- If the new bucket name already exists, use another one and try again. Each OBS bucket name must be globally unique. Specifically, it must be different from that of buckets created by its owner or by any other users (including those under other Huawei Cloud accounts).
- Check whether you are using the name of a bucket that was deleted within the past 30 minutes. After a user deletes a bucket, neither the user nor other users (including other Huawei Cloud accounts) can immediately reuse the name of the deleted bucket to create another bucket or parallel file system. They must wait at least 30 minutes before reusing the bucket name, or the creation will fail.
- If message "A conflicting operation is being performed on this resource. Try again later." is displayed when you are creating a bucket, it 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 due to arrears in a short period. In such case, try another bucket name.
- Check whether the account has required permissions. If not, grant the account permissions as needed.
  a. Log in to the management console.
  b. On the top navigation menu, click the username and select **Identity and Access Management** to log in to the IAM console and verify the permissions of the user.
     i. On the **Users** page, search for the username.
     ii. Click the username to view details for that user, and check the user groups where the user belongs. If the user is not a member of any user group, click **Modify** and select a user group.
     iii. In the navigation pane, click **User Groups** and find the user group to which the user belongs. Click the icon of the downward arrow next to the user group name to view user group permissions. Find **OBS** under the **Project Name** column and click **View** under the

Operation column, to check whether the user group has the permission required to create buckets. If not, **create a user group**, configure a policy that grants the user group the bucket creation permission, and add the user to this group.

- Check whether the account is in arrears or the account balance is insufficient. If this is the case, pay off the outstanding balance or top up the account.
  a. Log in to OBS Console.
  b. On the top navigation menu, click **Billing & Costs** to go to Billing Center.
  c. On the **Overview** page, you can view the balance of the account.
  d. If your account is in arrears, top it up by referring to **Renewal Management**.
  e. If your object upload still fails after the account is brought current, contact customer service.
- Check whether the network connectivity between the local computer and OBS is normal. If the network is faulty, restore the network connection.
- If the failure is not caused by any of the described reasons, you can check the returned error code to try to find the reason.

4.2 Why Am I Unable to Upload an Object?

- Check whether the size or number of objects to be uploaded exceeds what is supported.

  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.

  A single file as large as 5 GB can be uploaded as part of a batch upload. For a single file upload, it cannot exceed 50 MB.

  If a file is larger than 5 GB, you can use OBS Browser+ or obsutil to upload it. Or you can use the OBS SDKs or API to upload the file (up to 48.8 TB) with a multipart 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.
- Check whether the network connectivity between the local computer and OBS is normal. If the network is faulty, restore the network connection.
- If a message indicating "service unavailable" is displayed when objects are being uploaded, try again later.
- Check whether the account is in arrears or the account balance is insufficient. If this is the case, pay off the outstanding balance or top up the account.
  a. Log in to OBS Console.
  b. On the top navigation menu, click **Billing & Costs** to go to Billing Center.
  c. On the **Overview** page, you can view the balance of the account.
  d. If your account is in arrears, top it up by referring to **Renewal Management**.

e. If your object upload still fails after the account is brought current, contact customer service.

- Check whether the account has the permissions required to upload objects. This check should cover IAM permissions, bucket policies, and bucket ACLs. If the account does not have the required permissions, grant the permissions first.

  a. Log in to the management console.

  b. On the top navigation menu, click the username and select **Identity and Access Management** to log in to the IAM console and verify the permissions of the user.

     i. On the **Users** page, search for the username.

     ii. Click the username to view details for that user, and check the user groups where the user belongs. If the user is not a member of any user group, click **Modify** and select a user group.

     iii. In the navigation pane, click **User Groups** and find the user group to which the user belongs. Click the icon of the downward arrow next to the user group name to view user group permissions. Find **OBS** under the **Project Name** column and click **View** under the **Operation** column, to check whether the user group has the permission required to upload objects. If not, **create a user group**, configure a policy that grants the user group the object upload permission, and add the user to this group. Alternatively, you can configure a bucket policy to grant the IAM user the permission to upload objects to the bucket. Refer to **c** for more information.

     iv. If the account that attempted to upload files is not the owner of the bucket, take the actions described in **c** to check the bucket policy.

  c. On the top navigation menu, click **Service List** and choose **Object Storage Service**. On the OBS Console page, check whether the bucket to which the object is to be uploaded prevents users from uploading objects.

     i. In the navigation pane, choose **Permissions** > **Bucket Policies** and check whether there is a policy preventing the account or IAM user from uploading objects. If yes, modify the bucket policy to grant the account or IAM user the permission. For details, see **Granting Specific Operation Permissions on a Bucket to Other Accounts** or **Granting an IAM User the Permissions Required to Perform Specific Operations on a Specific Bucket**.

     ii. Alternatively, you can also use the bucket ACL to grant the account write permissions for the bucket. For details, see **Configuring a Bucket ACL**.

- If the fault persists, contact customer service.

4.3 Why Am I Unable to Download an Object?

- Check whether the network connectivity between the local computer and OBS is normal. If the network is faulty, restore the network connection.
- Check whether the account is in arrears or the account balance is insufficient. If this is the case, pay off the outstanding balance or top up the account.

a. Log in to OBS Console.
b. On the top navigation menu, click **Billing & Costs** to go to Billing Center.
c. On the **Overview** page, you can view the balance of the account.
d. If your account is in arrears, top it up by referring to **Renewal Management**.
e. If your object upload still fails after the account is brought current, contact customer service.

- Check whether the account has the permissions needed to download objects from the bucket. This check should cover IAM permissions, bucket policies, object policies, bucket ACLs, and object ACLs. If the account does not have the required permissions, grant the permissions first.
  a. Log in to the management console.
  b. On the top navigation menu, click the username and select **Identity and Access Management** to log in to the IAM console and verify the permissions of the user.
     i. On the **Users** page, search for the username.
     ii. Click the username to view details for that user, and check the user groups where the user belongs. If the user is not a member of any user group, click **Modify** and select a user group.
     iii. In the navigation pane, click **User Groups** and find the user group to which the user belongs. Click the icon of the downward arrow next to the user group name to view user group permissions. Find **OBS** under the **Project Name** column and click **View** under the **Operation** column, to check whether the user group has the permission required to download objects. If not, **create a user group**, configure a policy that grants the user group the object download permission, and add the user to this group. Alternatively, you can configure a bucket policy to grant the IAM user the permission to download objects from the bucket. Refer to **c** for more information.
     iv. If the account that attempted to download files is not the owner of the bucket, take the actions described in **c** to check the bucket policy.
  c. On the top navigation menu, click **Service List** and choose **Object Storage Service**. On the OBS Console page, check whether the bucket from which the object is to be downloaded restricts users from downloading objects.
     i. In the navigation pane, choose **Permissions** > **Bucket Policies** and check whether there is a policy that restricts the account or IAM user to download objects. If yes, modify the bucket policy to grant the account or IAM user the permission. For details, see **Granting Specific Operation Permissions on a Bucket to Other Accounts** or **Granting an IAM User the Permissions Required to Perform Specific Operations on a Specific Bucket**.
     ii. Alternatively, you can also use the bucket ACL to grant the account write permissions for the bucket. For details, see **Configuring a Bucket ACL**.
- Check whether the current object is encrypted with KMS. If the object is encrypted, downloading it from OBS Console, OBS Browser+, or obsutil will fail. To download it by using an SDK or API, the decryption key must be provided.

- Check whether the object is in the Archive storage class. If it is and the status is **Unrestored**, restore the object first.
- If the fault persists, contact customer service.

4.4 Why Can't I Delete a Bucket?

Problem Description

A bucket cannot be deleted.

Problem Analysis

Possible causes are described here in order of how likely they are to occur. To locate the root cause as fast as possible, go through the list in order, from most likely to least.

If the fault persists after a possible cause is rectified, move down the list to the next most likely cause.

Figure 4-1 Analysis process

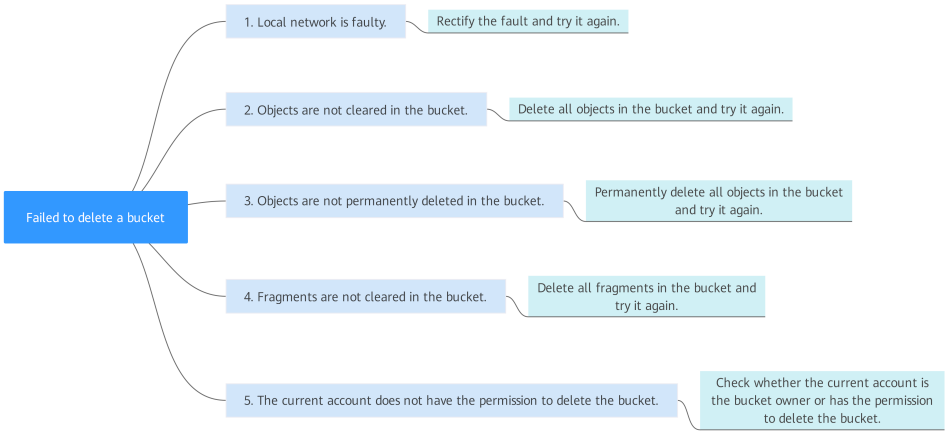


Table 4-1 Problem Analysis

Possible Cause	Solution
Local network is faulty.	Check whether the network connectivity between the local computer and OBS is normal. If the network is faulty, restore the network connection.
There are objects in the bucket.	For details, see **Deleting Objects in a Bucket**.

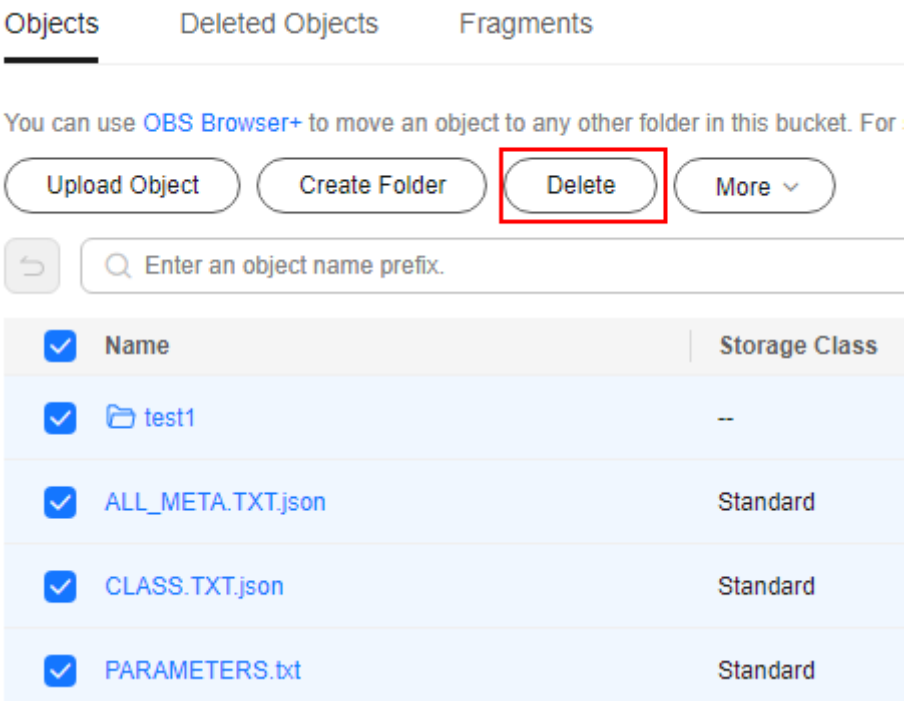
Possible Cause	Solution
There are objects that were not permanently deleted from the bucket.	For details, see **Permanently Deleting Deleted Objects from a Bucket**.
There are object fragments in the bucket.	For details, see **Deleting Fragments from a Bucket**.
The current account does not have the permissions required to delete the bucket.	For details, see **Checking Whether the Current Account Has the Permission to Delete the Bucket**.

Deleting Objects in a Bucket

The following procedure describes how to manually delete objects from a bucket on OBS Console. For details about the deletion using other methods (obsutil or SDKs), see **Deleting an Object**. You can also use the **lifecycle management** to batch delete all objects in a bucket.

1. In the bucket list on OBS Console, click the bucket you need to delete objects from. The **Objects** page is displayed.
2. Select all of the objects and click **Delete** above the object list.

Figure 4-2 Deleting all objects



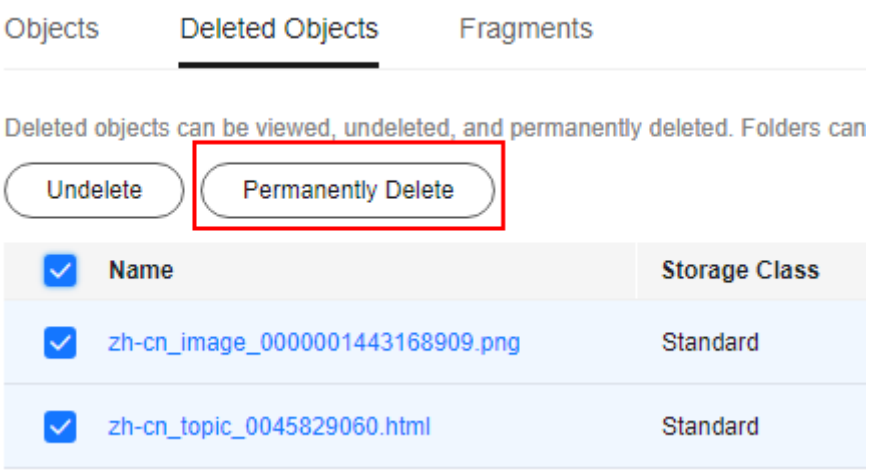
After all objects are deleted, try to delete the bucket again. If the bucket still cannot be deleted, go to the next step.

Permanently Deleting Deleted Objects from a Bucket

If versioning is or was enabled for a bucket, deleted objects may still exist in the bucket. In this case, you need to permanently delete deleted objects in the bucket. For details about deleted objects, see **Deleting an Object**.

1. In the bucket list on OBS Console, click the bucket you want to permanently delete the deleted objects from. The **Objects** page is displayed.
2. Click the **Deleted Objects** tab. The deleted object list is displayed.
3. Select all deleted objects and click **Delete** above the list.

Figure 4-3 Deleting all deleted objects



After all deleted objects are permanently deleted, try to delete the bucket again. If the bucket still cannot be deleted, check the bucket for fragments.

Deleting Fragments from a Bucket

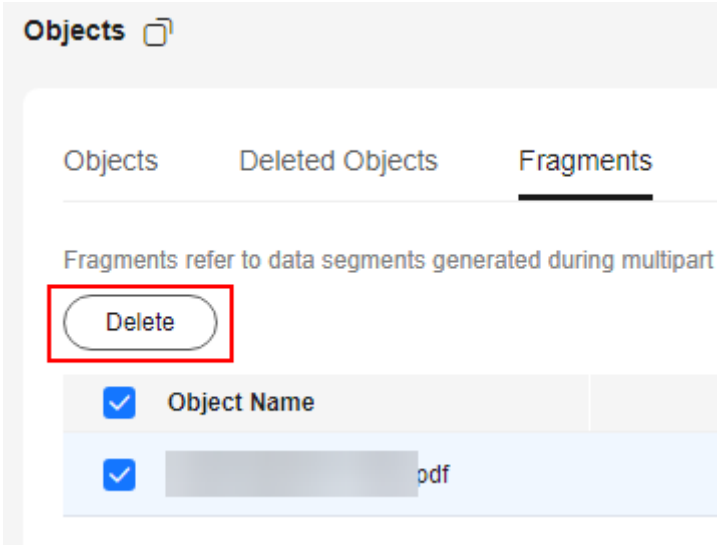
Fragments refer to incomplete data in a bucket. Data is uploaded to OBS in multipart mode. In the following common and other scenarios, an upload fails and fragments are generated. You can clear these fragments to free up storage space.

- 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.

The following describes how to manually delete fragments on OBS Console. For details about how to delete fragments in other ways, see **Managing Fragments**.

1. In the bucket list on OBS Console, click the bucket containing fragments. The **Objects** page is displayed.
2. Click the **Fragments** tab. The fragment list is displayed.
3. Select all fragments and click **Delete** above the list.

Figure 4-4 Deleting all fragments



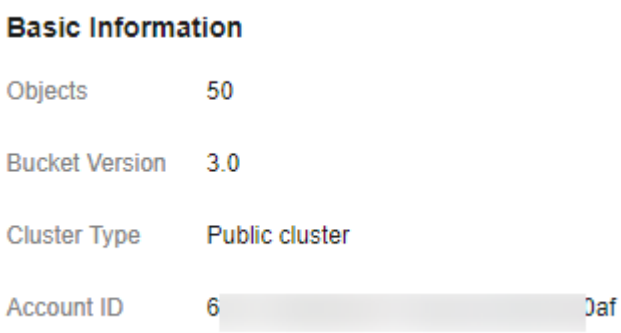
After deleting all fragments, try deleting the bucket again. If the bucket still cannot be deleted, you may need to check the permissions.

Checking Whether the Current Account Has the Permission to Delete the Bucket

By default, only the bucket owner has the permission needed to delete a bucket. However, the bucket owner can also grant other users this permission (**DeleteBucket**).

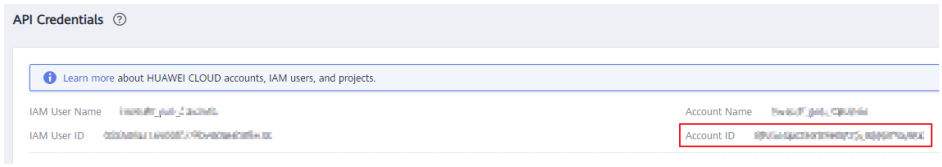
1. Check whether the current account that you use is the bucket owner.
   a. In the bucket list on OBS Console, click the bucket you want to delete. The **Objects** page is displayed.
   b. In the navigation pane, choose **Overview**.
   c. In the **Basic Information** area, find the account ID (the bucket owner's account ID).

      Figure 4-5 Viewing the bucket owner

   d. Move the mouse over your username displayed in the upper right corner. Choose **My Credentials** from the drop-down list, and find the account ID.

Figure 4-6 Viewing the current account ID



- If the current account ID is consistent with the bucket owner account ID, and you logged in to the console using that account, not as an IAM user, then the current account is the bucket owner. If the bucket still cannot be deleted, submit a service ticket to get technical support.
- If the two account IDs are inconsistent, or you logged in to the console as an IAM user, then you are not the bucket owner. In this case, continue to the next step.

2. Contact the bucket owner to check whether the user you are using has been granted the permission to delete the bucket.
   - If the user does not have the permission, ask the bucket owner to grant it.
   - If the user has the permission to delete the bucket but still cannot delete the bucket, submit a service ticket to get technical support.

Submitting a Service Ticket

If the problem persists, **submit a service ticket** to contact Huawei Cloud customer service for assistance.

4.5 Why Can't I Delete an Object?

Problem Description

An existing object cannot be deleted.

Problem Analysis

Possible causes are described here in order of how likely they are to occur. To locate the root cause as fast as possible, go through the list in order, from most likely to least.

If the fault persists after a possible cause is rectified, move down the list to the next most likely cause.

Table 4-2 Problem analysis

Possible Cause	Solution
Local network is faulty.	Check whether the network connectivity between the local computer and OBS is normal. If the network is faulty, restore the network connection.
The current account does not have the permissions required to delete the object.	See **Checking Whether the Current Account Has the Permission to Delete the Object**.
The bucket where the object is stored has versioning enabled.	See **Permanently Deleting an Object from the Deleted Objects List**.
The deleted object is within the WORM retention period.	See **Permanently Deleting an Object in the WORM Retention Period**.
The deleted folder has lots of objects.	See **Deleting a Folder with Lots of Objects**.
Other	See **Submitting a Service Ticket**.

Checking Whether the Current Account Has the Permission to Delete the Object

If the "Insufficient permissions. Contact the administrator." message is displayed when you are trying to delete the object, do as follows:

1. Check whether the ACL of the bucket has write access configured.
   a. In the bucket list on OBS Console, click the bucket you need to delete the object from. The **Objects** page is displayed.
   b. In the navigation pane, choose **Permissions** > **Bucket ACL**.
   c. In the **Access to Bucket** column, check whether the **Write** access is configured for the required user type.

   Figure 4-7 Checking the write access

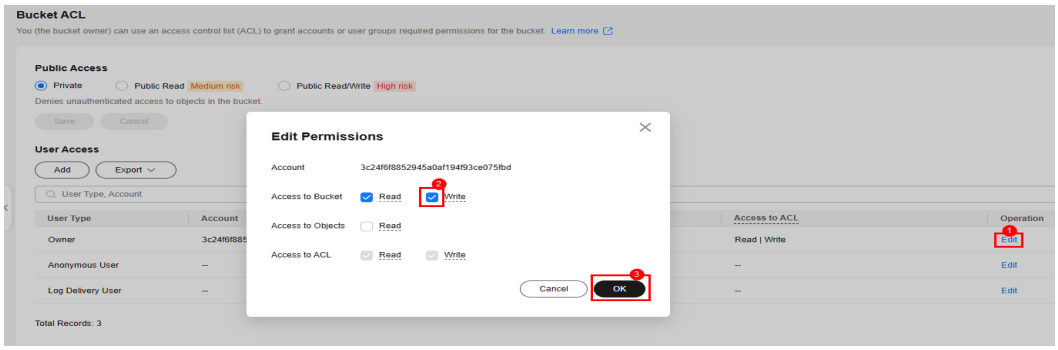
   

   - If the write access is displayed but the object still cannot be deleted, go to **Step 3**.

- If there is no write access displayed, go to **Step 2**.

2. Grant the write access to the required user type.
   a. Locate the user type and click **Edit** in the **Operation** column.
   b. In the dialog box that is displayed, select **Write** for **Access to Bucket**.
   c. Click **OK**.

Figure 4-8 Granting the write access



3. Ask the bucket owner whether the **DeleteObject** or **DeleteObjectVersion** permission is granted in the bucket policy.
   - If the required permission is not granted, ask the bucket owner to grant them.
   - If the object still cannot be deleted after the required permission is granted, **submit a service ticket** for help.

Permanently Deleting an Object from the Deleted Objects List

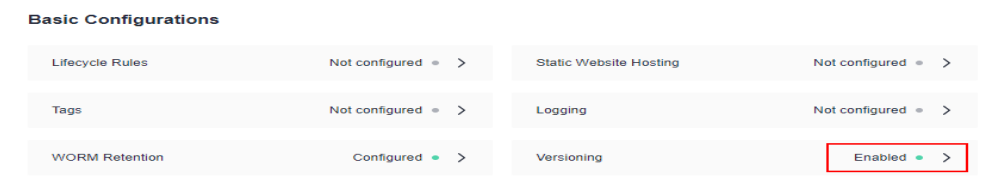
NOTE

If an object is stored in a bucket with versioning enabled, deleting this object will only move the object to the **Deleted Objects** list, and the object will still incur charges. To stop being billed, you need to delete the object permanently.

If an object has a WORM retention policy configured, delete it permanently by referring to **Permanently Deleting an Object in the WORM Retention Period**.

1. Check whether the bucket where the object is stored has versioning enabled.
   a. In the bucket list on OBS Console, click the bucket you need to delete the object from. The **Objects** page is displayed.
   b. In the navigation pane, choose **Overview**.
   c. In the **Basic Configurations** area, check the versioning status.

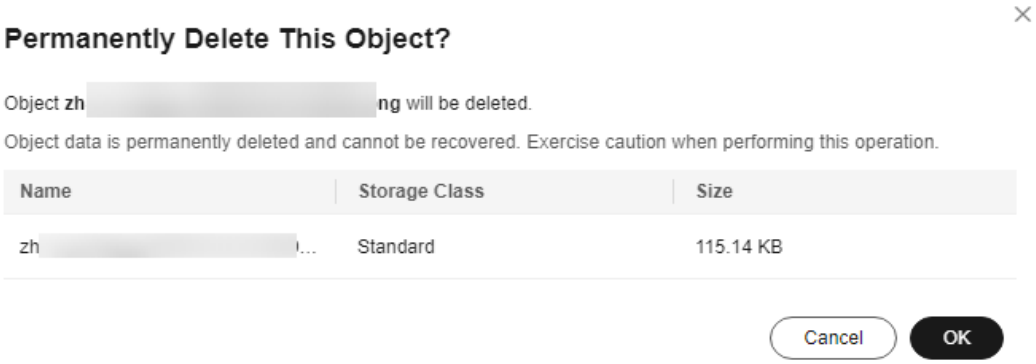
Figure 4-9 Checking the versioning status



- If versioning is enabled for the bucket, go to the next step.
- If versioning is disabled or suspended for the bucket but the object still cannot be deleted, **submit a service ticket** for help.

2. Permanently delete an object.
   a. Click the **Deleted Objects** tab. The deleted object list is displayed.
   b. Locate the object and click **Permanently Delete** in the **Operation** column.
   c. Click **OK**.

Figure 4-10 Permanently deleting an object



Permanently Deleting an Object in the WORM Retention Period

In the **Deleted Objects** list, objects that are within the WORM retention period can only be permanently deleted after their retention policy expires. For details about how to delete such an object, see **Manually and Permanently Deleting Objects from a WORM-Enabled Bucket** or **Using a Lifecycle Rule to Delete Objects from a WORM-Enabled Bucket**.

To view the WORM retention period of an object, go to the details page of the object and choose the **Versions** tab. Find the object version and choose **More** > **Extend Retention Period**. In the displayed dialog box:

- If the object version is within the retention period, you can view how long the object version will remain protected, as shown in **Figure 4-11**.
- If the retention period of the object version has expired, you can view how long the object version has not been protected, as shown in **Figure 4-12**.
- If the object version has no retention policy configured, there is no retention information displayed, as shown in **Figure 4-13**.

Figure 4-11 Object version within the WORM retention period

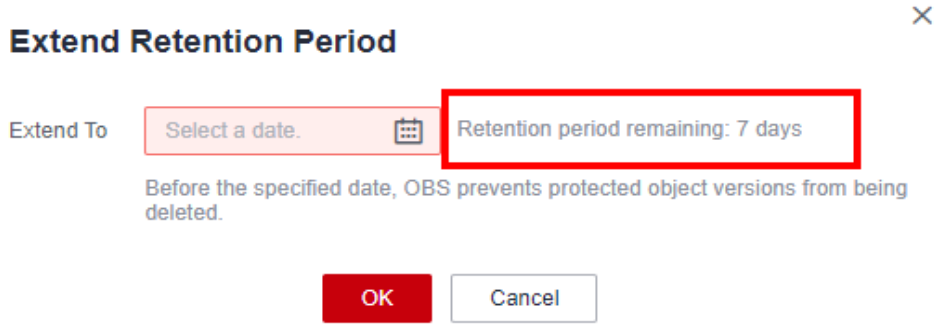


Figure 4-12 Object version whose WORM retention has expired

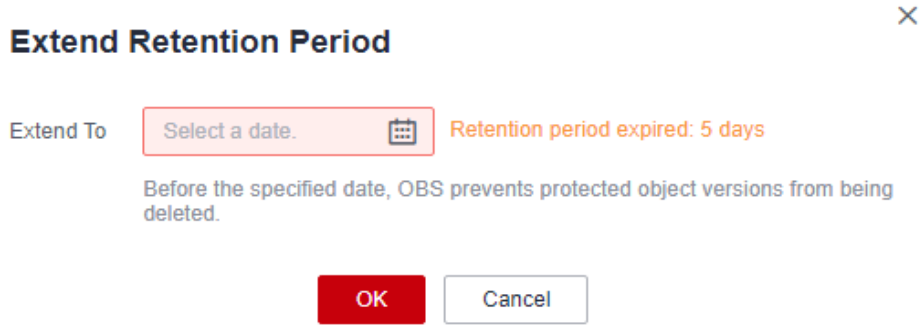
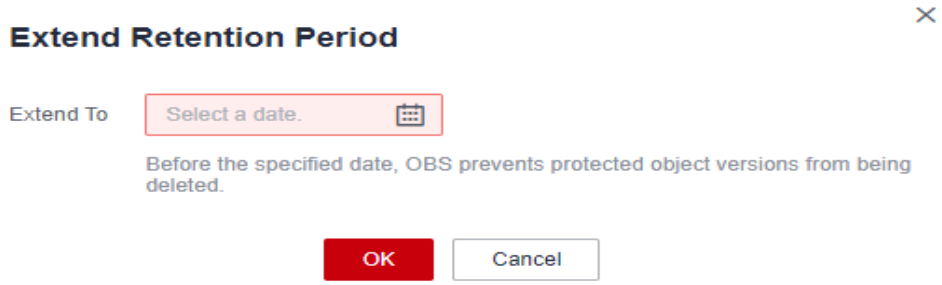


Figure 4-13 Object version with no WORM retention policy



Deleting a Folder with Lots of Objects

To delete objects on OBS Console is to list objects and then delete them. If a folder has lots of objects or lots of levels of subfolders, deleting it on OBS Console may time out. To avoid such issues, obsutil is recommended for you to delete a folder containing lots of objects or lots of levels of subfolders. For details, see **Deleting an Object**.

Submitting a Service Ticket

If the problem persists, **submit a service ticket** to contact Huawei Cloud customer service for assistance.

4.6 Why Can't I Access an Object Through Its URL?

NOTE

This case describes the scenario where an object cannot be accessed using its URL. If you can use a URL to download an object, but cannot use the URL to preview the object, resolve the issue by referring to **How Do I Preview OBS Objects in My Web Browser?**

If you are the owner of the object and cannot access the object using its URL, check the following items:

- If your object URL is customized, check whether it contains forbidden characters. For details, see **Guidelines on Naming Object Keys**.
- If you are using a user-defined domain name, check whether your domain name has been mapped to the OBS bucket's domain name. For details, see the part for configuring a CNAME record on the DNS in **Binding a User-Defined Domain Name**.

If the object URL is provided by others, contact the object owner for the following items:

- Check whether the object is encrypted. If it is, that is normal. An encrypted object cannot be shared. If the object owner wants to share that encrypted object, the object should be deleted and then uploaded again without the encryption settings.
- If the object URL is generated by sharing, check whether the sharing has expired. If it does, share the object and set the validity period again. This can be performed by the object owner on OBS Console or OBS Browser+. You can determine whether an object URL is generated by sharing based on its format. For details, see **Sharing an Object**.

Tool	Configuration
OBS Console	**Sharing an Object**
OBS Browser+	**Sharing a File**

- If the object URL is in the format of *BucketName*.*Endpoint*/*ObjectName*, for example, *bucketname*.**obs.ap-southeast-1.myhuaweicloud.com/object.txt**, the object URL is not generated by sharing. In this case, check whether the user has been granted object access permissions. Check the bucket policy, bucket ACL, object policy, and object ACL. If the user does not have required permissions, grant them to the user.

  You can use the following tools to grant permissions:

Tool	Configuration
OBS Console	**Configuring a Bucket ACL**, **Configuring a Bucket Policy**, **Configuring an Object ACL**, and **Configuring an Object Policy**
OBS Browser+	-

Tool	Configuration
obsutil	**Setting Bucket Properties** and **Setting Object Properties**
SDKs	Section about using URL to authorize access permissions in the **SDK Reference**
API	**Configuring a Bucket ACL**, **Configuring a Bucket Policy**, and **Configuring an Object ACL**

- Check whether a URL validation whitelist or blacklist has been configured for the bucket storing the object.

4.7 How Do I Preview OBS Objects in My Web Browser?

Context

For security and compliance purposes, Huawei Cloud OBS prohibits the preview of objects in a bucket by using the default OBS domain name (**a bucket domain name or static website domain name**). When you use such a domain name to access objects (such as videos, images, and web pages) in a browser, no content will be displayed. Instead, the content is downloaded as an attachment.

The effective time and supported regions are as follows:

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

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

Troubleshooting

Use a user-defined domain name to preview objects.

The following solutions are available:

Solution 1: Use a User-Defined Domain Name

Solution 2: Use a User-Defined Domain Name and CDN

Solution 3: Use Private Bucket Retrieval on CDN

NOTE

If you have bound a user-defined domain name to a bucket and enabled CDN acceleration, but the objects are still directly downloaded without object preview, handle the problem by referring to **With CDN Acceleration Enabled, Why Are the Objects in My OBS Bucket Directly Downloaded When I Access Them?**

Solution 1: Use a User-Defined Domain Name

NOTE

Solution advantages and restrictions

- The bucket policy must be public read, so that all objects in the bucket can be accessed by anonymous users.
- As required by the China's Ministry of Industry and Information Technology (MIIT), you must complete the Internet Content Provider (ICP) filing, if the bucket to which your user-defined domain name is bound is in any of the following regions:

  CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, and CN South-Guangzhou
- HTTP requests are supported. HTTPS requests are not supported.

Procedure

Step 1 Bind a user-defined domain name to the OBS bucket.

For details, see **Accessing a Bucket Using a User-Defined Domain Name**. During the configuration, add a CNAME record set for the OBS bucket domain name.

Step 2 Check whether objects can be previewed in a browser online.

Share an object link formatted in **http://***User-defined domain name***/***Object access path* with other users for them to preview the object.

If the object still cannot be previewed, check whether its metadata **ContentType** is supported by the browser.

For example, **ContentType** should be set to **video/mp4** for an MP4 video or set to **image/jpeg** for a JPG image. For details about all supported **ContentType** values, see **Object Metadata Content-Type**.

You can configure **ContentType** using OBS Console, APIs, or SDKs.

----End

Solution 2: Use a User-Defined Domain Name and CDN

NOTE

Solution advantages and restrictions

- The bucket policy must be public read, so that all objects in the bucket can be accessed by anonymous users.
- As required by the China's Ministry of Industry and Information Technology (MIIT), you must complete the Internet Content Provider (ICP) filing, if the bucket to which your user-defined domain name is bound is in any of the following regions:

  CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, and CN South-Guangzhou
- HTTPS requests are supported. To use HTTPS, you need to import a certificate to CDN. For details, see **Configuring an HTTPS Certificate**.

Procedure

Step 1 On the **CDN console**, add the prepared user-defined domain name as an acceleration domain name.

For details, see **Adding a Domain Name**. Set **Type** to **OBS bucket** and **Address** to the OBS bucket domain name. On the **Advanced Settings** tab of the domain

name's details page, click **Edit** next to **HTTP Headers**. Then, add response header **Content-Disposition** and set its value to **inline**.

Step 2 Bind the user-defined domain name to the OBS bucket.

For details, see **Binding a User-Defined Domain Name**. During the configuration, use the CNAME record set allocated by CDN.

Step 3 Check whether objects can be previewed in a browser online.

Share an object link formatted in **http://***User-defined domain name***/***Object access path* with other users for them to preview the object.

If the object still cannot be previewed, check whether its metadata **ContentType** is supported by the browser.

For example, **ContentType** should be set to **video/mp4** for an MP4 video or set to **image/jpeg** for a JPG image. For details about all supported **ContentType** values, see **Object Metadata Content-Type**.

You can configure **ContentType** using OBS Console, APIs, or SDKs.

Step 4 (Optional) If the preview still fails, resolve the issue by referring to **Method 1** under **Solutions** and try again.

----End

Solution 3: Use Private Bucket Retrieval on CDN

NOTE

Solution advantages and restrictions

- The bucket policy can be public read or private.
- You only need to configure an acceleration domain name on CDN. No user-defined domain name of OBS is required. As required by the China's Ministry of Industry and Information Technology (MIIT), the used acceleration domain name must complete the Internet Content Provider (ICP) filing, if your bucket is in any of the following regions:

  CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, and CN South-Guangzhou
- HTTPS requests are supported. To use HTTPS, you need to import a certificate to CDN. For details, see **Configuring an HTTPS Certificate**.

Procedure

Step 1 On the **CDN console**, add your domain name as an acceleration domain name and set the private OBS bucket as the origin server.

For details, see **Adding a Domain Name**. Set **Type** to **OBS bucket** and **Address** to the OBS bucket domain name. On the **Advanced Settings** tab of the domain name's details page, click **Edit** next to **HTTP Headers**. Then, add response header **Content-Disposition** and set its value to **inline**.

Step 2 Configure the CNAME record set on DNS.

For details, see the CNAME record configuration in **Binding a User-Defined Domain Name**. Use the CNAME record set allocated by CDN.

Step 3 Check whether objects can be previewed in a browser online.

Share an object link formatted in **http://***User-defined domain name***/***Object access path* with other users for them to preview the object.

If the object still cannot be previewed, check whether its metadata **ContentType** is supported by the browser.

For example, **ContentType** should be set to **video/mp4** for an MP4 video or set to **image/jpeg** for a JPG image. For details about all supported **ContentType** values, see **Object Metadata Content-Type**.

You can configure **ContentType** using OBS Console, APIs, or SDKs.

----End

4.8 Can I Rename an Object?

Yes. If you encounter an error when calling the API for renaming an object, handle it by referring to **Error Codes**.

Renaming an Object in a Bucket

You can rename a single object on OBS Browser+.

The specific steps are as follows:

Step 1 **Log in to OBS Browser+**.

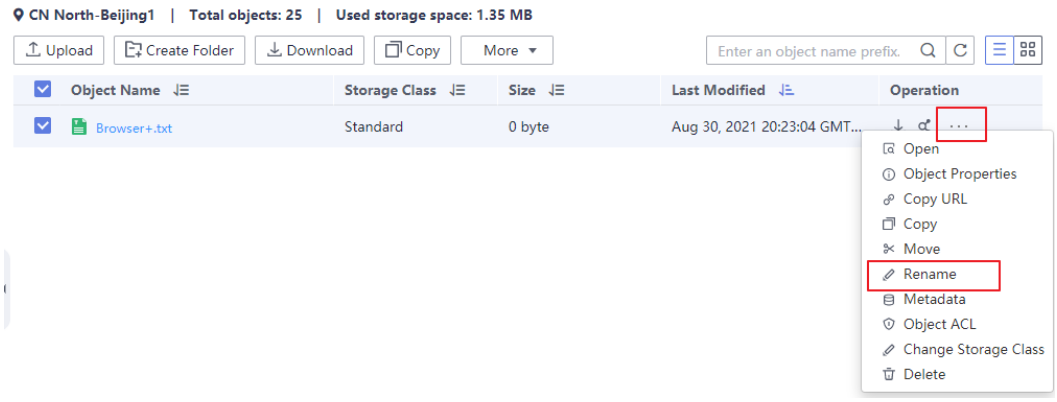
If you have not installed OBS Browser+, **download** and **install** it.

Step 2 In the bucket list, click the name of the bucket that contains the object you want to rename.

Step 3 In the object list, locate the object to be renamed and click ··· in the **Operation** column.

Step 4 Click **Rename**.

Figure 4-14 Renaming an object



Step 5 In the displayed dialog box, enter a new object name and click **OK**.

----End

Renaming a File in a Parallel File System

You can rename files in parallel file systems using APIs, SDKs, or OBS Browser+.

- **Renaming an Object Using an API**
- **Renaming an Object Using the Java SDK**
- Renaming an Object Using OBS Browser+ (Performing the Following Steps)

Step 1 **Log in to OBS Browser+**.

If you have not installed OBS Browser+, **download** and **install** it.

Step 2 In the parallel file system list, click the file system you want.

Step 3 In the file list, locate the file you want to rename and click ··· in the **Operation** column.

Step 4 Click **Rename**.

Step 5 In the displayed dialog box, enter a new file name and click **OK**.

----End

4.9 Can I Edit Objects in OBS Online?

OBS is a cloud storage service. It provides massive, secure, highly reliable, and low-cost data storage capabilities.

Generally, OBS does not support online editing of object content. You can download the object that you want to edit to a local path, modify the object, and then upload it to OBS again.

There are a few exceptions. Online, you can use OBS to:

1. **Modify object metadata**, such as **ContentDisposition** and **ContentLanguage**.
2. Process images stored in OBS. For details, see **Object Storage Service Image Processing Feature Guide**.
3. Add data to the end of an object. For details, see **Appending an Object** in the *Object Storage Service API Reference*.

4.10 How Do I Obtain the Access Path to an Object?

Object access paths use the following format: **https://***{bucket name}*.*{domain name}*/*{object name}*. The following is an example: **https://bucketname.obs.ap-southeast-1.myhuaweicloud.com/objectname**.

You can combine a path manually or use the tools in the following table to obtain it.

Table 4-3 How to obtain an object URL

Tool	Object URL
OBS Console	Click the object and copy the URL for the detailed information of the object.
OBS Browser+	Click the **Attribute** button of the object and then you can copy the URL displayed in the detailed information about the object.
obsutil	Not supported
SDKs	You can get the URL of an object by calling the **getObjectUrl** interface. **NOTE** When uploading an object, you can obtain its URL from the returned value. The URL of an existing object in the bucket cannot be obtained.
APIs	Not supported

NOTE

If the object access path is user-assembled, you need to escape the object name by referring to the URL encoding rules.

Suppose you have a **test** bucket in the CN North-Beijing4 region and the bucket stores an object named **@@obs.png**. When assembling the object access path, you must escape the **@@** in the object name based on URL encoding. After the escaping, the actual object access path should be **https://test.obs.cn-north-4.myhuaweicloud.com/%40%40obs.png**.

4.11 Can I Change the Region of a Bucket?

No.

Once a bucket is created, its region cannot be changed.

4.12 How Do I Change the Enterprise Project Where My Bucket Belongs?

You can group your OBS buckets using enterprise projects or change the enterprise project where your bucket belongs as needed.

To change the enterprise project where your bucket belongs, move your bucket from its enterprise project to another one. For details, see **Removing Resources from an Enterprise Project**.

4.13 Can I Copy a File Between Buckets?

Yes.

You can use APIs, SDKs, OBS Browser+, or obsutil to copy objects in the same region.

- To use APIs, see **Copying an Object**.
- To use SDKs, see **Copying an Object**.
- To use OBS Browser+, see **Copying a File or Folder**.
- To use obsutil, see **Copying an Object**.

If you want to copy objects across regions, see **Configuring Cross-Region Replication**.

4.14 Can I Move a File Between Buckets?

Yes.

You can use OBS Browser+ or obsutil to move files in the same region. You can move a single file or folder to another specified path. After a file or folder is moved, the file or folder in the source path is deleted. For details, see **Moving a File or Folder** or **Moving an Object**.

In addition, you can use OMS to migrate data between OBS buckets across accounts, across regions, or in the same region. For details, see **Using OMS to Migrate Data Between Buckets**.

NOTE

OBS tools cannot move files between parallel file systems in different clusters.

4.15 Can I Upload Objects with the Same Name to the Same Folder?

Yes.

- If versioning is enabled for a bucket, OBS automatically assigns a unique version ID to each object uploaded to the bucket. Objects with the same name are stored in OBS with different version IDs.
- If versioning is not enabled for a bucket, a newly uploaded object in the folder will overwrite the previously uploaded object with the same name.

4.16 Does OBS Support Resumable Transfer?

The following table lists the resumable transfer support for different OBS tools:

Table 4-4 Support for resumable transfer by different OBS tools

OBS Tool	Resumable Data Transfer
OBS Console	Not supported
OBS Browser+	Supported

OBS Tool	Resumable Data Transfer
obsutil	Supported For details, see **Using obsutil for Resumable Data Transfer**.
SDKs	Supported Before using SDK for resumable transfer, you must enable the resumable transfer option. Only in this way, can the progress of the last upload be read when you continue the transfer process again. For the setting details, see the corresponding SDK documentation. **Uploads Using the Java SDK Downloads Using the Java SDK** **Uploads Using the Python SDK Downloads Using the Python SDK** **Uploads Using the C SDK Downloads Using the C SDK** **Uploads Using the Go SDK Downloads Using the Go SDK** **Uploads Using the BrowserJS SDK** **Uploads Using the .NET SDK Downloads Using the .NET SDK** **Uploads Using the Android SDK Downloads Using the Android SDK** **Uploads Using the iOS SDK Downloads Using the iOS SDK** **Uploads Using the Node.js SDK Downloads Using the Node.js SDK**
APIs	Not supported

4.17 Does OBS Support Batch Upload?

The following table lists the batch upload support for different OBS tools:

Table 4-5 Support for batch upload by different OBS tools

Tool	Batch Upload
OBS Console	OBS Console allows you to upload files in a batch. Up to 100 files can be uploaded at a time, with the total size of no more than 5 GB. For details, see **Uploading a File**.
OBS Browser+	Supports batch upload of files and folders. A maximum of 500 files or folders can be uploaded at a time.
obsutil	Supports upload of a single folder with the maximum size of 48.8 TB. For details, see **Uploading an Object**.
SDKs	Not supported
APIs	Not supported

4.18 Does OBS Support Batch Download?

The following table lists the batch download support for different OBS tools:

Table 4-6 Support for batch download by different OBS tools

Tool	Batch Download
OBS Console	Not supported
OBS Browser+	Supported For details, see **Downloading a File or Folder**.
obsutil	Supported. For details, see **Downloading Objects**.
SDKs	Not supported
APIs	Not supported

4.19 Can I Batch Delete Objects or Empty a Bucket in OBS?

The following table lists the batch deletion support for different OBS tools:

Table 4-7 Support for batch deletion by different OBS tools

Tool	Batch Deletion
OBS Console	Supported. A maximum of 100 objects can be deleted at a time. If you are deleting a folder, only one folder can be deleted at a time. For details, see **Deleting an Object**. You can also specify **Delete Objects After (Days)** in a lifecycle rule to delete objects in batches or empty buckets. For details, see **Configuring a Lifecycle Rule**.
OBS Browser+	Supported. Files and folders can be deleted in a batch, and the number of files and folders to be deleted is not limited. For details, see **Deleting a File or Folder**.
obsutil	You can delete objects in batches by prefix. For details, see **Deleting an Object**.
SDKs	Supported. A maximum of 1,000 objects can be deleted at a time. For details, see **SDK Reference**.

Tool	Batch Deletion
APIs	Supported. A maximum of 1,000 objects can be deleted at a time. For details, see **Deleting Objects**.

NOTE

The batch deletion performance is negatively correlated with the number of objects in a single request. When it comes to QPS, deleting *N* objects is counted as *N* operations. If a large number of objects named with prefixes in lexicographic order are deleted, lots of requests may be concentrated in a specific partition, which results in hot access. This limits the request rate in the hot partition and increases access delay.

To address this problem, you can reduce the number of objects in a single batch deletion request, initiate more concurrent requests, and name objects with random prefixes.

4.20 What If an Object Can't Be Found in a Bucket or a 403 Error Is Returned?

Check whether what you entered for search is an object name prefix.

On OBS Console and OBS Browser+, you can search for objects by object name prefix. For example, if you search for **test**, you will find all objects whose name starts with **test**.

However, if the keyword entered is in the middle or at the end of the object name, the search will not return those results. For example, you want to search for **testabc** and you enter **abc** in the search box, **testabc** will not be found. Only objects whose name starts with the prefix **abc** will be found.

If you encounter a 403 error when accessing an object, you lack the **obs:bucket:ListBucket** permission for listing objects in the bucket and obtaining the bucket metadata. If the accessed object does not exist, a 404 error will be returned.

4.21 What Should I Do If an Error Message Is Displayed When I Use Internet Explorer to Access an Object URL That Contains Chinese Characters?

Description

HTTP 400 error is returned when using the Internet Explorer to access an object URL that contains Chinese characters?

Handling Method

By default, the Internet Explorer does not use the UTF-8 to send query strings. To solve this problem, change the default configuration of the Internet Explorer.

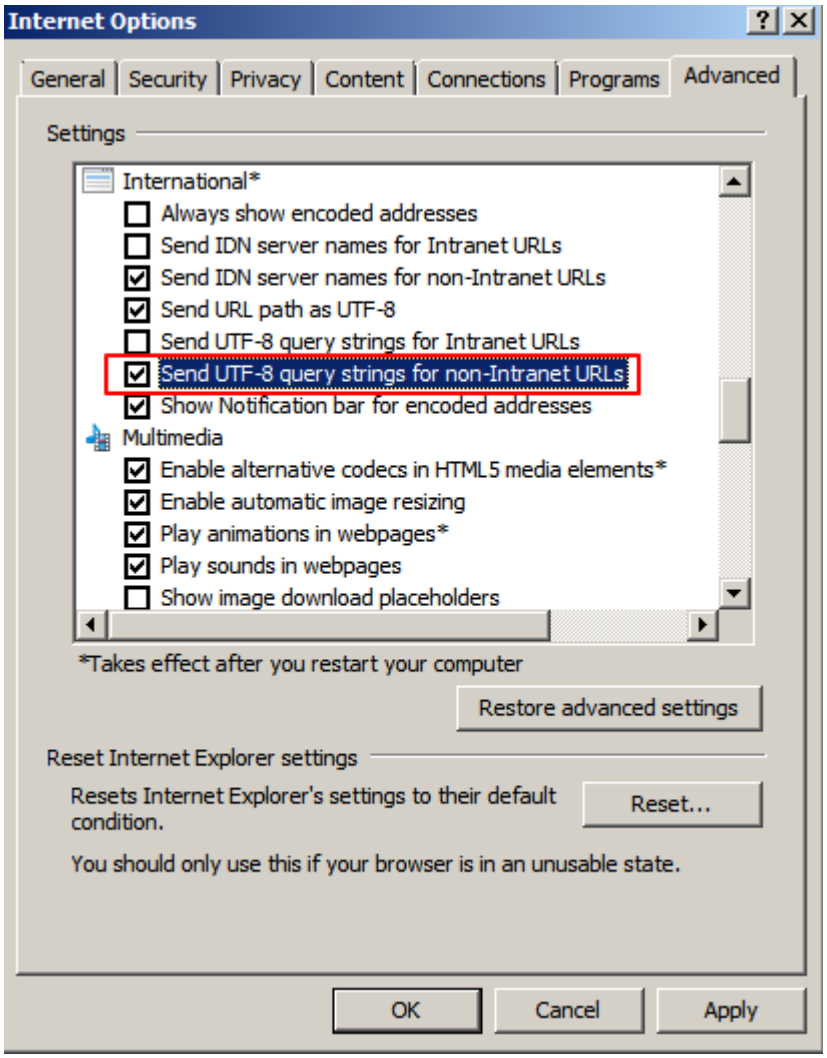
Procedure

Step 1 Open Internet Explorer, for example, IE 11.

Step 2 Click **Settings** in the upper right corner of the browser and choose **Internet Options** > **Advanced**.

Step 3 Select **Send UTF-8 query string for non-Internet URLs**, as shown in the following figure.

Figure 4-15 Changing IE default settings



Step 4 Click **Apply**, and then click **OK**.

Step 5 Restart Internet Explorer.

Then, you can properly access the object URL.

----End

4.22 Why Is an Error Reported Even If OBS CORS Has Been Configured?

- Check whether the CORS rule is correctly configured by referring to **Configuring CORS**.
- Response headers are cached for the same URL. The result of the first simple request will be cached even if the request does not contain the CORS header. When the URL is accessed for the second time, the first response result is used and CORS is generated. This issue is caused by the browser mechanism.

  Use either of the following methods to try to resolve this issue:

  a. Add random parameters to the end of the requested resource URL. For example, **1.html?a=1** is displayed after a random parameter is added to **1.html**.

  b. Set **Cache-Control** to **no-cache** in the object metadata.

  c. Press **Ctrl+Shift+Delete** to clear the browser cache.

4.23 How Do I Query the Size of a Folder in a Bucket?

Run the **object list command with obsutil**. In this command, specify the prefix to the name of the folder to be queried.

Take Linux as an example. Run the **./obsutil ls obs://bucket-test/test/ -du -limit=0** command to query the size of the **test** folder in bucket **bucket-test**.

```
./obsutil ls obs://bucket-test/test/ -du -limit=0

Start at 2023-03-16 06:40:18.2773873 +0000 UTC

Listing objects .

Remove the -du parameter to view more information
[DU] Total prefix [test/] size: 990.85MB
```

NOTE

Only obsutil 5.4.6 and later support **-du** and earlier versions can only use **-limit=0**, so the latest version of obsutil is recommended.

4.24 How Do I Upload Objects Larger Than 5 GB?

Context

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.

A single file as large as 5 GB can be uploaded as part of a batch upload. For a single file upload, it cannot exceed 50 MB.

Methods

- **5 GB < Object ≤ 48.8 TB**

  If an object is larger than 5 GB, you can use OBS Browser+ or obsutil to upload it. Or you can use the OBS SDKs or API to upload the object (up to 48.8 TB) with a multipart upload.

  - Using OBS Browser+

    Files are uploaded using multipart upload on OBS Browser+. With multipart upload, you can upload a single file with the maximum size of 48.8 TB.

    OBS Browser allows up to 500 files to be uploaded at a time.

    For details about using OBS Browser+ to upload objects, see **Uploading a File or Folder**.

  - Using obsutil

    With multipart upload, you can upload a single file with the maximum size of 48.8 TB. There is no limit on the number of files that can be uploaded at a time.

    For details about using obsutil to upload objects, see **Uploading an Object**.

  - Using OBS SDKs

    OBS SDK supports uploading a large object with a multipart upload. A multipart upload consists of initiating a multipart upload, uploading parts one by one or concurrently, and assembling parts.

    Table 4-8 Multipart upload using OBS SDKs

Language	References
Java	**Multipart Upload (SDK for Java)**
Python	**Multipart Upload (SDK for Python)**
C	**Multipart Upload (SDK for C)**
Go	**Multipart Upload (SDK for Go)**
BrowserJS	**Multipart Upload (SDK for BrowserJS)**
.NET	**Multipart Upload (SDK for .NET)**
Android	**Multipart Upload (SDK for Android)**
iOS	**Multipart Upload (SDK for iOS)**
PHP	**Multipart Upload (SDK for PHP)**
Node.js	**Multipart Upload (SDK for Node.js)**

  - Using OBS APIs

    You can upload a large object with a multipart upload API. A multipart upload consists of:

i. **Initiating a multipart upload**
ii. **Uploading parts**
iii. **Completing a multipart upload**

- **Object > 48.8 TB**

  If you need to upload data greater than 48.8 TB to OBS, see **Migrating Local Data to OBS**.

5 Data Security, Migration, and Backup

5.1 How Is Data Security Ensured in OBS?

OBS is very secure and provides end-to-end security services.

- **Data accuracy**: OBS only determines whether data blocks exist or are damaged (repairs data if damaged) by scanning for the data. It does not read specific data.
- **Preventing data theft:**
  - Only the owner can access an undisclosed bucket or object, requiring both AK and SK. Even background engineers cannot export data stored in OBS.
  - You can also use various access control mechanisms (such as bucket policies and ACLs) to grant specific permissions to users and user groups.
- **Data transfer and access encryption**: OBS supports data transfer over HTTPS or SSL. Data encryption prior to upload is available to meet your higher security requirements.

5.2 Can I Recover OBS Data After It Is Deleted or Overwritten?

No. OBS data that you manually delete or overwrite or that is automatically deleted (by a lifecycle rule or when the account is frozen or deregistered) cannot be recovered on Huawei Cloud.

Scenarios where data can be deleted or overwritten:

- Use OBS Console, API, SDKs, OBS Browser+, obsutil, or obsfs to delete objects. For details, see **Deleting an Object**.
- Using OBS Console, API, SDKs, OBS Browser+, obsutil, or obsfs to upload a file with the same name as a previously uploaded file will overwrite the previous file in OBS.
- Based on a lifecycle rule, OBS automatically deletes the files that meet the deletion criteria defined in the rule. For details, see **Lifecycle Management**.

- If you have configured a cross-region replication rule that also synchronizes the add, modify, or delete actions, file modifications or deletions made on the source bucket will be applied to the destination bucket. For details, see **Cross-Region Replication**.
- Inappropriate access control causes files to be maliciously deleted or overwritten by others. For details, see **Permissions Management**.
- If your account is in arrears, a retention period is provided according to your tier. During the retention period, your data stored in OBS will be retained, and your account will be suspended. If your outstanding balance is not paid off when the retention period ends, data stored in OBS will be deleted and cannot be recovered. For details, see **Arrears**.

Methods of preventing accidental deletions or overwrites:

- Access control
  - Use the access control capabilities provided by OBS.
  - Enable Operation Protection. With this function enabled, OBS authenticates a user's identity when they perform any risky operation like deleting a bucket. For details, see **Critical Operation Protection**.
- Versioning

  When versioning is enabled for a bucket, OBS can keep multiple versions of an object in the bucket. That way you can quickly retrieve and restore every object version as needed, or recover data from both accidental actions and application failures. For details, see **Versioning**.
- Cross-region replication

  Replicate data from one region to another for remote backup. For details, see **Cross-Region Replication**.
- WORM

  Use WORM to protect objects from being deleted or overwritten during a specified protection period. For details, see **WORM**.

5.3 Can the AK/SK Pair Used to Access OBS Be Changed or Shared with Others?

Yes.

The pair of AK and SK can be replaced at any time.

Different users can use the same pair of AK and SK to access the same resources in OBS.

5.4 How Do I Migrate Data to OBS?

Migration Scenarios

The migration scenarios include:

- Migrating local data to OBS

- Migrating data from a third-party vendor to OBS
- Migrating data between OBS buckets across accounts or regions, or in the same region

Scenario 1: Migrating Local Data to OBS

The following table lists specific solutions for migrating local data to OBS. For details, see **Best Practices for Migrating Local Data to OBS**.

Table 5-1 Migration solutions

Migration Method	Data Volume	Requirement	Time Taken	Cost
Using OBS Tools to Migrate Data	Not larger than 1 TB	Sufficient public network bandwidth; requiring manual operations on clients or scripts to start data upload.	About 1 day for 1 TB data with the bandwidth of 100 Mbit/s	Data transmission is offered for free. Fees are charged only for storage space used on OBS.
Using CDM to Migrate Data	Less than 8 TB at a time	Subscription to the CDM service is required.	1 TB to 8 TB each day (depending on the network condition and the read and write performance of the data source)	Billing is based on CDM instance specifications and the running duration. For details, see **CDM Pricing Details**.
Using Disk-based DES to Migrate Data	Less than 30 TB at a time	Disks need to be prepared.	For details, see **How Long Does It Take to Migrate My Data to Huawei Cloud After I Have Created a DES Order?**	Billing is based on the number of disks and the running duration. For details, see **DES Pricing Details**.

Migration Method	Data Volume	Requirement	Time Taken	Cost
Using Teleport-based DES to Migrate Data	Less than 500 TB at a time	Huawei data centers provide Teleports for data transmission.	For details, see **How Long Does It Take to Migrate My Data to Huawei Cloud After I Have Created a DES Order?**	Billing is based on the number of disks and the running duration. For details, see **DES Pricing Details**.
Using a Direct Connect Connection to Migrate Data	More than 100 TB data that needs real-time online transmission every month	Private lines need to be deployed.	Depends on the bandwidth of the private line.	Fees are charged based on the distance and bandwidth of the private line. For details, see **Direct Connect Pricing Details**.

You can also **use backup software to back up local data to OBS**.

Scenario 2: Migrating Data from a Third-Party Vendor to OBS

The following table lists specific solutions for migrating data from a third-party vendor to OBS. For details, see **Best Practices for Migrating Data from Third-Party Cloud Service Vendors to OBS**.

Table 5-2 Migration solutions

Migration Mode	Application Scenarios	Supported Migration Source	Migration Speed	Cost
Using OMS to Migrate Data	Full or incremental migration of large-scale object data (less than 500 TB)	For details about the supported third-party cloud service vendors, see **Creating a Migration Task**.	10 to 20 TB per day	For billing details, see **OMS Pricing Details**.

Scenario 3: Migrating Data Between OBS Buckets

Use Object Storage Migration Service (OMS) to migrate OBS data across accounts, across regions, or in the same region.

- Cross-account migration: Data is migrated from a bucket in one Huawei Cloud account to a bucket in another one.
- Cross-region migration: Data is migrated from a bucket in one region to a bucket in another one.
- Intra-region migration: Data is migrated between buckets in the same region.

For details, see **Migrating Data Between OBS Buckets**.

5.5 How Does OBS Implement Backup and Disaster Recovery?

OBS implements backup and disaster recovery in the following ways:

- You can enable the multi-AZ mode when creating a bucket, so that data is stored in multiple AZs redundantly.
- You can also enable the cross-region replication function. Then copy data in buckets from one region to another region to implement cloud backup.
- You can also download data from OBS to your local host and back up data locally.

5.6 How Can I Migrate Data Between SFS and OBS?

Background Information

OBS is a stable, secure, efficient, and easy-to-use cloud storage service provided by Huawei Cloud. It supports standard REST APIs and can store unstructured data of any amount and format.

SFS is a high-performance file storage (NAS) provided by Huawei Cloud. It can provide storage sharing among multiple ECSs, CCEs, CCIs, and BMSs on the cloud.

How to Migrate?

SFS file systems are mounted ECSs, containers, or BMSs. Data migration between SFS and OBS is actually the data migration between servers/containers and OBS. Data in servers or containers is stored in the mounted SFS file systems.

Therefore, after an SFS file system is mounted to a server or container, you can log in to the server or container and use OBS tools, APIs, or SDKs to migrate data. If you want to migrate data from SFS to OBS, you use the OBS upload function on the server or container to upload data to OBS. If you want to migrate data from OBS to SFS, you can use the OBS download function on the server or container to download data to the SFS file system mounted on the server or container.

OBS provides various methods for data migration, as listed in **Table 5-3**. Select a proper migration method based on your operating system and business needs, and migrate data by referring to the upload and download sections in the guide manual.

NOTE

The supported operating systems, data volume, and operation complexity vary according to the migration mode. obsutil is recommended.

To reduce costs, it is recommended that you configure the intranet DNS and migrate data over the intranet of Huawei Cloud. For details, see **Accessing OBS over an Intranet**.

Table 5-3 OBS data migration tools

Tool	Supported OS (Refer to each tool guide to check supported versions)	Guide Manual
OBS Console	Windows	**Console Operation Guide**
OBS Browser+	Windows	**OBS Browser+ Tool Guide**
obsutil (recommended)	Windows/Linux	**obsutil Tool Guide**
SDKs	All	**SDK Reference**
APIs	All	**API Reference**

5.7 Does OBS Scan My Data for Other Purposes?

No.

OBS only determines whether data blocks exist or are damaged (repairs data if damaged) by scanning for the data. It does not read specific data.

5.8 Can Engineers Export My Data from the Background of OBS?

No. Background engineers cannot export your data.

For example, if a bucket or an object is undisclosed when you access the bucket or object, only the owner of the bucket or object can access it. Further, the access to the bucket or object requires access keys (AK/SK).

5.9 How Does OBS Protect My Data from Being Stolen?

OBS provides multiple security mechanisms to ensure your data security.

- Access security: Only the bucket or object owner can access the bucket or object and access keys (AK and SK) are required. Multiple permissions control methods, such as ACL and bucket policies, are used to control access of non-bucket owners to the bucket or object.
- Data security: Multiple functions, such as server-side encryption, WORM, and URL validation, are provided to ensure data security in OBS.

5.10 What Are the Durability and Availability of OBS?

OBS provides multi-level reliability assurance for storage media, servers, cabinets, data centers, and regions by leveraging the following technologies: slow disk or bad sector detection, intra-AZ device and data redundancy, cross-AZ data disaster recovery, cross-region replication, and more. OBS delivers up to 99.9999999999% (12 nines) of data durability, and up to 99.995% of availability, far higher than a conventional architecture would offer.

NOTE

OBS data durability and availability vary depending on the storage class and redundancy storage policy. For details, see **Comparison of Storage Classes**.

The 12 nines of durability means that the average annual loss rate of objects is expected to be 0.0000000001%. For example, if you store 100 million objects in OBS, only one object may be lost every 10,000 years.

Availability is the service continuity. A 99.995% availability means that if you keep accessing OBS for 100,000 minutes (about 69 days), you can expect no more than 5 minutes of unavailability.

In addition, the availability of OBS is double ensured by the **Service Level Agreement**. Compensation is offered if the committed service availability is not met.

5.11 What Are the Differences Between Single-AZ and Multi-AZ Storage in OBS?

Question 1:

Q: What are the differences when multi-AZ storage is enabled or disabled during the bucket creation?

A: When the multi-AZ mode is enabled, data is redundantly stored in multiple AZs, improving data reliability. Data is stored in a single AZ if the multi-AZ mode is disabled, with lower costs. For details, see **Product Pricing Details**.

Question 2:

Q: Is data stored as copies in multiple AZs after the multi-AZ mode is enabled? If an AZ is faulty, is data complete in other AZs?

A: The Erasure Code (EC) algorithm, instead of multiple copies, is used to ensure data redundancy in the multi-AZ mode. If the multi-AZ storage is enabled for a bucket, data is stored in multiple AZs in the same region. If an AZ is unavailable, data can still be properly accessed in other AZs. The multi-AZ mode is suitable for data storage scenarios that require high reliability. The multi-AZ storage tolerates only faults of a single AZ.

Question 3:

Q: Can I change the status of the multi-AZ mode without deleting the bucket?

A: No. If the multi-AZ mode is enabled upon creation of a bucket, it cannot be disabled. You can migrate data to another bucket and delete the bucket that has the multi-AZ mode enabled, if you do not need multi-AZ storage.

5.12 What Redundancy Storage Technology Does OBS Use?

OBS uses the Erasure Code (EC) algorithm, instead of multiple copies, to ensure data redundancy.

Compared with the multi-copy redundancy, EC delivers a higher storage space utilization while maintaining the same reliability level.

A bucket with single-AZ storage uses the EC algorithm for data redundancy among nodes in one AZ. A bucket with multi-AZ storage not only ensures redundancy for the data among nodes in an AZ, but also across multiple AZs.

6 Versioning

6.1 Can I Recover a Deleted Object?

- When versioning is enabled, if you delete an object without specifying a version ID, the object is tagged with a delete marker and displayed in the list of **Deleted Objects**. You can recover the object from that list.
- Versioning enabled for a bucket:
  - If the **Historical Versions** button is disabled, a deleted object is not displayed in the object list. After the button is enabled, the current object version with a delete marker and the deleted object (also the historical object version) are displayed in the object list. In this case, you can click **Permanently Delete** in the **Operation** column of the current object version with a delete marker to recover the deleted object.

    NOTE

    If you delete an object from a versioning-enabled bucket, instead of deleting the object permanently, OBS inserts a delete marker, which becomes the current object version. The deleted object becomes the historical version. After that, if you enable the **Historical Versions** button above the object list, you can see the current object version with a delete marker and the deleted object that has become a historical version.
  - If the **Historical Versions** button is enabled, you choose **More** > **Permanently Delete** in the **Operation** column of an object version other than the current one with a delete marker to permanently delete the object. The deleted object cannot be recovered.
- If you delete an object with a version ID specified when versioning is enabled or you delete an object when versioning is not enabled, OBS permanently deletes the object, and you cannot recover it.

For details, see **Versioning Overview**.

7 Server-Side Encryption

7.1 How Do I Access or Download an Encrypted Object?

Encrypting an Object

Method 1: Enable server-side encryption when you create a bucket. Then, all types of objects uploaded to the bucket will be automatically encrypted with the encryption method and key you specified during bucket creation.

Method 2: Specify an encryption method and a key type when you upload an object.

Accessing or Downloading an Encrypted Object

When an object is encrypted with SSE-OBS, configure a public read policy (which grants anonymous users access to an object) for the object and then you can directly access this object.

When an object is encrypted with SSE-C, it cannot be accessed directly, even if it has a public read policy (which grants anonymous users access to an object) configured. Whereas, you can call an API to access or download the object. For details, see **Downloading Objects**.

When an object is encrypted with SSE-KMS, it cannot be accessed directly, even if it has a public read policy (which grants anonymous users access to an object) configured. To access or download an encrypted object, use either of the following methods:

Method 1: Access the encrypted object as a user with the **KMS CMKFullAccess** permission. The region where your **KMS CMKFullAccess** permission applies must be the one where the bucket storing the object is located. For details about how to grant users the **KMS CMKFullAccess** permission, see **Assigning Permissions to an IAM User**.

Method 2: Use the temporary URL generated by sharing the encrypted object. When you use the shared URL for access, the server automatically decrypts the object.

For example, if you want your encrypted object (such as a video or audio file) to be accessed by anonymous users, you can **share your object** and send the generated URL to others.

7.2 Why Cannot an Authorized Account or User Upload or Download KMS Encrypted Objects?

Before using the server-side encryption of OBS, ensure that the **OBS OperateAccess** and KMS-related permissions have been granted to the account or user on IAM. If the current account or user is the grantee, it also requires the **OBS OperateAccess** permission. Contact your delegating party for authorization. For details, see **Account Delegation**.

CAUTION

- To access OBS, you need to **obtain a temporary access key pair and a security token using an agency**.
- DEW is not a global service and KMS is a sub-service of it, so the **KMS Administrator** permission must be configured for the region where the bucket is located.
- The agency information is stored on IAM. The configuration takes effect approximately 15 minutes after the configuration is complete.

7.3 Are Additional Permissions Required When I Share an Object with SSE-OBS Encrypted?

No.

SSE-OBS uses a data key derived from the OBS root key to encrypt or decrypt an object.

OBS does not need to interact with KMS. Therefore, you do not need to grant special permissions when sharing objects.

7.4 Does OBS Support Encrypted Upload?

OBS provides server-side encryption function. You can encrypt objects while uploading. Data is encrypted on the server and then stored in OBS. When downloading the encrypted objects, the encrypted data will be decrypted on the server and displayed for you in plaintext.

Table 7-1 lists the encryption methods supported by OBS Console, client, and tools.

Table 7-1 Object upload encryption in different access modes

Access Mode	Support for Upload Encryption	Reference
OBS Console	Yes	**Uploading a File with Server-Side Encryption**
OBS Browser+	No If a bucket has server-side encryption enabled, objects uploaded to it will be automatically encrypted.	-
obsutil	No If a bucket has server-side encryption enabled, objects uploaded to it will be automatically encrypted.	-
API	Yes	
SDKs	Yes	For details, see the "Server-Side Encryption" in the **SDK Developer Guide** for different programming languages.

7.5 What Techniques Can I Use to Encrypt Data on OBS?

Before uploading your data to OBS, you can encrypt the data to ensure security during transmission and storage. OBS has no restrictions on client encryption techniques.

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

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

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

OBS supports SSE-KMS, SSE-OBS, and SSE-C when calling APIs. With SSE-C, OBS uses the customer-provided keys and their MD5 values for server-side encryption.

7.6 Will OBS Server-Side Encryption Encrypt My Existing Objects That Are Unencrypted?

No.

No. OBS encrypts only objects that are uploaded after the server-side encryption configuration is effective. If you want to encrypt existing objects, delete them and upload them again.

7.7 Will I Be Billed for the Encryption Provided by OBS Server-Side Encryption?

When using SSE-KMS, you are billed for both storage and KMS key requests.

When using SSE-OBS and SSE-C, you are only billed for storage.

To learn the billing for KMS key requests, see **How Is DEW Charged?**

To learn the billing for storage, see **Storage Space**.

7.8 Does OBS SSE-KMS Allow Anonymous Access?

No.

Anonymous users do not have access to KMS, so SSE-KMS does not allow anonymous access.

8 How Do I Use Cross-Region Replication?

8.1 Why Objects Are Not Copied to the Destination Bucket After the Cross-Region Replication Rule Has Been Created?

- If the function of synchronizing existing objects is not enabled for a cross-region replication rule, existing objects in a bucket will not be copied to the destination bucket.
- Newly uploaded objects in the Archive storage class are not replicated to the destination bucket.
- A cross-region replication rule may not take effect immediately upon its configuration. Accordingly, the objects that this rule is applied to may not be replicated immediately after the rule is configured.

8.2 Will an Object Deletion in a Source Bucket Be Synchronized to the Destination Bucket?

- If your cross-region replication rules are configured on OBS Console, object deletions in the source bucket will not be synchronized to the destination bucket by default.
- If your cross-region replication rules are configured using the API, the synchronization depends on the setting of the **DeleteData** parameter.
  - If the value of **DeleteData** is **Enabled**, the deletions will be synchronized.
  - If the value of **DeleteData** is **Disabled**, the deletions will not be synchronized.

After the cross-region replication rule is enabled, objects that meet the following conditions are copied to the destination bucket:

- Newly uploaded objects (excluding objects in the Deep Archive or Archive storage class)
- Updated objects, for example, objects whose content or ACL information is updated

- Historical objects in a bucket with **Synchronize Existing Objects** enabled (excluding objects in the Archive or Deep Archive storage class)

9 Domain Name Management

9.1 Why Is the Message "NoSuchBucket" Displayed When I Use a User-Defined Domain Name to Access a Bucket That Can Be Accessed by the OBS Domain Name?

The CNAME resolution is not configured, after the domain name is bound to your OBS bucket.

To configure a user-defined domain name for an OBS bucket, perform the following steps:

1. **Configure a user-defined domain name** to bind the default bucket domain name of the bucket with its user-defined domain name.
2. **Add a CNAME record set** to map the default bucket domain name of the bucket to its user-defined domain name.

For details, see **Configuring a User-Defined Domain Name**.

9.2 With CDN Acceleration Enabled, Why Are the Objects in My OBS Bucket Directly Downloaded When I Access Them?

Symptoms

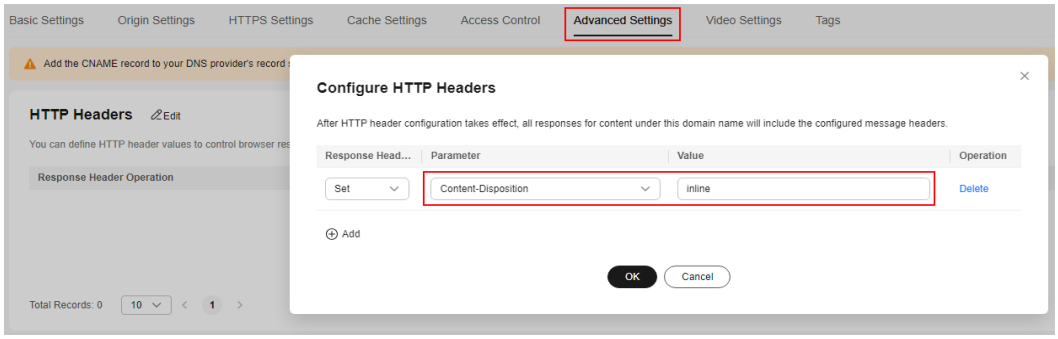
After CDN acceleration is enabled for a user-defined domain name on OBS Console or the origin server address for an acceleration domain name added through the CDN console is set to an OBS bucket domain name, the objects stored in OBS cannot be previewed, but are directly downloaded when they are accessed.

Solutions

You can use the following two methods to fix this issue:

Method 1

Log in to the CDN console and go to the **Domains** page. On the **Domains** page, click the target domain name and then the **Advanced Settings** tab. Add the **Content-Disposition** response header and set its value to **inline**.

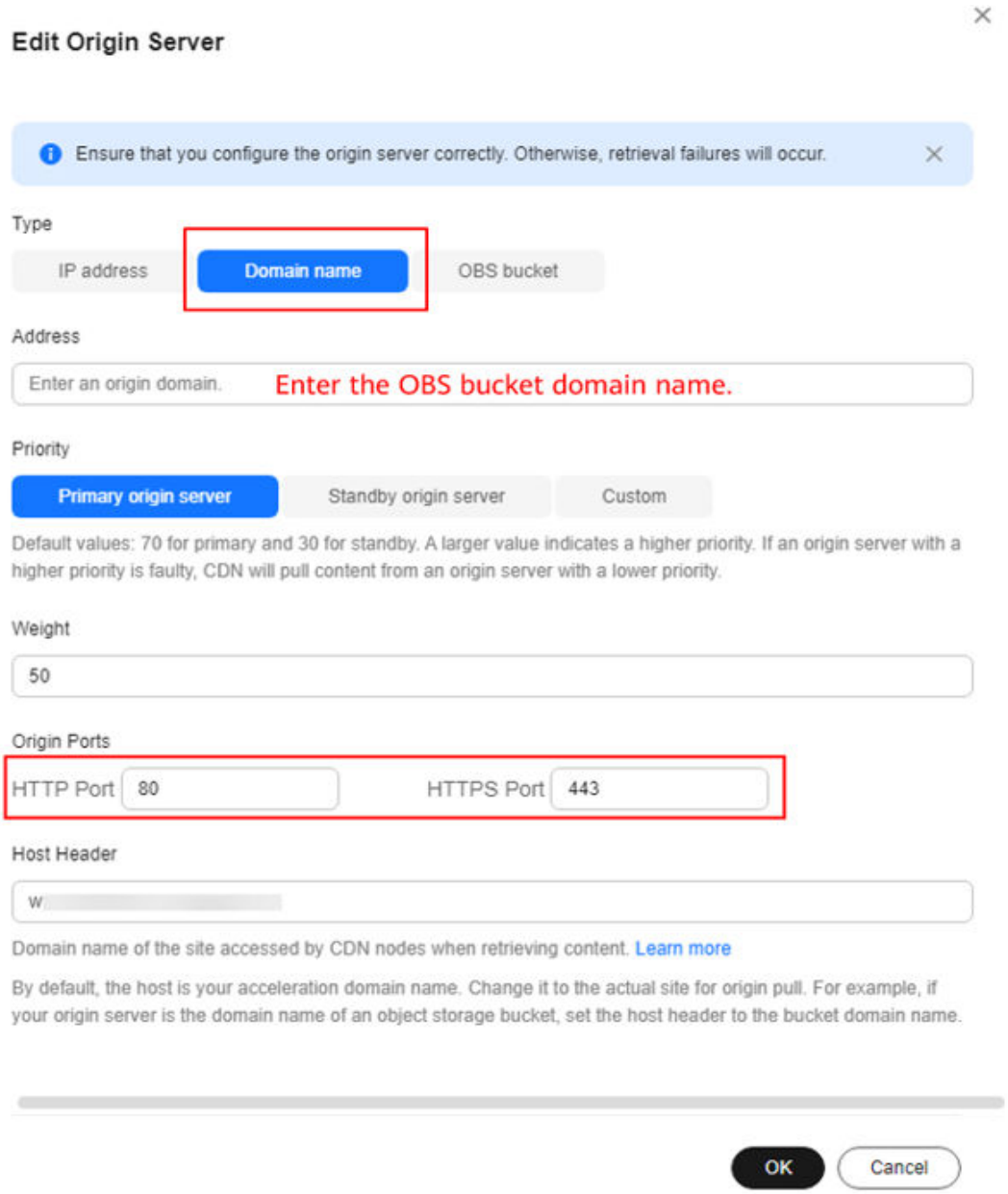


NOTE

If the issue persists after the preceding configuration is complete, refresh the cache on the CDN console. For details, see **Cache Refreshing**.

Method 2

Log in to the CDN console and go to the **Domains** page. On the **Domains** page, click the target domain name, then the **Basic Settings** tab, and click **Edit** next to **Origin Server Settings**. In the displayed dialog box, change the value of **Type** from **OBS bucket** to **Domain name**, configure **Origin** to the OBS bucket domain name, and set **HTTP port** and **HTTPS port** to **80** and **443** respectively.



NOTE

In this method, the origin server's domain name is used to access CDN. Generated retrieval traffic will be billed as the outbound Internet traffic and cannot be covered by pull traffic packages offered by OBS.

If the issue persists after the preceding configuration is complete, refresh the cache on the CDN console. For details, see **Cache Refreshing**.

9.3 What Is the Relationship Between OBS Bucket Names and Domain Names?

An OBS bucket name is the name of the bucket you created.

The domain name is the endpoint of the region where the bucket is located.

The domain name for accessing your bucket is the bucket name plus the regional domain name (*bucket_name.domain_name*).

9.4 Why Is the CNAME Resolution Status Unknown?

If the domain name you bound to a bucket is not provided by Huawei Cloud Domains, your ownership for this domain name cannot be confirmed. This results in an unknown CNAME resolution status.

To handle this, you need to configure a resolution rule. For details, see **Configuring a CNAME Record**.

9.5 Why Can Only the Domain Names I Bought on Huawei Cloud Be Automatically Resolved In One Click?

When you purchase a user-defined domain name on Huawei Cloud, you can bind the domain name to a bucket and click **Resolve** to automatically add a CNAME record set for the domain name.

If your domain name is from another domain name service provider, you need to specify DNS settings. For details, see **Configuring a CNAME Record**.

10 How Do I Use Static Website Hosting?

10.1 What Types of Websites Can I Use OBS to Host?

Static websites contain static web pages and some scripts that can run on clients, such as JavaScript and Flash.

OBS supports static website hosting. You can configure the static website hosting function for your buckets on OBS Console. When a client accesses objects from the website address of a bucket, the browser can directly resolve the web resources and present them to end users.

10.2 How Do I Obtain the Static Website Hosting Address of a Bucket?

You can obtain the static website hosting address of the bucket on OBS Console.

You can also get the address according to the following rule and format. Address format: https://*Bucket name.Domain name of the hosted static website*

For example, if the static website hosting has been configured for bucket **testbucket** in region CN-Hong Kong, the static website access address of the bucket is **https://testbucket.obs-website.ap-southeast-1.myhuaweicloud.com**.

For more information about static website hosting, see **Using a User-Defined Domain Name to Host a Static Website**.

11 Image Processing

11.1 How Do I Access Image Processing with a URL?

Accessing Images Not Publicly Readable

To access images that cannot be read by the public, add image processing parameters during signature calculation to create a signed temporary URL.

A Java SDK sample code is provided as follows. For details, see **SDK Overview**.

```
// Here uses the endpoint corresponding to the CN-Hong Kong region as an example.
String endPoint = "https://obs.ap-southeast-1.myhuaweicloud.com";
// Hard-coded or plaintext AK and SK are risky. For security purposes, encrypt your AK and SK and store them in the configuration file or environment variables.
// In this example, the AK and SK are stored in environment variables for identity authentication. Before running this example, configure environment variables ACCESS_KEY_ID and SECRET_ACCESS_KEY.
// Obtain an AK and SK pair on the management console. For details, see https://support.huaweicloud.com/intl/en-us/usermanual-ca/ca_01_0003.html.
String ak = System.getenv("ACCESS_KEY_ID");
String sk = System.getenv("SECRET_ACCESS_KEY");

// Create an ObsClient instance.
ObsClient obsClient = new ObsClient(ak, sk, endPoint);

// Set the URL validity period to 3600 seconds.
long expireSeconds = 3600L;
TemporarySignatureRequest request = new TemporarySignatureRequest(HttpMethodEnum.GET, expireSeconds); request.setBucketName("bucketname");
request.setObjectKey("objectname");

// Configure image processing parameters.
Map<String,Object> queryParams = new HashMap<String, Object>();
queryParams.put("x-image-process", "image/resize,m_fixed,w_100,h_100/rotate,100");
request.setQueryParams(queryParams);

// Obtain the URL that supports image processing.
TemporarySignatureResponse response = obsClient.createTemporarySignature(request);
System.out.println("Getting object using temporary signature url:");
System.out.println("\t" + response.getSignedUrl());
```

Accessing Images Publicly Readable

To access images that can be read by the public, add image processing parameters to the URL request.

Sample URL for obtaining the information about the **example.jpg** image:

https://hw-image-demo.obs.ap-southeast-1.myhuaweicloud.com/example.jpg?x-image-process=image/info

11.2 After CDN Acceleration Is Enabled, Where Are Processed Images Stored?

If you access the image processing service through CDN, processed images will be cached by CDN.

Therefore, if you perform the same processing operations on the same images again, CDN returns the processed images without accessing the image processing service, and you will not be charged for the image processing requests.

11.3 After I Performed Image Processing in My Logging-enabled Bucket, Why Was My Bucket Accessed by IP Addresses Starting with 100?

It is found that IP addresses starting with 100 accessed a bucket, after logging was enabled for the bucket and images were processed in the bucket.

This is because original images to be processed are downloaded from the bucket over the intranet by OBS, and the logging function records intranet IP addresses. Download requests also incur costs.

11.4 How Is Image Processing Billed?

To learn the pricing details of image processing, see the **Product Pricing Details** tab page at **OBS Pricing Details**.

Billing Factors

- Size of the original image, in GB

  The feature will be charged at a fixed unit price based on the number of service months.

If more than one image is processed, the total size of these images will be automatically calculated. For example, if an image of 0.01 GB is cropped and compressed into 0.005 GB, the image size is still regarded as 0.01 GB by OBS.

Billing Formulas

The following formulas apply to Standard storage and Infrequent Access storage. Archive or Deep Archive storage is not considered. For details, see **Table 11-1**.

- 0–10 TB (inclusive): Each HUAWEI ID has a monthly free quota of 10 TB.
- More than 10 TB: Cost = (Total image size – 10 TB) × Unit price (USD/GB)

Table 11-1 Billing criteria of image processing

Item	Unit Price for Standard Storage (Monthly)	Unit Price for Infrequent Access Storage (Monthly)	Unit Price for Archive Storage (Monthly)	Unit Price for Deep Archive Storage (Monthly)
Image processing	• 0–10 TB (inclusive): free • More than 10 TB: See the **Product Pricing Details** tab page at **OBS Pricing Details**.	• 0–10 TB (inclusive): free • More than 10 TB: See the **Product Pricing Details** tab page at **OBS Pricing Details**.	N/A	N/A

11.5 How Many Image Styles Can I Create in a Bucket?

A bucket can have a maximum of 100 styles.

You can create an image style in either of the following ways:

- **Using OBS Console**
- **Making an API call**

12 Parallel File System

12.1 Why Is 256 TB Displayed After I Mounted a Parallel File System?

Background

When you run the **df -h** command on a client, the system returns 256 TB just for display purposes.

Description

256 TB does not mean anything. There is no limit on the capacity of the parallel file system that you can use.

12.2 Can I Sort Files in the File List?

Yes.

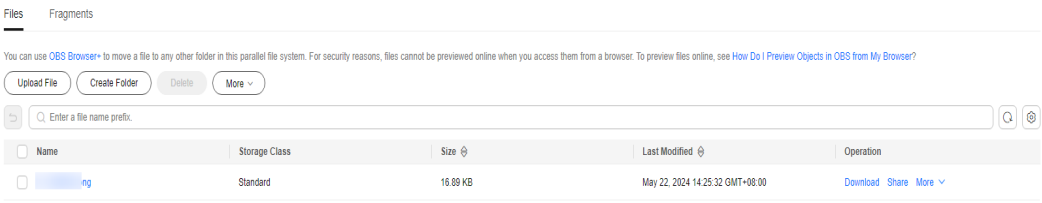
In the file list, you can click next to the size or last modification time to sort files.

The first 1,000 files can be sorted by last modification time. If there are over 5,000 files in a parallel file system, they will be sorted in alphabetical order and can only be searched by object or file name prefix.

NOTE

Folders can be sorted by size, but not by their last modification time.

Figure 12-1 File list



13 Monitoring

13.1 Why Can't I Find the Statistics on OBS 5XX Status Codes on Cloud Eye?

OBS metrics on Cloud Eye are displayed based on your requests. Once you perform a request or storage action, Cloud Eye will display the corresponding request or storage metric.

For instance, if the server returns a 5*XX* status code to you, the metric for measuring the number of 5*XX* status codes will appear on Cloud Eye.

14 OBS Console

14.1 Web Browser Compatibility

Table 14-1 lists the web browser versions compatible with OBS Console.

Table 14-1 Supported web browser versions

Web Browser	Version
Internet Explorer	• Internet Explorer 9 (IE9) • Internet Explorer 10 (IE10) • Internet Explorer 11 (IE11)
Firefox	Firefox 55 and later
Chrome	Chrome 60 and later

14.2 Time Difference Is Longer Than 15 Minutes Between the Client and Server

Symptom

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.

Cause

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.

Solution

To resolve this problem, adjust your local time (UTC) and try again.

14.3 The Object Name Changes After an Object with a Long Name Is Downloaded to a Local Computer

Symptom

After an object with a relatively long name is downloaded to a local path, the object name changes.

Cause

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.

Solution

Change the object name to a string of no more than 255 characters.

14.4 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.

14.5 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?

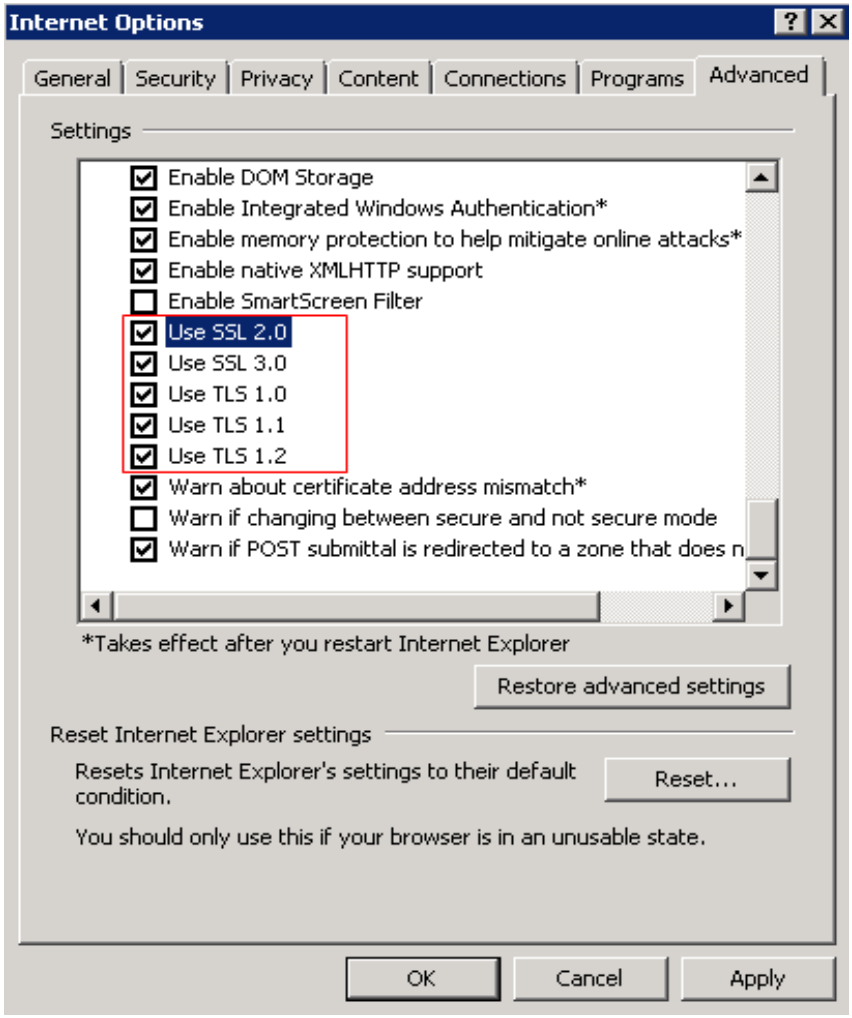
Answer

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 14-1**.

Figure 14-1 Internet Options



Step 3 Click **OK**.

----End

14.6 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 14-2** lists some common error codes in OBS error responses.

Table 14-2 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.
Obs.0009	A conflicting operation is being performed on this resource. Please retry. 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.
Obs.0010	Deletion failed. Check whether objects or objects of historical versions exist in the bucket.
Obs.0011	The bucket policy is invalid. Configure it again.
Obs.0012	The requested bucket name already exists. Bucket namespace is shared by all users in the system. Enter a different name and try again.
Obs.0013	The requested folder name already exists. Enter a different name and try again.
Obs.0014	The file size has exceeded 50 MB. Use OBS Browser+ to upload it.

Error Code	Description
Obs.0015	The absolute path in the search criteria cannot exceed 1023 characters. Please retry.
Obs.0016	Upload failed. Possible causes: 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	The end time of the new validity period must be later than that of the old validity period.
Obs.0018	The validity period cannot be shorter than the remaining period.
Obs.0019	Cannot determine whether the bucket has objects or fragments. Check whether you have the read permission for this bucket.
Obs.0020	TMS system error. Try again later.
Obs.0021	You do not have permissions to access TMS. Configure the required permissions in IAM.
Obs.0022	The TMS system is busy. Try again later.

15 OBS Browser+, obsutil, and Other OBS Tools

15.1 When Downloading a Folder Using obsutil, the Download Speed Slows After the Folder Download Progress Reaches 90%

This problem may occur in the following scenarios:

- Scenario 1: The folder contains a few large objects among a large number of small objects. Large objects are downloaded at fast speed. But the download speed of small objects in large quantity is closely related to the TPS performance. Therefore, if the remaining 10% are mostly small objects, the download speed may decrease.
- Scenario 2: The folder contains same-size objects. It is possible that all objects have been downloaded but are queuing to be written to disks, which may be reflected as a slowdown in the download progressing. In this case, check the writing speed of your clients.

15.2 With obsutil, Downloading a File Fails After the Download Progress Reaches 99%

Possible causes:

1. Network fluctuation
2. Failure in caching the file to the target folder due to disk I/O freezes.

Solution:

1. Run the download command again.

   The resumable download function is enabled by default for obsutil download tasks. You only need to run the same download command again, the failed file download will be resumed and the file will be downloaded to your local path.

2. If the problem persists, upgrade obsutil to the latest version and try again.
3. If the problem persists still, contact the customer service for further support.

15.3 Slow Upload and Download Through obsutil

OBS does not limit the upload or download rate, nor does obsutil limit the data transfer rate.

If obsutil is used to upload and download files over the public network, the bandwidth is determined by the public network bandwidth. If internal networks are used, the network condition is determined by the network adapter, disk I/O, and restrictions on resource preemption.

If you are experience slow upload or download, perform the following operations:

1. Check the network.

   Ping the OBS endpoint (for example, **obs.ap-southeast-1.myhuaweicloud.com**) in the current region to check the network latency and packet loss rate.

   Regions and Endpoints
2. Check whether OBS is accessed over internal networks.

   For details, see **How Do I Determine Whether I Am Accessing OBS over an Intranet?**
3. For batch uploading or downloading small files in huge numbers, the speed is mainly determined by TPS (number of files processed in a second) instead of the bandwidth.
4. For batch upload, you can add **-j** and **-p** parameters, and raise the parameter values, and check whether the speed is improved. For details, see **Fine-Tuning obsutil Performance**.

15.4 How Do I Use the obsutil cp Command to Enable Incremental Upload, Download, or Replication?

When running the **obsutil cp** command to upload or download data, you can add the **-u** parameter to enable the incremental upload/download function.

This parameter indicates that the system will compare the source path with the target path when uploading, downloading, or replicating an object. The system uploads, downloads, or replicates an object only when the target object does not exist, the object size is inconsistent, or the last modification time of the target object is earlier than that of the source object.

15.5 Can I Mount My Parallel File System to a Windows Server?

No. A parallel file system can currently only be mounted to a Linux server through obsfs.

For details, see **Mounting a Parallel File System**.

16 APIs and SDKs

16.1 Failure with OBS SDK in Uploading a File Greater than 5 GB

OBS server has a restriction on the object upload API, which only allows a maximum of 5 GB for an upload. If you want to upload a file greater than 5 GB, use the multipart upload API. Operations are detailed in the following procedure:

1. Call the OBS API for initializing a multipart upload task to generate a multipart upload ID (Upload ID).
2. Call the OBS API for uploading parts one by one or in parallel. The size of each part can be up to 5 GB.
3. After parts are uploaded, call the OBS API to merge parts to generate the complete object.

OBS SDKs support atomic operations. In the section "Multipart Upload" of *OBS SDK Reference* in different programing languages, you can find more information about how to implement multipart upload using OBS SDKs.

16.2 What Can I Do When Error Message "okhttp3.RequestBody.create(java.lang.String,okhttp3.MediaType)" Is Displayed for Java SDK?

Symptom

Error message "okhttp3.RequestBody.create(java.lang.String,okhttp3.MediaType)" is reported for Java SDK.

Cause

Spring Boot specifies the version of third-party dependencies. For details, see **Spring Boot Managed Dependency Coordinates**. When the OBS SDK is introduced to a Spring Boot framework, the version of OkHttp3 (dependency

specified by the SDK) will be changed from 4.8.0 to 3.14.9. As a result, the specified method cannot be obtained. To avoid this issue, you can use the bundle SDK that integrates third-party dependencies, or explicitly reference OkHttp3 4.8.0 in your project.

Solution

Refer to **Resolving Dependency Missing and Dependency Conflict** to check whether the third-party dependency version is correctly referenced. Alternatively, use the following code to import the bundle SDK to replace the original one.

```
<dependency>
    <groupId>com.huaweicloud</groupId>
    <artifactId>esdk-obs-java-bundle</artifactId>
    <version>[3.21.8,)</version>
</dependency>
```

16.3 What Are the Differences Between PUT and POST Upload Methods?

Parameters are passed through the request header if the PUT method is used to upload objects; if the POST method is used to upload objects, parameters are passed through the form field in the message body.

With the PUT method, you need to specify the object name in the URL, but object name is not required with the POST method, which uses the bucket domain name as the URL. Request lines of these two methods are given as follows:

```
PUT /ObjectName HTTP/1.1
POST / HTTP/1.1
```

Either PUT or POST method allows the object size of [0, 5 GB] for each upload. If you need to upload an object greater than 5 GB, use the multipart upload method.

For details about PUT and POST APIs, see **Uploading Objects - PUT** and **Uploading Objects - POST**.

16.4 Does an Append Upload Support the Lock Mechanism for Concurrent Operations?

OBS itself does not support this mechanism. If you want to prevent an object from being concurrently accessed, you must add a lock mechanism for objects in upper-layer applications.

If multiple clients simultaneously upload, query, or delete the same object or bucket, these operations may reach the system at different times and have different latency periods, so different results may return. For example, if multiple clients simultaneously upload the same object, the last upload request received by the system will replace the previous one.

For details, see **Consistency of Concurrent Operations**.

16.5 Why Don't the Signatures Match?

Symptom

The following error is reported during an OBS API call.

Status code: 403 Forbidden

Error code: SignatureDoesNotMatch

Error message: The request signature we calculated does not match the signature you provided. Check your key and signing method.

Possible Causes

The provided signature does not match the signature calculated by the system.

Solution

Step 1 Check the endpoint.

Check the endpoint if you are using the OBS SDK.

The correct endpoint format is **obs.***regionID***.myhuaweicloud.com**. If the endpoint is set to a bucket domain name (*bucketname***.obs.***regionID***.myhuaweicloud.com**), a signature mismatch error will also be reported.

Step 2 Check the AK and SK.

Ensure that the AK and SK you entered are correct, so they can match those used in the request.

Step 3 Check **HTTP-Verb**.

Ensure that the **HTTP-Verb** in the signature is the same as that in the request.

Step 4 Check **Date** and **Expires**.

- Signature in a header: Check whether the **Date** in the signature is the same as that in the request header.
- Signature in a URL: Check whether the **Expires** in the signature is the same as that in the request URL.

  NOTE

  If the URL signature generator is used, the **Expires** is set to a value in seconds, for example, **3600** for one hour. The value of **Expires** in the generated URL is the last point in time of the validity period.

Step 5 Check headers.

Check **Content-MD5**, **Content-Type**, and **Canonicalized Headers**. If any of them are contained during signature calculation, they must be also contained in the request.

> **NOTE**
>
> If a URL with a signature contained is used to access OBS resources through a browser, the header parameters above cannot be contained during signature calculation.

Step 6 Check **Canonicalized Resource**.

Canonicalized Resource indicates the OBS resources that are requested. Configure this parameter based on the requirements in the API reference. For details, see **Authentication of Signature in a Header** or **Authentication of Signature in a URL**.

Step 7 Check **StringToSign**.

Check whether **StringToSign** is constructed based on the following rules:

- Signature in a header:
  ```
  HTTP-Verb + "\n" + Content-MD5 + "\n" + Content-Type + "\n" + Date + "\n" + CanonicalizedHeaders + CanonicalizedResource
  ```
- Signature in a URL:
  ```
  HTTP-Verb + "\n" + Content-MD5 + "\n" + Content-Type + "\n" + Expires + "\n" + CanonicalizedHeaders + CanonicalizedResource
  ```

> **NOTE**
>
> If a parameter is left blank, put it in a new line.

Step 8 Check the signature calculation.

Check whether the signature is calculated as follows:

1. Construct the request string **StringToSign**.
2. Perform UTF-8 encoding on the result in the **1**.
3. Use the SK to perform the HMAC-SHA1 signature calculation on the result in **2**.
4. Perform Base64 encoding on the result in **3**. If the signature is contained in a header, this step generates the final signature and no further actions are required.
5. If the signature is contained in a URL, perform the URL encoding on the result in **4** to obtain the final signature.

Step 9 Verify the signature by referring to **User Signature Verification**.

----End

